



**An Roinn Gnóthaí
Eachtracha agus Trádála**
Department of
Foreign Affairs and Trade

**Request for Tenders dated 14/09/2026
for the provision of**

External ICT Technical Support Services

Tender procedure: Open procedure

Tender Response Deadline 16/10/2026 13:00

Contents

Part 1:	Introduction
Part 2:	Instructions to Tenderers
Part 3:	Selection and Award Criteria
Appendix 1:	Requirements and Specifications
Appendix 2:	Pricing Schedule
Appendix 3:	Tenderer's Statement
Appendix 4:	Declaration as to Personal Circumstances of Tenderer
Appendix 5:	Services Contract
Appendix 6:	Confidentiality Agreement
Appendix 7:	European Single Procurement Document (ESPD)
Appendix 8	Tender Response Document (TRD)

Part 1: Introduction

1.1 The Minister for Foreign Affairs and Trade (the “Contracting Authority”) invites tenders (“Tenders”) to this request for tenders (“RFT”) from economic operators (“Tenderers”) for the provision of the services as described in Appendix 1 to this RFT (the “Services”).

1.2 In summary, the Services comprise: the provision of suitably qualified and experienced ICT service provider(s) to deliver professional ICT services and resources in support of its current and evolving technology environment.

The Services will encompass the provision of skilled personnel with appropriate experience and competencies to support, maintain, and enhance the Contracting Authority’s infrastructure and technologies, and to contribute to future digital and operational initiatives.

The Services will be delivered in accordance with the requirements and specifications set out in this RFT, with further detail provided in Appendix 1.

1.3 This public procurement competition will be divided into 3 lots (each a “Lot”) as described below. Each Lot will result in a separate contract. Tenderers may bid for one, two or all three Lots. A Tenderer may be awarded one, two or three Lots, subject to meeting the requirements of the RFT and the outcome of the tender evaluation.

Lot 1: Networks and Communications Team

- 1 x Network Architect (Enterprise & Communications Infrastructure) - Senior Level
- 1 x Network Security Architect (Enterprise Security Infrastructure) - Senior Level
- 1 x Network Security Engineer (Enterprise Security Infrastructure) - Senior Level
- 2 x Network VoIP Webex Engineer (Enterprise & Communications Infrastructure) - Intermediate Level
- 1 x Network Security Engineer (Enterprise Security Infrastructure) - Intermediate Level
- 1 x Network Engineer (Enterprise & Communications Infrastructure) - Junior Level

Lot 2: Infrastructure Team

- 1 x Enterprise Infrastructure Architect - Senior Level
- 1 x ICT Infrastructure Engineer (SQL Server Design & DBA) - Senior Level
- 1 x ICT Infrastructure Engineer (Enterprise Services & Linux) - Senior Level
- 2 x ICT Infrastructure Engineer (Microsoft Cloud & Power Platform) - Senior Level
- 1 x ICT Infrastructure Engineer (SCCM Endpoint Configuration Manager) - Senior Level
- 2 x ICT Infrastructure Engineer (Microsoft Hybrid Cloud & Enterprise Services) - Senior Level
- 2 x ICT Infrastructure Engineer (Microsoft Hybrid Cloud & Enterprise Services) - Intermediate Level

Lot 3: SharePoint Team

- 1 x SharePoint Programme Manager - Senior Level
- 1 x SharePoint Technical Project Manager - Senior Level
- 1 x SharePoint Infrastructure Engineer - Senior Level
- 1 x SharePoint Solutions Designer (Forms & Business Solutions) - Senior Level
- 1 x Power Platform Developer - Senior Level
- 1 x SharePoint Testing & Quality Assurance Specialist - Intermediate Level
- 1 x SharePoint Administrator - Junior Level

1.4 This public procurement competition (the “Competition”) will be conducted in accordance with the open procedure under the European Union (Award of Public Authority Contracts) Regulations 2016 (Statutory Instrument 284 of 2016) (the “Regulations”). Any contract that may result from this Competition (the “Services Contract”) will be issued for a term of **three (3) years** (“the Term”).

1.5 The Contracting Authority reserves the right to extend the Term for a period or periods of up to one (1) year with a maximum of two (2) such extension or extensions on the same terms and conditions, subject to the Contracting Authority’s obligations at law. The maximum term for the contract will be five (5) years (60 months).

1.6 The Contracting Authority estimates that the expenditure on the Services to be covered by the proposed Service Contract may amount to some €17,500,000 (excl. VAT) across all Lots over the Term and any possible extensions.

- Lot 1: Networks and Communications Team may amount to some €5,202,590 (excl. VAT).
- Lot 2: Infrastructure Team may amount to some €6,900,655 (excl. VAT).
- Lot 3: SharePoint Team may amount to some €5,396,755 (excl. VAT).

Tenderers must understand that these figures are estimates only based on current and future expected usage.

1.7 Contracting Authority policy seeks to encourage participation on a fair and equal basis by Small and Medium Enterprises (“SME”s) in this Competition. SMEs that believe the scope of this Competition is beyond their technical or business capacity are encouraged, subject to paragraph 2.5, to explore the possibilities of forming relationships with other SMEs or with larger enterprises. Through such relationships they can participate and contribute to the successful implementation of any Services Contract that may result from this Competition and therefore increase their social and economic benefits.

Larger enterprises are also encouraged, subject to paragraph 2.5, to consider the practical ways that SMEs can be included in their proposals to maximise the social and economic benefits of any Services Contracts that may result from this Competition.

Part 2: Instructions to Tenderers

2.1 IMPORTANT NOTICES

2.1.1 While every effort has been made to provide comprehensive and accurate information in all notices and documents prepared for the purposes of this Competition, the Contracting Authority does not accept any liability or provide any express or implied warranty in respect of any such information. Tenderers must form their own conclusions about the solution needed to meet the requirements set out in this RFT and may wish to consult their legal advisers.

2.1.2 The Contracting Authority does not bind itself to accept the lowest priced or any Tender.

This RFT does not constitute an offer or commitment to enter a Services Contract.

No contractual rights in relation to the Contracting Authority will exist unless and until a formal written Services Contract has been executed by or on behalf of the Contracting Authority.

Any notification of preferred bidder status by the Contracting Authority shall not give rise to any enforceable rights by the Tenderer.

The Contracting Authority may cancel this Competition (or, for the avoidance of doubt, any individual Lot) at any time prior to a formal written Services Contract being executed by or on behalf of the Contracting Authority.

The award of a Services Contract does not confer exclusivity on the successful Tenderer.

2.1.3 This RFT supersedes and replaces any and all previous documentation, communications and correspondence between the Contracting Authority and Tenderers, and Tenderers should place no reliance on such previous documentation and correspondence.

2.1.4 In this clause 2.1.4, “Data Protection Laws” means all applicable national and EU data protection laws, regulations and guidelines including but not limited to Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the “General Data Protection Regulation”), and any guidelines and codes of practice issued by the Office of the Data Protection Commission or other supervisory authority for data protection in Ireland from time to time.

The Contracting Authority will be a Data Controller (where Data Controller has the meaning given under the Data Protection Laws) in respect of any Personal Data (where Personal Data has the meaning given under the Data Protection Laws) required to be provided by the Tenderer in response to this RFT.

The Tenderer, as Data Controller in respect of any Personal Data provided by it in its Tender, is required to confirm in the statement required under paragraph 2.4 below that all Data Subjects (where Data Subject has the meaning given under the Data Protection Laws) whose Personal Data is provided by the Tenderer have consented to the processing of such Personal Data by the Tenderer, the Contracting Authority, the Evaluation Team and the supplier of the etenders.gov.ie website, for the purposes of the participation of the Tenderer in this Competition or that the Tenderer otherwise has a legal basis for providing

such Personal Data to the Contracting Authority for the purposes of its participation in this Competition .

- 2.1.5** The Contracting Authority would refer Tenderers in particular to the provisions of Regulation (EU) 2022/1031 on the access of third country economic operators, goods and services to the Union's public procurement and concession markets and procedures supporting negotiations on access of Union economic operators, goods and services to the public procurement and concession markets of third countries (International Procurement Instrument – IPI), and to their obligations to comply therewith.

In particular, tenderers and candidates should note Article 6 of the Regulation (EU) 2022/1031, the obligations for a Contracting Authority in the context of a procurement procedure where the EU Commission has adopted an IPI measure.

2.2 COMPLIANT TENDERS

- 2.2.1** If a Tenderer fails to comply in any respect with the requirements of this paragraph 2.2.1, the Contracting Authority reserves the right to reject the Tenderer's Tender as non-compliant or, without prejudice to this right and subject to its obligations at law, to take any other action it considers appropriate including but not limited to:

- seeking written clarification from the Tenderer;
- seeking further information from the Tenderer; or
- waiving a requirement, which in the Contracting Authority's view, is non-material or procedural.

Tenderers are required:

- (a) To complete and submit with their Tender the European Single Procurement Document ("[ESPD](#)"), which is available at Appendix 7 of the RFT. Tenderers may submit an ESPD which has already been used in a previous procurement procedure PROVIDED THAT they confirm that: (i) the information contained in it continues to be correct and (ii) that they satisfy the Selection Criteria for this Competition as set out at part 3.2 below;
- (b) To submit all documentation which this RFT requires to be submitted with their Tender;
- (c) To follow the format of this RFT and respond to each element in the order as set out in this RFT;
- (d) To conform to and comply with all instructions and requirements set out in this RFT;
- (e) To submit the statement required under paragraph 2.4 below; and
- (f) Not to alter or edit this RFT in any way.
- (g) Tenderers are required to complete and submit the Tender Response Document (TRD) at Appendix 8 in the format provided. Tenderers must complete and submit a separate TRD for each lot for which they wish to tender. Each TRD must be complete in its own right. Failure to complete the TRD as instructed will result in the tender being considered non-compliant.

- 2.2.2** Without prejudice to the generality of paragraphs 2.2.1, failure to comply with paragraphs 2.6.1, 2.6.2 or 2.6.3 below will render the Tender non-compliant and it will be rejected.

2.3 SERVICES CONTRACT

- 2.3.1** Tenderers should note the terms and conditions of the Services Contract at Appendix 5 to this RFT.
- 2.3.2** Tenderers are required to confirm their acceptance of the terms and conditions of the Services Contract by signing the Tenderer's Statement at Appendix 3. Tenderers may not amend the Services Contract.

2.4 ACCEPTANCE OF RFT REQUIREMENTS

Each Tenderer is required to accept the provisions of this RFT. ALL TENDERERS MUST RETURN, with their Tender, a scanned signed copy of the Tenderer's Statement, as set out in Appendix 3, printed on the Tenderer's letterhead. The Contracting Authority must be able to read the scanned signature of the Tenderer. If possible, please sign documents using blue ink. If the Contracting Authority cannot read the scanned signature, Tenderers may be requested to re-submit. Tenderers may not amend the Tenderer's Statement.

2.5 CONSORTIA AND PRIME / SUBCONTRACTORS

Where a group of undertakings (in whatever form and regardless of the legal relationship between them) come together to submit a Tender in response to this RFT, the Contracting Authority will deal with all matters relating to this Competition through a single nominated entity authorised to represent all members of the group of undertakings. The Tenderer must provide details of all members of the group of undertakings and their role in the Tender and clearly set out the contact details including name, title, telephone number, postal address, facsimile number and e-mail address of the nominated entity authorised to represent the Tenderer and to whom all communications shall be directed and accepted until this Competition has been completed or terminated. Correspondence from any other person will NOT be accepted, acknowledged or responded to.

Prior to and as a condition of award of any Services Contract, the successful Tenderer shall be required to designate a single entity who will carry overall responsibility for the Services Contract (the "Prime Contractor"), irrespective of whether or not tasks are to be performed by a subcontractor or other consortium member (the "Subcontractor").

2.6 TENDER SUBMISSION REQUIREMENTS

- 2.6.1** Tenders must be submitted via the 'electronic tenderbox' available on www.etenders.gov.ie. Only Tenders submitted to the electronic tenderbox will be accepted. Tenders submitted by any other means (including but not limited to: by email, fax, post, hand delivery, etc.) will NOT be accepted.

Tenderers must ensure that they give themselves sufficient time to upload and submit all required tender documentation in their Tender before the Tender Deadline (as defined in paragraph 2.6.2). Tenderers should take into account the fact that upload speeds vary.

Tenderers must note that in the electronic tenderbox, there is a file size limit of 250MB for each single file uploaded, with a maximum total limit of 2GB for all documentation (combined) in the Tender submitted.

In order to submit a Tender to the electronic tenderbox, Tenderers must ensure that they follow the necessary steps on the eTenders platform to ensure that their tender has been submitted properly, which includes ensuring that the “Submit” button has been clicked.

In the event that Tenderers need to modify or change any aspect of their Tender before the Tender Deadline, the Tender in its entirety will need to be re-submitted. Tenderers should be aware that the “Submit” button will be disabled automatically at the Tender Deadline.

- 2.6.2 Tenders must be received not later than 13:00 hrs (Irish time) on Friday 16 October 2026 (the “Tender Deadline”). Tenders that are received late WILL NOT be considered in this Competition.
- 2.6.3 Tenders must be submitted in English.
- 2.6.4 Subject to paragraph 2.14 and 2.18, each Tenderer is limited to submitting one Tender in its own capacity and one Tender as part of a consortium/group of undertakings under this RFT for each Lot.
- 2.6.5 All Tender Response Documents submitted in soft copy must be compiled such that they can be read immediately using Adobe Acrobat Reader (PDF Format). All Pricing Schedules must be submitted in Excel format. The Contracting Authority is not responsible for corruption in electronic documents. Tenderers must ensure electronic documents are not corrupt.

2.7 QUERIES AND CLARIFICATIONS

- 2.7.1 All queries relating to any aspect of this Competition or of this RFT must be directed to the messaging facility on www.etenders.gov.ie. Queries will be accepted no later than 13:00 hrs (Irish time) on Friday 2 October 2026 unless otherwise published by the Contracting Authority. For the avoidance of doubt, Tenderers may not contact the Contracting Authority directly regarding any aspect of this Competition.
- 2.7.2 All responses to queries will be issued by the Contracting Authority via the messaging facility on www.etenders.gov.ie. Where appropriate, queries may be amalgamated. Tenderers should note that the Contracting Authority will not respond to individual Tenderers privately.
- 2.7.3 The Contracting Authority reserves the right to issue or seek written clarifications.
- 2.7.4 The Contracting Authority reserves the right at any time before the Tender Deadline, to update or amend the information contained in this document and/or to extend the Tender Deadline. Participating Tenderers will be informed of any such amendment or extension through the eTenders website.
- 2.7.5 Tenderers should ensure that they register their interest in this Competition, by clicking on the “Accept” button on www.etenders.gov.ie, in order to receive all responses to queries and other updates in relation to this Competition.

2.8 TENDERING COSTS

- 2.8.1 All costs and expenses incurred by Tenderers relating to their participation in this Competition including, but not being limited to, site visits, field trials, demonstrations and/or presentations shall be borne by and are a matter for discharge by the Tenderers exclusively.

2.9 CONFIDENTIALITY

- 2.9.1 All documentation, data, statistics, drawings, information, patterns, samples or material disclosed or furnished by the Contracting Authority to Tenderers during the course of this Competition:
- (a) are furnished for the sole purpose of replying to this RFT only;
 - (b) may not be used, communicated, reproduced or published for any other purpose without the prior written permission of the Contracting Authority;
 - (c) shall be treated as confidential by the Tenderer and by any third parties (including subcontractors) engaged or consulted by the Tenderer; and
 - (d) must be returned immediately to the Contracting Authority upon cancellation or completion of this Competition if so requested by the Contracting Authority.

2.10 PRICING

- 2.10.1 All Tenderers must complete the Pricing Schedule at Appendix 2 to this RFT.
- 2.10.2 All prices quoted must be all-inclusive (i.e. including but not being limited to shipping, packaging, delivery, ancillary costs and all other costs/expenses), be expressed in Euro only and exclusive of VAT. The VAT rate(s) where applicable should be indicated separately.
- 2.10.3 Tenderers must confirm that all prices quoted in the Tender will remain valid for 90 days commencing from the Tender Deadline.
- 2.10.4 Any currency variations occurring over the term of the Services Contract shall be borne by the Tenderer.
- 2.10.5 Payments for Services provided pursuant to this RFT shall be subject to and made in accordance with the Services Contract at Appendix 5 to this RFT.
- 2.10.6 Tenderers should note that prices may be increased or decreased only on the first anniversary of the Effective Date of the Services Contract (as defined in the Services Contract) and on subsequent anniversaries of the Effective Date thereafter, and then only by the percentage by which the Services Producer Price Index has increased or decreased in the edition of that index published by the Central Statistics Office most recently prior to that anniversary.
- 2.10.7 Notwithstanding the price adjustment provisions set out above in Clause 2.10.6, before exercising any extension option, the Contracting Authority reserves the right to benchmark the Contractor's rates against prevailing market rates for comparable ICT technical support services. Where the benchmarking exercise indicates that the Contractor's rates are no longer competitive in comparison with prevailing market rates, the Contracting Authority

may invite the Contractor to enter into discussions with a view to agreeing revised rates for the extension period. Where agreement cannot be reached, the Contracting Authority reserves the right not to exercise the relevant extension option.

For the avoidance of doubt, where revised rates are agreed under this benchmarking provision, no index-linked price adjustment under 2.10.6 shall apply to the contract rates for the commencement of that specific extension period.

Any agreed revisions to the contract rates shall apply only from the commencement of the relevant extension period and shall be reflected in a written contract variation.

2.11 ENVIRONMENTAL, SOCIAL AND LABOUR LAW

- 2.11.1** In the performance of any Services Contract awarded, the successful Tenderers and their Subcontractors (if any), shall be required to comply with all applicable obligations in the field of environmental, social and labour law that apply at the place where the services are provided, that have been established by EU law, national law, collective agreements or by international, environmental, social and labour law listed in Schedule 7 of the Regulations.
- 2.11.2** Tenderers shall be required to include an undertaking to comply fully with the provisions of Council Directive 2001/23/EC of 12 March 2001 on the approximation of the laws of the Member States relating to the safeguarding of employees' rights in the event of transfers of undertakings, business or parts of undertakings or business and as implemented in Irish law by Statutory Instrument No. 131 of 2003, the European Communities (Protection of Employees on Transfer of Undertakings) Regulations 2003 and to indemnify the Contracting Authority for any claim arising or loss or costs incurred as a result of its failure or incapacity to fulfil its obligations under the said Directive and Statutory Instrument.
- 2.11.3** The Protection of Employees (Temporary Agency Work) Act 2012 (the "2012 Act") provides that an Agency Worker (as defined in the 2012 Act) is entitled to the same basic working and employment conditions as those which apply to employees recruited directly by the Hirer (as defined in the 2012 Act) to do the same or a similar job. Where the provision of the Services will involve the provision to the Contracting Authority of Agency Workers (within the meaning of the 2012 Act), Tenderers should ensure that they consider their obligations under the 2012 Act when pricing their Tender. The Contracting Authority shall have no liability for any increase in salaries that may be payable as a result of the application of the 2012 Act to the provision of the Services.

2.12 PUBLICITY

No publicity regarding this Competition or any Services Contract pursuant to this Competition is permitted unless and until the Contracting Authority has given its prior written consent to the relevant communication.

2.13 REGISTRABLE INTEREST

Any Registrable Interest involving any Tenderer or Subcontractor and the Contracting Authority, members of the Government, members of the Oireachtas, or employees and officers of the Contracting Authority and their relatives must be fully disclosed in the Tender or, in the event of this information only coming to the notice of the Tenderer or Subcontractor after the submission of a

Tender, must be communicated to the Contracting Authority immediately upon such information becoming known to the Tenderer or Subcontractor.

The terms “Registrable Interest” and “Relative” shall be interpreted as per Section 2 of the Ethics in Public Office Acts 1995 and 2001, copies of which are available at www.irishstatutebook.ie. The Contracting Authority will, at its absolute discretion, decide on the appropriate course of action, which may in appropriate circumstances include eliminating a Tenderer from this Competition or terminating any Services Contract entered into by a Tenderer.

2.14 ANTI-COMPETITIVE CONDUCT

Tenderers’ attention is drawn to the Competition Act 2002 (as amended, the “2002 Act”). The 2002 Act makes it a criminal offence for Tenderers to collude on prices or terms in a public procurement competition.

2.15 INDUSTRY TERMS USED IN THIS RFT

Where reference is made to a particular item, source, process, trademark, or type in this RFT then all such references are to be given the meaning generally understood in the relevant industry and operational environment.

2.16 FREEDOM OF INFORMATION

- 2.16.1** Tenderers should be aware that, under the Freedom of Information Act 2014 and the European Communities (Access to Information on the Environment) Regulations 2007 to 2014, information provided by them during this Competition may be liable to be disclosed.
- 2.16.2** Tenderers are asked to consider if any of the information supplied by them in their Tender should not be disclosed because of its confidentiality or commercial sensitivity. If Tenderers consider that certain information is not to be disclosed because of its confidentiality or commercial sensitivity, Tenderers must, when providing such information, clearly identify the specific sections of their Tender containing such information and specify the reasons for its confidentiality or commercial sensitivity. For the avoidance of doubt Tenderers may not assert confidentiality or commercial sensitivity over the entire Tender but must clearly identify the specific section containing such information. If Tenderers do not identify information as confidential or commercially sensitive, it is liable to be released in response to a request under the above legislation without further notice to or consultation with the Tenderer. The Contracting Authority will, where possible, consult with Tenderers about confidential or commercially sensitive information so identified before making its decision on a request received. The Contracting Authority accepts no liability whatsoever in respect of any information provided which is subsequently released (irrespective of notification) or in respect of any consequential damage suffered as a result of such obligations.

2.17 TAX CLEARANCE

It will be a condition of any Services Contract pursuant to this Competition that the successful Tenderer(s) shall, for the term of such contract(s), comply with all applicable EU and domestic tax laws. Tenderers are referred to www.revenue.ie for further information. Prior to the award of any Services Contract arising out of this Competition the successful Tenderer shall be required to supply its Tax Clearance Access Number and Tax Reference Number to facilitate online verification of their tax status by the Contracting Authority. By supplying these numbers the successful Tenderer acknowledges and agrees that the Contracting Authority has the permission of the successful Tenderer to verify its tax cleared position online.

2.18 CONFLICTS OF INTEREST

Any conflict of interest or potential conflict of interest on the part of a Tenderer, Subcontractor or individual employee(s) or agent(s) of a Tenderer or Subcontractor(s) must be fully disclosed to the Contracting Authority as soon as the conflict or potential conflict is or becomes apparent. Tenderers are required to declare that the preparation of their Tender was carried out independently. In the event of any actual or potential conflict of interest, the Contracting Authority may invite Tenderers to propose means by which the conflict of interest might be removed and in circumstances where there are links between Tenderers, the Contracting Authority may seek further information to confirm the Tenders have been prepared independently. The Contracting Authority will, at its absolute discretion, decide on the appropriate course of action, which may in appropriate circumstances include eliminating a Tenderer from this Competition or any Mini-Competition or terminating any Framework Agreement or Services Contract entered into by a Tenderer.

2.19 WITHDRAWAL FROM THIS COMPETITION

Tenderers are required to notify the Contracting Authority immediately via the e-tenders website, if at any stage they decide to withdraw from this Competition.

2.20 SITE VISIT

2.20.1 Not Used

2.20.2 Not Used

2.21 INSURANCE

- 2.21.1 The successful Tenderer shall be required to hold for the term of the Services Contract the following insurances:

TYPE OF INSURANCE	INDEMNITY LIMIT
Employer's Liability	€13 million Limit for any one claim or series of claims arising out of a single occurrence, per insurance year.
Public Liability	€6.5 million Limit for any one claim or series of claims arising out of a single occurrence, per insurance year.
Product Liability	Not applicable.
Professional Indemnity	€1 million Limit on aggregated no. of claims per insurance year.
Cyber Insurance	€1 million Limit on aggregated no. of claims per insurance year.

- 2.21.2 By signing the Tenderer's Statement at Appendix 3, Tenderers confirm that, if awarded a Services Contract under this Competition, (i) they will, from the Effective Date of the Services Contract (as defined in the Services Contract), obtain and hold the types and levels of insurance as specified at paragraph 2.21.1, (ii) the territorial limits and jurisdiction of its insurance policies include Ireland and (iii) they are not aware of any exclusions, restrictions, conditions or warranties or, in the case of policies with an aggregate limit of indemnity, any outstanding claims, which could have a material adverse impact on the level of coverage specified above. A formal confirmation from the Tenderer's insurance company or broker to this effect will be requested from the successful Tenderer(s) prior to the award of (and shall be a condition of) any Services Contract.

- 2.21.3 The successful Tenderer will, during the term of the Services Contract, be required to:

- (a) immediately advise the Contracting Authority of any material change to its insured status;
- (b) produce proof of current premiums paid upon request;
- (c) produce valid certificates of insurance upon request.

Part 3: Selection and Award Criteria

3.1 COMPLIANT TENDERS

3.1 Only those Tenderers who have:-

- (a) Submitted compliant Tenders pursuant to paragraph 2.2 above, and
- (b) Declared by way of ESPD that either:
 - (i) no mandatory grounds for exclusion of the Tenderer pursuant to Regulation 57 of the Regulations apply to them, or
 - (ii) in circumstances where any mandatory exclusion grounds apply to the Tenderer (and where the Tenderer is not precluded from doing so under Regulation 57(17) of the Regulations), that it can provide evidence to the effect that measures taken by it are sufficient to demonstrate its reliability despite the existence of any such relevant exclusion ground, and
- (c) Declared by way of ESPD that they satisfy the selection criteria for each Lot applied for in this Competition as set out in part 3.2 below (the “Selection Criteria”), will be evaluated in accordance with the Award Criteria at part 3.3 below.

However, please note that the Contracting Authority also reserves the right to exclude from evaluation a Tenderer to whom a discretionary ground for exclusion pursuant to Regulation 57 of the Regulations applies.

Tenderers should note that where a Tenderer is relying on the capacity of other entities (for example, Subcontractors) for the purposes of fulfilling any of the Selection Criteria in part 3.2 below it must ensure that each such entity:

- (i) completes and submits a separate ESPD in respect of each such entity, and
- (ii) when requested by the Contracting Authority, submit proof, to the satisfaction of the Contracting Authority, that each such entity will place the necessary resources at the disposal of the Tenderer.

The Contracting Authority may decide to examine Tenders before verifying the absence of exclusion grounds in Regulation 57 of the Regulations (the “Exclusion Grounds”) and the fulfilment of the Selection Criteria.

However, notwithstanding anything to the contrary in this part 3.1, the Contracting Authority reserves the right to ask Tenderers at any moment during the Competition to submit any or all of the following for the purposes of verification of the status of the Tenderer (including the Prime Contractor and any Subcontractor):

- (i) a Declaration in the form attached at Appendix 4;
- (ii) evidence to the effect that measures taken by the entity concerned are sufficient to demonstrate its reliability despite the existence of a relevant Exclusion Ground; and
- (iii) in the case of the Prime Contractor and any Subcontractor on whose capacity the Prime Contractor relies, all or any of the supporting documents specified at paragraph 3.2 below.

- (iv) Information concerning the Tenderer, and any Subcontractors, for the purposes of Regulation (EU) No 833/2014 (as amended by EU Regulation 2022/576 or any subsequent amendments to same) including but not limited to, in respect of natural persons, copies of identity documents and, in respect of legal persons, a certificate or extract from the commercial register or other competent authority of the country in which the legal person is established

and

- (v) Information concerning the origin of goods, if any, for the purposes of assessing compliance with Regulation (EU) No 833/2014 (as amended by EU Regulation 2022/576 or any subsequent amendments to same).

If a Tenderer does not, upon request by the Contracting Authority, provide evidence which is considered by the Contracting Authority as sufficient to demonstrate (i) its fulfilment of the Selection Criteria (or any one of them) in accordance with this RFT and (ii) the absence of Exclusion Grounds, or its reliability despite the existence of a relevant Exclusion Ground, and (iii) that it does not come within the category of prohibited economic operators identified in Regulation (EU) No 833/2014 of 31 July 2014 (as amended by EU Regulation 2022/576 or any subsequent amendments to same) and (iv) that its origin of goods, if any, are not subject to the prohibitions set out in Regulation (EU) No 833/2014 of 31 July 2014 (as amended by EU Regulation 2022/576 or any subsequent amendments to same) then it shall be excluded from further participation in this Competition.

If a Tenderer does not, upon request by the Contracting Authority, provide evidence which is considered by the Contracting Authority as sufficient to demonstrate (i) the fulfilment by any Subcontractor on whose capacity the Prime Contractor relies of the Selection Criteria (or any one of them) in accordance with this RFT and (ii) the absence of Exclusion Grounds in respect of any Subcontractor, or the reliability of any Subcontractor despite the existence of a relevant Exclusion Ground and (iii) that any proposed Subcontractor on whose capacity the Tenderer relies (where the value of that subcontract exceeds 10% of the value of the Services Contract) does not come within the category of prohibited economic operators identified in Regulation (EU) No 833/2014 of 31 July 2014 (as amended by EU Regulation 2022/576 or any subsequent amendments to same) then, it shall be excluded from further participation in this Competition *unless* it replaces the Subcontractor with one which meets all relevant requirements of this RFT.

3.2 SELECTION CRITERIA

- 3.2 Tenderers will either pass OR fail each of the Selection Criteria in this part 3.2. A Tenderer who fails a selection criterion will be excluded from participating in this Competition. Tenderers must provide their responses using the Tender Response Document at Appendix 8.

3.2.A Economic and Financial Standing (Pass/Fail)

Tenderers must declare by way of ESPD that they satisfy the financial and economic standing requirement(s) set out below in respect of each Lot tendered for and that they are able, upon request and without delay, to provide the supporting documentation specified below to the Contracting Authority in each case.

Pass Requirement: Tenderers must declare, in Appendix 8, the Tender Response Document, information regarding their financial standing and viability.

Minimum Turnover Level Requirement - Lots 1, 2 & 3

The requirement is as follows:

- Tenderers must have an annual turnover of at least €600,000 (excl. VAT) in each of the last three (3) financial years.
- Where figures for the most recent financial year are not yet available, Tenderers may provide figures for the three most recently completed financial years for which accounts are available.
- Tenderers must complete the Economic and Financial Standing section of the Tender Response Document.

Note #1: In the case of an Applicant being a grouping, this condition may be satisfied by the group members as a whole, or by reliance on the lead Applicant. Where group members are relying on the lead Applicant's financial capacity, self-declaration / evidence will only be required of the lead.

Note #2: If the date of establishment of the Tenderer is more recent, the annual turnover must meet the turnover required as set out above for each year(s) the tenderer has been established (pro-rata for companies established within one year).

Note #3: Applicants are required to complete a Self-Declaration Form in the Tender Response Document. Applicants should note that, they may be required to provide evidence to demonstrate that they meet the minimum turnover requirement by way of an external auditor's statement or audited accounts for the corresponding years.

Note #4: Where the Tenderer is unable, for a valid reason, to provide the specified documentation, the Tenderer must inform the Contracting Authority of the reason why the documentation cannot be supplied and, if the Contracting Authority considers the reason given to be valid, provide such other suitable alternative documentation to prove, to the satisfaction of the Contracting Authority, their economic and financial capacity.

Tenderers must provide the supporting documentation specified above without delay when requested by the Contracting Authority.

Economic and Financial Standing is a 'pass or fail' criterion. Tenderers that do not meet the above criterion will be eliminated from the Competition.

3.2.B Technical and Professional Ability (Pass/Fail)

Experience and References

Tenderers must demonstrate substantial experience in delivering ICT services of comparable technical complexity and operational importance to those required by the Department.

For each lot tendered for, the Tenderer must provide a minimum of one (1) and a maximum of three (3) contract examples relevant to that lot and relating to services delivered within the last five (5) years. The same contract example may be used for more than one lot where it demonstrates experience relevant to that lot.

Minimum Requirement (Pass/Fail)

To satisfy this criterion, at least one of the contract examples submitted for the relevant Lot must demonstrate successful delivery of ICT services of comparable technical complexity and operational importance to the services required under that Lot.

Failure to provide at least one (1) contract example satisfying this minimum requirement will result in the Tenderer failing this selection criterion in respect of the relevant Lot.

For each contract example, Tenderers must provide the information specified in the TRD:

- Client organisation details,
- A summary of the relevant contract, including scope, scale, duration, technologies covered,
- The number and types of resources supplied, and services delivered,
- Sufficient information to demonstrate the relevance of the example to the requirements of the Lot, and,
- A named referee, including email address and telephone number, who can verify the information provided and satisfactory delivery of the services.

The Contracting Authority reserves the right to contact referees directly to verify the information provided.

3.2.C Environmental and Sustainability (Pass/Fail)

As part of the All of Government Plan on [Climate Action 2025](#) and giving regard to [Circular 17/2025](#), all Government Departments are seeking to reduce the environmental impact of the goods and services that they procure. The Department of Foreign Affairs and Trade is committed to sustainability and to working in an environment-friendly way, supporting national and global efforts to reduce carbon emissions and to promote sustainability.

The impact to the environment is a key consideration for the Department. As such all services must be completed in a sustainable manner with due consideration given to minimising the environmental impact.

Where indicated in the TRD, Tenderers must demonstrate that they have documented environmental management arrangements in place and provide details of the measures and practices used to implement and monitor these arrangements. Evidence may include certification to ISO14001 or equivalent, or other documented environmental management measures appropriate to the nature and size of the organisation.

Minimum Requirement (Pass/Fail)

To satisfy this criterion, Tenderers must demonstrate that they have documented environmental management arrangements in place and provide details of the measures and practices used to implement and monitor these arrangements. Evidence may include certification to ISO14001 or equivalent, or other documented environmental management measures appropriate to the nature and size of the organisation.

3.3 Award Criteria

3.3.1 The Services Contract will be awarded based on the most economically advantageous tender(s) as identified in accordance with the following criteria:

Note #1: Qualifying tenders will be evaluated in each Lot with a maximum of 1000 points allocated.

Note #2: Tenderers must achieve the minimum points specified in the table below for each scored criterion.

In addition:

- (a) tenderers must achieve the minimum score specified for each role in Sections 3.3.1.1 to 3.3.1.3; and
- (b) tenderers must achieve the overall minimum score specified for the Quality of Proposed Team of Resources criterion.

Failure to satisfy either requirement shall result in the Tender being excluded from further evaluation for the relevant lot.

CRITERION	WEIGHTING	AVAILABLE POINTS	MINIMUM POINTS REQUIRED
Qualitative (700 points)			
Quality of the proposed Team of Resources	60%	600	360
Quality of Resource Management proposal	10%	100	60
Financial (300 points)			
Overall Cost	30%	300	N/A
Total	100%	1000	N/A

Quality of Proposed Team of Resources (600 Points)

The evaluation of the proposed team of resources shall be undertaken on a role-by-role basis. Each proposed resource will be assessed against the relevant role profile contained in Appendix 1 and scored in accordance with the evaluation criteria applicable to that role category using the standard scoring methodology for qualitative criteria set out below. The weighted scores for all roles will be aggregated to determine the total quality score for the relevant lot.

Assessment will focus on:

1. Demonstrated relevant experience;
2. Depth of technical expertise;
3. Experience delivering services in comparable enterprise environments;
4. Operational support and service delivery capability;
5. Problem-solving and troubleshooting capability;

6. Governance, documentation and stakeholder engagement capability.

Professional certifications will not be separately scored but may be considered by the Evaluation Panel as supporting evidence of a Tenderer's demonstrated experience and technical expertise.

Scoring Methodology for Qualitative Criteria

SCORE	MEANING	INTERPRETATION
90% - 100%	Excellent	An excellent response demonstrating excellent understanding, offering assurance. Strongly supported tender.
80% - 89%	Very Good	A very good response demonstrating very good understanding, offering assurance. Fully supported tender.
70% - 79%	Good	A good response demonstrating good understanding, offering assurance. Well supported tender.
60% - 69%	Satisfactory	An acceptable response demonstrating a minimum understanding, offering assurance. Satisfactorily supported tender.
Less than 60%	Unacceptable	Response demonstrates limited understanding with limited or insufficient or no detail with a risk of non-delivery.

3.3.1.1 Lot 1 – Networks and Communications Team

ROLE	AVAILABLE POINTS	MINIMUM POINTS REQUIRED
Network Architect (Enterprise & Communications Infrastructure) – Senior Level	120	72
Network Security Architect (Enterprise Security Infrastructure) – Senior Level	120	72
Network Security Engineer (Enterprise Security Infrastructure) – Senior Level	90	54
Network VoIP / Webex Engineer (Enterprise & Communications Infrastructure) – Intermediate Level	75	45
Network VoIP / Webex Engineer (Enterprise & Communications Infrastructure) – Intermediate Level	75	45
Network Security Engineer (Enterprise Security Infrastructure) – Intermediate Level	75	45

Network Engineer (Enterprise & Communications Infrastructure) – Junior Level	45	27
Total	600	

3.3.1.2 Lot 2 – Infrastructure Team

ROLE	AVAILABLE POINTS	MINIMUM POINTS REQUIRED
Enterprise Infrastructure Architect – Senior Level	120	72
ICT Infrastructure Engineer (SQL Server Design & DBA) – Senior Level	60	36
ICT Infrastructure Engineer (Enterprise Services & Linux) – Senior Level	55	33
ICT Infrastructure Engineer (Microsoft Cloud & Power Platform) – Senior Level	55	33
ICT Infrastructure Engineer (Microsoft Cloud & Power Platform) – Senior Level	55	33
ICT Infrastructure Engineer (SCCM Endpoint Configuration Manager) – Senior Level	55	33
ICT Infrastructure Engineer (Microsoft Hybrid Cloud & Enterprise Services) – Senior Level	55	33
ICT Infrastructure Engineer (Microsoft Hybrid Cloud & Enterprise Services) – Senior Level	55	33
ICT Infrastructure Engineer (Microsoft Hybrid Cloud & Enterprise Services) – Intermediate Level	45	27
ICT Infrastructure Engineer (Microsoft Hybrid Cloud & Enterprise Services) – Intermediate Level	45	27
Total	600	

3.3.1.3 Lot 3 – SharePoint Team

ROLE	AVAILABLE POINTS	MINIMUM POINTS REQUIRED
SharePoint Programme Manager – Senior Level	120	72
SharePoint Technical Project Manager – Senior Level	110	66
SharePoint Infrastructure Engineer – Senior Level	85	51

SharePoint Solutions Designer (Forms & Business Solutions) – Senior Level	85	51
Power Platform Developer – Senior Level	85	51
SharePoint Testing & Quality Assurance Specialist – Intermediate Level	70	42
SharePoint Administrator – Junior Level	45	27
Total	600	

3.3.1.4 Resource Assessment Methodology

Architect, Programme Manager and Project Manager roles shall be evaluated against the following criteria:

CRITERION	WEIGHTING
Relevant Experience in Comparable Enterprise Environments	30%
Technical Expertise and Depth of Knowledge	25%
Delivery of Enterprise-Scale Solutions / Programmes	20%
Problem Solving and Decision-Making Capability	10%
Governance, Risk Management and Operational Assurance	7.5%
Stakeholder Engagement, Communication and Documentation	7.5%

Senior Engineer, Developer and Solutions Designer roles shall be evaluated against the following criteria:

CRITERION	WEIGHTING
Relevant Experience in Comparable Enterprise Environments	30%
Technical Expertise and Depth of Knowledge	30%
Enterprise Service Delivery and Operational Support Capability	20%
Troubleshooting, Analysis and Problem Resolution	10%
Governance, Documentation and Operational Discipline	5%
Communication and Stakeholder Engagement	5%

Intermediate Engineer and Specialist roles shall be evaluated against the following criteria:

CRITERION	WEIGHTING
Relevant Experience in Comparable Enterprise Environments	30%
Technical Expertise	30%
Operational Support Capability	20%
Troubleshooting and Incident Resolution	10%
Documentation and Operational Discipline	5%
Communication and Stakeholder Engagement	5%

Junior Engineer and Administrator roles shall be evaluated against the following criteria:

CRITERION	WEIGHTING
Relevant Experience	30%
Technical Knowledge and Understanding	30%
Exposure to Enterprise Environments	20%
Troubleshooting and Analytical Capability	10%
Communication, Teamwork and Customer Service	10%

3.3.1.5 Minimum Resource Threshold

Each proposed resource must achieve a minimum score of 60% of the points available for that role.

Failure of any proposed resource to achieve the minimum score specified for that role will result in the Tender being excluded from further evaluation, irrespective of the overall score achieved for the Quality of Proposed Team of Resources criterion.

3.3.1.6 Quality of Resource Management Proposal (100 Points)

The resource management proposal will be evaluated against the criteria set out below using the scoring methodology for qualitative criteria set out at 3.3.1 of this RFT. The marks awarded for each criterion will be aggregated to produce a total score out of 100 marks. Tenderers must achieve a minimum score of 60 points out of the 100 available for the Quality of Resource Management Proposal criterion. Tenderers failing to achieve this minimum score will be excluded from further consideration.

CRITERION	AVAILABLE POINTS
Workforce Planning	25
Continuity Arrangements	25
Performance Management (including multi-lot capability where applicable)	20
Succession Planning	15
Knowledge Transfer	15
Total	100

3.3.2 Subject to paragraphs 2.1 (Important Notices) and 3.5 (Standstill Period) of this RFT, award of the Services Contract to the highest ranked Tenderer (as determined by paragraph 3.3.1) will be conditional upon:

- the Tenderer submitting the following evidence in respect of the Tenderer (including the Prime Contractor and any Subcontractors, as applicable in accordance with paragraph 3.1 above) to the extent not already provided, within seven (7) days of request by the Contracting Authority: (i) a Declaration in the form attached at Appendix 4; (ii) if applicable, evidence to the effect that measures taken by the entity concerned are sufficient to demonstrate its reliability despite the existence of a relevant Exclusion Ground; (iii) all or any of the supporting documents specified at paragraph 3.2; and
- the evidence specified at paragraph 3.3.2(a) above demonstrating that each entity concerned meets the Selection Criteria and the compliance requirements specified at paragraph 3.1 above.

3.3.3 Tenderers should note that the award criterion “Overall cost” will only be evaluated after any tenders which fail to reach any one or more of the minimum marks required are eliminated. Eliminated tenders will not be evaluated in relation to the criterion for “Overall cost”.

3.3.4 It should be noted that the Contracting Authority will use a standard formula to calculate the marks in respect of “Overall cost”, whereby maximum marks are awarded to the lowest priced tender and costs of the remaining tenders are expressed as a percentage of the lowest priced tender (Inverse Proportionality).

Cost Score	=	$\frac{\text{Lowest Tendered Pricing}}{\text{Tendered Pricing Under Evaluation}}$	x	$\frac{\text{Maximum Number of Marks Available}}{\text{Maximum Number of Marks Available}}$
-------------------	----------	---	----------	---

3.4 PRESENTATION OF PROPOSALS

Tenderers may be required to make a presentation of the proposal contained in their Tender. The Contracting Authority will not be responsible for the cost of such presentations (in accordance with paragraph 2.8). Performance at presentations will NOT be evaluated.

3.5 STANDSTILL PERIOD

- 3.5.1** In circumstances where the European Communities (Public Authorities' Contracts) (Review Procedures) Regulations 2010 (Statutory Instrument 130 of 2010), as amended by the European Communities (Public Authorities' Contracts) (Review Procedures) (Amendment) Regulations 2015 (Statutory Instrument 192 of 2015) and the European Communities (Public Authorities' Contracts (Review Procedures) (Amendment) Regulation 2017 (Statutory Instrument 327 of 2017) apply, no contract can or will be executed or take effect until at least fourteen (14) calendar days after the day on which the Tenderers have been sent a notice informing them of the result of this Competition (the "Standstill Period") if such notice is sent by electronic means. The Standstill Period shall be sixteen (16) calendar days if such notice is sent by other means. The preferred bidder will be notified of the decision of the Contracting Authority and of the expiry date of the Standstill Period.
- 3.5.2** Tenderers should note that the Contracting Authority may, when notifying Tenderers of the results of this Competition, include the scores obtained by the Tenderer concerned and the scores obtained by the preferred bidder in respect of each award criterion assessed by the Contracting Authority.

3.6 RETURN OF SIGNED CONTRACTS

- 3.6.1** The successful Tenderer must sign and return the Services Contract and the Confidentiality Agreement, both in duplicate, to the Contracting Authority no later than fifteen (15) calendar days from the date of expiry of the Standstill Period unless notified otherwise in writing by the Contracting Authority.
- 3.6.2** Not Used.

Appendix 1: Requirements and Specifications

Tenderers must address each of the issues and requirements in this part of the RFT and submit a detailed description in each case which demonstrates how these issues and requirements will be dealt with / met and their approach to the proposed delivery of the Services. A mere affirmative statement by the Tenderer that it can/will do so, or a reiteration of the tender requirements is NOT sufficient in this regard. Tenderers must respond to the requirements and specifications using the Tender Response document included in Appendix 8.

DEPARTMENT OVERVIEW

The Department of Foreign Affairs and Trade (DFAT) is responsible for promoting and protecting Ireland's interests, values, and citizens abroad. It leads foreign policy, manages diplomatic and consular relations, coordinates engagement with the European Union and international organisations, and delivers services such as passports and consular assistance. The Department operates under the direction of the Tánaiste and Minister for Foreign Affairs, supported by a global network of embassies and missions.

Core Responsibilities

DFAT's key functions include developing foreign and security policy; managing EU relations; representing Ireland in multilateral organisations; delivering passport and consular services; administering the Official Development Assistance programme (Irish Aid); supporting peace and reconciliation initiatives; and promoting Ireland's economic, cultural, and political interests internationally.

Organisation and Structure

The Department is led by the Secretary General, supported by a Management Board. Headquarters is based in Dublin, with a global network of approximately 100 diplomatic and consular missions. Operations are structured across functional and geographic divisions, including EU Affairs, Development Cooperation, Bilateral Relations, Political and Security Policy, Citizen Services, and Corporate Support functions (including ICT, HR, and Finance).

Operational Context and Challenges

DFAT operates in a complex, globally distributed environment requiring consistent support across headquarters and overseas missions with varying connectivity and time zones. The Department must meet stringent security, data protection, and sovereignty requirements aligned with government standards.

Information on the Department's strategy and guiding principles can be found at www.dfa.ie.

TEAM(S) OF RESOURCES

This RFT is for the provision of expert resources across three (3) distinct functions within the ICT Unit.

- Lot 1: Networks and Communications Team
- Lot 2: Infrastructure Team
- Lot 3: SharePoint Team

Tenderers may submit a tender for one, two or all three Lots. A separate Tender Response Form must be completed and submitted for each Lot tendered for.

All resources engaged under this RFT shall be assigned to the Department's ICT Unit and primarily based at its Dublin offices. Standard service delivery hours shall be Monday to Friday, 09:00–17:30.

Remote working may be facilitated; however, all resources must be available for and attend onsite in Dublin as required by the Department. Regular onsite attendance is a mandatory requirement of this engagement.

Provision must also be made for occasional service delivery outside standard working hours, as well as travel to other locations where necessary to fulfil the Services. All travel, subsistence and related expenses associated with the delivery of the services shall be included in the Tenderer's proposed rates and will not be separately reimbursed by the Contracting Authority. Rates for services delivered outside standard working hours must be clearly specified as per Appendix 2: Pricing Schedule.

Any requirement for services outside standard working hours shall be subject to prior agreement between the Department and the service provider.

Tenderers are required to provide:

- Profiles of all proposed personnel, demonstrating relevant and recent experience appropriate to the role for which they are proposed. Such experience must be verifiable and reflect an appropriate level of technical complexity and responsibility, evidencing competence in the required skillsets;
- References for each proposed resource. These may comprise one or more referees per individual, provided sufficient evidence of relevant prior experience is demonstrated.

The Department reserves the right to increase, decrease or vary the number and composition of resources engaged under any Lot during the term of this RFT in accordance with operational requirements, available funding, project demands, technology evolution, service transformation initiatives, and future business requirements.

Additional resources may be required to support emerging technologies, new projects, service enhancements, programme delivery requirements, cybersecurity initiatives, cloud adoption, digital transformation activities, or other ICT-related requirements falling within the scope of the relevant Lot.

=====

Lot 1: Networks and Communications Team

- 1 x Network Architect (Enterprise & Communications Infrastructure) - Senior Level
 - 1 x Network Security Architect (Enterprise Security Infrastructure) - Senior Level
 - 1 x Network Security Engineer (Enterprise Security Infrastructure) - Senior Level
 - 2 x Network VoIP Webex Engineer (Enterprise & Communications Infrastructure) - Intermediate Level
 - 1 x Network Security Engineer (Enterprise Security Infrastructure) - Intermediate Level
 - 1 x Network Engineer (Enterprise & Communications Infrastructure) - Junior Level
- =====

Job Title:

Network Architect (Enterprise & Communications Infrastructure) – Senior Level

Role Summary:

The Senior Network Architect (Enterprise & Communications Infrastructure) is responsible for the design, operation, and continuous evolution of the Department's global network and communications platforms. This role is focused on hands-on architectural leadership within complex, live enterprise environments, ensuring the stability, resilience, and performance of business-critical infrastructure while enabling controlled modernisation.

The successful candidate will demonstrate extensive professional experience and advanced hands-on expertise in designing, implementing, and operating large-scale network and IP telephony environments.

The Senior Network Architect will report to the Network Manager of the ICT Unit and support the coordination of Network Engineers. The role is responsible for assigning duties and tasks based on skills, experience, and project requirements. The Senior Network Architect will also act as Project Manager for major network and communications initiatives within the ICT function.

Core Responsibilities:

- Design, implement, and maintain complex enterprise network architectures across LAN, WAN, data centre, wireless, and unified communications environments.
- Take operational ownership of business-critical network and communications infrastructure, ensuring stability, performance, and service continuity.
- Analyse and safely modify live network environments with embedded dependencies, integrations, and legacy components, implementing controlled changes with minimal risk.
- Diagnose and resolve production issues, including routing instability, latency, service degradation, and telephony failures, identifying root causes and implementing permanent fixes.
- Support and optimise global network environments, ensuring high availability and performance across distributed sites.
- Design and support IP telephony and unified communications platforms, including integration with legacy telephony systems and modern collaboration tools.
- Assess and manage risks associated with architectural changes, coexistence of legacy and modern platforms, and partial redesign initiatives.
- Deliver incremental improvements where full redesign is not feasible, while supporting long-term modernisation strategies.

- Engage stakeholders to understand operational requirements, service constraints, and undocumented dependencies, translating these into robust technical solutions.
- Produce clear and structured architectural, operational, and handover documentation to ensure ongoing supportability and maintainability.

Role Requirements:

Experience

- Minimum 7+ years' demonstrable experience delivering enterprise-scale network and communications solutions within large, complex environments.
- Proven experience delivering and stabilising large-scale, business-critical network and communications environments.
- Proven experience resolving production issues in high-dependency environments, with clear root-cause analysis and stable remediation.
- Proven ability to engage with business and technical stakeholders to interpret requirements and constraints, particularly where environments are not fully documented.

Enterprise Networking & Architecture

- Extensive hands-on experience designing and supporting enterprise network architectures across routing, switching, and security domains.
- Advanced practical knowledge of network behaviour under load, failure conditions, and change in live environments.
- Experience implementing resilient and highly available network designs, including redundancy, failover, and traffic optimisation strategies.
- Strong capability in analysing complex network dependencies and ensuring safe modification of live systems.

Network Infrastructure & Technologies

- Advanced experience with Cisco enterprise networking technologies, including routers (2900, 4300, 8200/8300, ASR series) and switching platforms (Catalyst, Nexus).
- Experience with data centre networking, high-speed backbone infrastructure, and fibre technologies.
- Strong working knowledge of wireless infrastructure, including controller-based and cloud-managed (Meraki) environments.
- Practical experience with network monitoring, diagnostics, and performance optimisation tools.

IP Telephony & Unified Communications

- Extensive hands-on experience with Cisco Unified Communications platforms (CUCM), including clustered enterprise deployments.
- Experience supporting voice infrastructure in live environments, including call routing, signalling, and service reliability.
- Integration experience with Cisco Unity Connection, UCCX, and Webex Contact Centre.
- Experience working with mixed telephony environments, including interoperability with legacy systems (QSIG, FXO).

Networking, Security & Protocols

- Advanced troubleshooting capability across routing protocols (EIGRP, OSPF) and core networking technologies (TCP/IP, GRE, IPSec, VRRP).
- Strong understanding of network security controls, including segmentation, encryption (AES, MACsec), and access control mechanisms.

- Experience implementing authentication and network access solutions (802.1x, ISE, or equivalent).
- Practical understanding of network behaviour, limitations, and failure modes in complex environments.

Operational Excellence & Risk Management

- Strong judgement in assessing risks associated with network changes, particularly in interconnected and legacy environments.
- Ability to maintain service continuity while introducing controlled improvements or architectural changes.
- Experience working within structured change management and governance frameworks.

Stakeholder Engagement & Delivery

- Ability to deliver practical, working solutions in the absence of complete specifications.
- Strong documentation discipline, ensuring solutions remain maintainable and supportable by others.

Skills & Competencies:

- Sound judgement on when to retain, optimise, or redesign network components.
- Ability to make safe, controlled changes to live systems with minimal service impact.
- Strong analytical and troubleshooting capability in complex, multi-layered environments.
- Ability to work independently and deliver consistently in a high-responsibility, outcome-focused role.
- Structured and disciplined approach to documentation, governance, and operational handover.
- Strong communication and stakeholder engagement skills, with the ability to influence technical decisions and architectural direction.

Qualifications and Certifications:

Depth of demonstrable, hands-on experience is essential. Candidates must demonstrate strong practical capability in designing, implementing, supporting, maintaining, and optimising enterprise network and communications infrastructure across complex, large-scale environments.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for practical experience and a proven track record of delivering and supporting enterprise-scale network and communications solutions.

Desirable Certifications (including but not limited to):

- Cisco Certified Internetwork Expert (CCIE)
- Cisco CCNP Security or equivalent.
- Certifications in collaboration, voice, or network security technologies.

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, and proven delivery of enterprise-scale network and communications solutions, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

Network Security Architect (Enterprise Security & Infrastructure) – Senior Level

Role Summary:

The Senior Network Security Architect (Enterprise Security & Infrastructure) is responsible for the design, implementation, and continuous evolution of the Department's cybersecurity architecture across network, perimeter, and endpoint domains. This role combines strategic architectural leadership with deep hands-on engineering expertise in complex, live enterprise environments.

The successful candidate will demonstrate advanced subject matter expertise across multi-vendor security platforms (including Cisco, Check Point, and Elastic), as well as strong operational capability in securing large-scale global infrastructures. The role requires practical, hands-on involvement in designing, implementing, troubleshooting, and optimising security controls while ensuring resilience, performance, and rapid detection of threats.

Core Responsibilities:

- Own, define, and maintain enterprise security architecture standards, patterns, and reference designs, ensuring consistency, scalability, and alignment with organisational risk objectives.
- Design, implement, and maintain enterprise security architectures across network, perimeter, endpoint, and cloud-integrated environments.
- Engineer, deploy, and monitor security controls to protect systems, networks, and sensitive data against evolving threats.
- Define and translate system security requirements into scalable and resilient architectural solutions.
- Take operational ownership of enterprise security platforms, ensuring stability, performance, and rapid incident detection and response.
- Lead the configuration, optimisation, and troubleshooting of firewalls, VPNs, proxies, endpoint security, and authentication systems in live environments.
- Analyse and safely modify live security environments with complex dependencies, implementing controlled and low-risk changes.
- Develop and implement automation solutions and security tooling to improve operational efficiency and reduce repeatable tasks.
- Monitor security events and ensure rapid visibility and escalation of incidents, minimising organisational risk exposure.
- Develop and maintain standard operating procedures (SOPs), security protocols, and technical documentation.
- Provide technical leadership, mentoring, and guidance to engineering teams, ensuring adherence to best practices.
- Engage with stakeholders to understand business risks and operational requirements, translating them into effective security controls.
- Support audit, compliance, and governance initiatives through structured documentation and reporting.
- Engage with senior management, business owners, and external stakeholders, including the NCSC, on operational security matters.

Role Requirements:

Experience

- Minimum 7+ years' demonstrable experience in enterprise network security architecture and engineering in large, complex environments.
- Proven experience designing, implementing, and operating multi-layered security architectures in business-critical environments.
- Strong track record of hands-on troubleshooting and stabilising security infrastructure in live production environments.
- Proven expert-level experience in threat hunting and incident response within enterprise environments.
- Strong experience detecting, analysing, and responding to security incidents in real time.

Enterprise Security Architecture

- Extensive experience designing layered security architectures (defence-in-depth), including perimeter, internal segmentation, and endpoint protection.
- Strong understanding of security architecture principles, threat modelling, and risk-based design.
- Experience balancing legacy infrastructure constraints with modern security controls and frameworks.
- Experience working in environments with legacy and modern security technologies, ensuring safe coexistence and incremental improvement.

Security Technologies & Platforms

- Expert experience with Cisco ASA and Firepower.
- Hands-on implementation and support of Cisco VPN technologies.
- Strong routing and switching background (aligned to CCNP level or higher).
- Extensive hands-on experience with Check Point R8x Management, Firewalls, VPNs, and IPS.
- Expert knowledge of Check Point Gaia OS and security management.
- Extensive experience with Check Point Security Suite, including AntiBot, Application Control, and Intrusion Prevention Systems (IPS).
- Extensive experience with Check Point Endpoint Security.
- Expert experience creating and implementing stateful firewall policies and securely deploying site-to-site VPN architectures.

General Security Technologies

- Hands-on experience with SIEM and logging platforms (Elastic, Kibana, Logstash, Kafka), with strong capability in security data analytics.
- Expert experience designing, implementing, and managing resilient centralised logging solutions, including log parsing and transformation pipelines.
- Experience with secure email gateways.
- Experience with Cisco WSA web proxy and content filtering.
- Strong understanding of identity and authentication systems (OTP, PKI, or equivalent MFA technologies).
- Experience with load balancing technologies.
- In-depth knowledge of DNS (Windows DNS and BIND) and its security implications.
- Strong system administration capability across Linux and Windows operating systems.
- Experience securing and hardening operating systems and services.
- Expert experience installing, configuring, and managing endpoint security agents across enterprise environments.
- Knowledge of Machine Learning techniques applied to threat detection, anomaly analysis, and advanced incident response use cases.

- Experience building, hosting, integrating, and maintaining in-house security tools using Python.
- Experience evaluating, deploying, supporting, and maintaining Generative AI solutions for security monitoring, analysis, threat detection, and operational use cases.

Networking & Security Fundamentals

- Full working knowledge of Ethernet, TCP/IP, IPSec, VRRP, NAT, and network access control technologies.
- Expert understanding of application layer protocols including HTTP/S, SMTP, SSH, SIP, WebRTC, and RTMP.
- Comprehensive experience with encryption technologies across Layer 2 and Layer 3, including data confidentiality, integrity, and authentication.
- High-level experience deploying and managing routing and switching protocols including EIGRP, OSPF, BGP, Policy-Based Routing, Static Routing, Spanning Tree, VLAN tagging (802.1q), and link aggregation (802.3ad).
- Advanced troubleshooting across TCP/IP, VPNs, encryption, and secure communications protocols.
- Expert knowledge of running and analysing packet captures across multiple devices (Linux, Windows, Cisco, Check Point).
- Strong knowledge of firewall policies, segmentation, and secure network design.
- Deep understanding of threat vectors, vulnerabilities, and mitigation strategies.

Operational Excellence & Incident Response

- Experience working under pressure in high-impact environments with strict deadlines.
- Ability to perform root cause analysis and implement long-term corrective actions.
- Experience defending against advanced persistent threats and nation-state-level threat actors.
- Demonstrated hands-on incident response experience, including leading investigations, containment, eradication, recovery, and post-incident analysis for complex network security incidents in enterprise environments.
- High-level experience with vulnerability scanning platforms (Tenable SC, Nessus) and remediation processes.
- Experience with malware analysis and the generation of indicators of compromise (IOCs).
- High-level experience with packet analysis tools such as Wireshark, tcpdump, fw monitor, Packetbeat.
- High-level experience with scripting for automation and analysis (Bash, Python).
- Familiarity with red team tools and methodologies including Kali Linux, Metasploit, and Mimikatz.
- Experience working within structured network change management and configuration control frameworks.

Additional Infrastructure Experience

- High-level experience designing and supporting enterprise IP telephony solutions and deployments.
- Experience supporting IP-based communications and collaboration platforms.
- Experience installing, configuring, and managing enterprise-scale video conferencing solutions.

Stakeholder Engagement & Delivery

- Proven ability to engage with business and technical stakeholders to interpret requirements and constraints, particularly where environments are not fully documented.
- Ability to deliver practical, working solutions in the absence of complete specifications.
- Strong experience liaising with internal and external ICT auditors.
- Strong documentation discipline, ensuring solutions remain maintainable and supportable by others.

Skills & Competencies:

- Strong hands-on engineering capability combined with strategic architectural thinking.
- Excellent analytical and problem-solving skills in complex, multi-vendor environments.
- Ability to make safe, controlled changes in live systems with minimal disruption.
- Strong focus on security resilience, performance, and continuous improvement.
- Ability to work independently while providing technical leadership and direction.
- High level of attention to detail, documentation discipline, and governance adherence.
- Strong communication and stakeholder engagement skills, with the ability to influence technical and security decisions.

Qualifications and Certifications:

Depth of demonstrable, hands-on experience is essential. Candidates must demonstrate strong practical capability in designing, implementing, securing, and optimising complex enterprise security architectures and infrastructure services.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for practical experience and a proven track record of delivering and securing complex enterprise environments.

Desirable Certifications (including but not limited to):

- Cisco CCNP.
- Check Point CCSE (R8x).
- Vendor certifications in SIEM, endpoint protection, or proxy technologies.

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, and proven delivery of enterprise-scale security architecture and cybersecurity solutions, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

Network Security Engineer (Enterprise Security & Infrastructure) – Senior Level

Role Summary:

The Senior Network Security Engineer (Enterprise Security & Infrastructure) is responsible for the implementation, operation, and continuous improvement of the Department's cybersecurity controls across network, perimeter, endpoint, and hybrid cloud environments.

This role is primarily engineering-focused, requiring deep hands-on expertise in deploying, managing, and optimising complex security platforms within live enterprise environments. The successful candidate will work within established architectural frameworks to deliver secure, resilient, and high-performing solutions, while contributing to their evolution through operational insight and continuous improvement.

The position demands strong practical capability across multi-vendor security technologies (including Cisco and Check Point), with a focus on operational excellence, proactive threat detection, and rapid incident response.

Core Responsibilities:

- Deploy, configure, and maintain enterprise security controls across network, perimeter, endpoint, and cloud-integrated environments.
- Implement architectural designs and security standards into robust, scalable, and operational solutions.
- Own and operate enterprise security platforms, ensuring availability, performance, and resilience.
- Perform advanced troubleshooting and root cause analysis across security infrastructure in live production systems.
- Manage and optimise firewalls, VPNs, proxies, endpoint security solutions, and authentication systems.
- Execute safe, controlled changes in complex live environments, minimising risk and service disruption.
- Make informed technical decisions in complex environments, balancing security, operational risk, and service continuity.
- Monitor security events and alerts, ensuring timely detection, investigation, and escalation of incidents.
- Lead and support incident response activities, including containment, remediation, and post-incident analysis.
- Design, develop, and maintain automation scripts and tooling to enhance operational efficiency and reduce manual effort.
- Contribute to the continuous improvement of security controls, processes, and platform configurations.
- Produce and maintain high-quality technical documentation, including procedures, configurations, and runbooks.
- Collaborate with architects, engineers, and stakeholders to deliver secure solutions aligned with business requirements.
- Support audit, compliance, and governance activities through accurate documentation and evidence gathering.
- Provide technical guidance and mentoring to junior engineers and team members.

Role Requirements:

Experience

- Minimum 7+ years' experience in enterprise network and security engineering in complex environments.
- Proven experience implementing and operating enterprise-grade security controls in production environments.
- Demonstrated hands-on expertise in troubleshooting and stabilising security platforms under real-world conditions.
- Experience supporting security operations, incident response, and threat remediation activities within enterprise environments.

Enterprise Security Engineering

- Strong experience implementing layered security controls (defence-in-depth) across perimeter, internal networks, and endpoints.
- Ability to interpret and implement security architecture designs and standards.
- Practical experience working with both legacy and modern security technologies in evolving environments.

Security Technologies & Platforms

- Strong hands-on experience with Cisco ASA, Firepower, and VPN technologies.
- Hands-on experience with Check Point R8x Firewalls, VPN, and IPS.
- Hands-on experience with Check Point Gaia OS and security management.
- Experience supporting Check Point Threat Prevention technologies.
- Experience supporting Check Point Endpoint Connect.

General Security Technologies

- Experience with SIEM and logging platforms (e.g., Elastic, Kibana, Logstash, Kafka).
- Experience managing the Elastic Cloud Enterprise platform.
- Knowledge of secure email gateways.
- Experience supporting web proxy and content filtering solutions (e.g., Bluecoat ProxySG/CAS).
- Understanding of identity and authentication systems (e.g., MFA platforms).
- Familiarity with load balancers.
- Strong knowledge of DNS (Windows DNS, BIND) and associated security considerations.
- Solid system administration skills across Linux and Windows environments.
- Strong experience with network access controls in a large enterprise network.

Networking & Security Fundamentals

- Strong troubleshooting skills across TCP/IP, VPNs, and secure communication protocols.
- Good understanding of firewall policy design, segmentation, and secure network architecture.
- Awareness of common threat vectors, vulnerabilities, and mitigation techniques.

Operational Excellence & Incident Response

- Experience monitoring and responding to security events in real time.
- Ability to work effectively under pressure in high-impact production environments.
- Proven capability in root cause analysis and implementing corrective actions.
- Experience operating within change management and governance frameworks.
- Ability to work closely with the Network Security Architect and provide technical cover and continuity as required.

Additional Infrastructure Experience

- Experience supporting enterprise IP telephony solutions and deployments.
- Experience supporting IP-based communications and collaboration platforms.
- Experience installing, configuring, and managing enterprise-scale video conferencing solutions.
- Experience deploying and maintaining on-premise S3-compatible storage platforms (e.g. MinIO, SeaweedFS).

Stakeholder Engagement & Delivery

- Ability to work with technical teams and stakeholders to deliver secure, practical solutions.
- Comfortable working in environments with incomplete documentation or evolving requirements.
- Strong documentation skills ensuring operational supportability and knowledge sharing.

Skills & Competencies:

- Strong hands-on engineering focus with attention to detail.
- Excellent analytical and problem-solving skills in complex environments.
- Ability to implement and maintain secure systems in live production environments.
- Strong focus on operational stability, performance, and continuous improvement.
- Ability to work independently while contributing to team objectives.
- Effective communication and collaboration skills.

Qualifications & Certifications:

Depth of demonstrable, hands-on experience is essential. Candidates must demonstrate strong practical capability in implementing, supporting, securing, maintaining, and optimising enterprise security platforms and infrastructure services within complex environments.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for practical experience and a proven track record of delivering and securing complex enterprise environments.

Desirable Certifications (including but not limited to):

- Cisco CCNP Security.
- Check Point CCSE (R8x).
- Cisco Certified Specialist - Security Identity Management Implementation.

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, and proven implementation, support, and optimisation of enterprise-scale cybersecurity platforms and security services, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

Network VoIP / Webex Engineer (Enterprise & Communications Infrastructure) – Intermediate Level

Role Summary:

The Network VoIP / Webex Engineer is responsible for the implementation, operation, and optimisation of the Department's enterprise voice and collaboration platforms within a large-scale, business-critical network environment. This role is focused on hands-on delivery and operational support of IP telephony and unified communications services, ensuring reliability, performance, and service continuity across distributed sites.

The successful candidate will demonstrate extensive professional experience and strong practical expertise in supporting Cisco Unified Communications and Webex platforms within complex, live environments.

Core Responsibilities:

- Implement, support, and optimise enterprise IP telephony and unified communications platforms, including Cisco CUCM and Webex services.
- Take operational responsibility for voice and collaboration services, ensuring reliability, availability, and performance.
- Diagnose and resolve production issues affecting voice and collaboration platforms, including call quality, signalling, routing, and service outages.
- Perform safe, controlled changes to live environments, including configuration updates, patching, and system upgrades.
- Support integration between IP telephony platforms, legacy telephony systems, and modern collaboration tools.
- Monitor and optimise voice infrastructure, including call routing, dial plans, and media performance across the network.
- Contribute to the delivery of communications-related projects, including migrations, upgrades, and platform modernisation initiatives.
- Provide technical input into architectural decisions from a voice and collaboration perspective.
- Produce and maintain clear operational documentation, configuration standards, and support procedures.

Role Requirements:***Experience***

- Minimum 4+ years' demonstrable experience supporting enterprise-scale IP telephony and unified communications environments.
- Proven experience operating and maintaining business-critical voice and collaboration platforms in production environments.

IP Telephony & Unified Communications

- Extensive hands-on experience with Cisco Unified Communications Manager (CUCM), including enterprise and clustered deployments.
- Strong experience supporting Webex platforms, including Webex Calling, Control Hub, and collaboration services.
- Experience managing call routing, dial plans, and signalling protocols in complex environments.
- Experience with Cisco Unity Connection, UCCX, and Webex Contact Centre integrations.

- Experience working in mixed telephony environments, including interoperability with other systems (e.g. SIP trunking).

Voice, Media & Collaboration Technologies

- Strong understanding of voice protocols and technologies, including SIP, SCCP, RTP, and media flows.
- Experience troubleshooting voice quality issues, including latency, jitter, and packet loss.
- Practical experience implementing and supporting QoS policies for voice traffic across enterprise networks.
- Understanding of call control, session management, and endpoint provisioning.

Network Integration & Infrastructure

- Solid working knowledge of enterprise networking concepts, including routing, switching, and VLAN design.
- Experience working within Cisco networking environments (Catalyst, Nexus, ISR/ASR platforms).
- Ability to diagnose issues impacting voice services.
- Experience supporting secure connectivity and its impact on voice traffic (e.g., VPNs, encryption).

Operational Support & Troubleshooting

- Strong analytical and troubleshooting capability in live production environments.
- Experience diagnosing complex issues spanning voice platforms and underlying network infrastructure.
- Ability to perform root-cause analysis and implement stable, long-term fixes.
- Experience working within structured incident, problem, and change management processes.

Operational Excellence & Risk Management

- Ability to perform controlled changes to live systems with minimal disruption to services.
- Experience assessing risks associated with upgrades, migrations, and configuration changes.
- Strong focus on maintaining service continuity and platform stability.
- Experience working within governance and change control frameworks.

Stakeholder Engagement & Delivery

- Ability to engage with technical teams and stakeholders to support service delivery and operations.
- Experience working in environments where systems may be partially documented or evolving.
- Ability to deliver reliable technical solutions within operational constraints.
- Strong documentation discipline to ensure maintainability and knowledge transfer.

Skills & Competencies:

- Strong troubleshooting mindset with a focus on root-cause resolution.
- Ability to work independently in a high-responsibility operational role.
- Attention to detail and discipline when working in live environments.
- Ability to prioritise and respond effectively to production incidents.
- Strong focus on service availability, reliability, and operational excellence.
- Ability to work effectively with network, infrastructure, security, and application teams.

Qualifications and Certifications:

Depth of demonstrable, hands-on experience is essential. Candidates must demonstrate strong practical capability in implementing, supporting, maintaining, and optimising enterprise voice, collaboration, and communications platforms within complex network environments.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for practical experience and a proven track record of supporting enterprise voice, collaboration, and communications services.

Desirable Certifications (including but not limited to):

- Cisco CCNP Collaboration or equivalent.
- Certifications in voice, collaboration, or network technologies.

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, and proven support and delivery of enterprise voice, collaboration, and communications services, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

Network Security Engineer (Enterprise Security & Infrastructure) – Intermediate Level

Role Summary:

The Network Security Engineer (Enterprise Security & Infrastructure) is responsible for supporting the implementation, operation, and maintenance of the Department's cybersecurity controls across network, perimeter, endpoint, and hybrid cloud environments.

This role is hands-on and delivery-focused, working under established architectural frameworks and technical leadership to deploy, support, and maintain enterprise security platforms. The successful candidate will contribute to the stability, security, and performance of critical systems while continuing to develop deeper expertise in enterprise security technologies and operational practices.

The position requires practical experience across network security technologies (including Cisco and Check Point), with a focus on reliable service delivery, incident support, and continuous improvement of security controls.

Core Responsibilities:

- Deploy, configure, and maintain security controls across network, perimeter, and endpoint environments.
- Support the implementation of security architecture designs and standards in enterprise environments.
- Operate and maintain enterprise security platforms to ensure availability, stability, and performance.
- Perform day-to-day troubleshooting of security infrastructure issues, escalating complex problems where required.
- Assist with the management and optimisation of firewalls, VPNs, proxies, endpoint security solutions, and authentication systems.
- Execute approved changes in live environments in accordance with change management processes.
- Monitor security alerts and events, performing initial investigation and escalating incidents appropriately.
- Support and contribute to incident response activities, including investigation, containment, and recovery actions.
- Assist in maintaining and improving security configurations, policies, and rulesets.
- Contribute to automation efforts through the development and maintenance of scripts and operational tooling where appropriate.
- Maintain accurate technical documentation, including system configurations, procedures, and runbooks.
- Work closely with Senior Engineers and Architects to implement and refine security solutions and controls.
- Support audit, compliance, and governance activities through documentation and evidence collection.
- Participate in knowledge sharing and continuous learning within the team.
- Assist with configuration and physical deployment of security and networking equipment across multiple locations.

Role Requirements:

Experience

- Minimum 4+ years' experience in network and security engineering in enterprise environments.
- Experience supporting and maintaining security technologies in production environments.
- Demonstrated ability to troubleshoot and resolve technical issues across network and security platforms.

Enterprise Security Engineering

- Experience working with layered security controls across network, perimeter, and endpoint environments.
- Understanding of security architecture principles and the ability to implement defined designs.
- Experience working in environments with a mix of legacy and modern technologies.
- Hands-on experience with vulnerability detection platforms and performing network and endpoint scans.
- Hands-on experience with network access controls within enterprise Cisco network environments.

Security Technologies & Platforms

- Experience with Cisco network security technologies.
- Experience supporting VPN technologies.
- Experience with Cisco web proxy and email security gateway technologies.
- Familiarity with Check Point firewalls and security management.
- Exposure to firewall policy management, NAT, and VPN configuration concepts.

General Security Technologies

- Exposure to SIEM and logging platforms (e.g., Elasticsearch, Graylog, or similar).
- Basic understanding of secure email gateways and web proxy technologies.
- Familiarity with identity and authentication systems (e.g., MFA solutions).
- Awareness of DNS services and related security considerations.
- Basic system administration skills across Linux and Windows environments.
- Familiarity with vulnerability detection and response.

Networking & Security Fundamentals

- Solid understanding of TCP/IP networking, routing, and switching fundamentals.
- Basic troubleshooting skills across network connectivity, VPNs, and firewall behaviour.
- Understanding of common security threats, vulnerabilities, and mitigation approaches.

Operational Excellence & Incident Response

- Experience monitoring systems and responding to alerts in operational environments.
- Ability to follow incident response procedures and escalate issues appropriately.
- Awareness of change management processes and operational governance.

Additional Infrastructure Experience

- Exposure to enterprise voice, collaboration, or communication platforms.
- Basic understanding of enterprise infrastructure components supporting network services.

Stakeholder Engagement & Delivery

- Ability to work effectively as part of a technical team to deliver security solutions.
- Willingness to learn and adapt in dynamic and evolving environments.
- Ability to follow documented procedures and contribute to improving them.

Skills & Competencies:

- Strong technical aptitude with a willingness to develop hands-on expertise.
- Good analytical and problem-solving skills.
- Ability to work collaboratively within a team environment.
- Strong attention to detail and commitment to quality.
- Good communication skills, both written and verbal.
- Proactive approach to learning and continuous improvement.

Qualifications & Certifications:

Depth of demonstrable, hands-on experience is important. Candidates must demonstrate practical capability in supporting, implementing, securing, maintaining, and troubleshooting enterprise security platforms and infrastructure services within complex environments.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for practical experience and a proven track record of delivering and securing complex enterprise environments.

Desirable Certifications (including but not limited to):

- Cisco CCNA (Routing & Switching).
- Cisco CCNA (Security).
- Check Point Certified Security Administrator (CCSA).

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, relevant experience, technical aptitude, problem-solving ability, and the successful support and operation of enterprise security platforms and services, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

Network Engineer (Enterprise & Communications Infrastructure) – Junior Level

Role Summary:

The Network Engineer is responsible for supporting the operation and maintenance of the Department's enterprise network and communications platforms within a large-scale, business-critical environment. This role is focused on supporting day-to-day operations while contributing to the delivery and support of LAN, WAN, wireless, and unified communications services.

The successful candidate will demonstrate a strong foundation in networking concepts and practical experience in supporting enterprise infrastructure, with the ability to develop technical skills within complex, live environments.

Core Responsibilities:

- Support the implementation, support, and maintenance of enterprise network and communications infrastructure.
- Contribute to the operation of LAN, WAN, wireless, and unified communications environments.
- Monitor network and communications systems, identifying and escalating issues where appropriate.
- Assist in diagnosing and resolving network and connectivity issues, including performance and availability concerns.
- Perform routine configuration tasks and controlled changes in live environments under supervision.
- Assist with the onboarding and configuration of network devices, user endpoints, and telephony systems.
- Assist in maintaining network documentation, diagrams, and configuration records.
- Contribute to infrastructure upgrade and improvement initiatives as part of project delivery teams.
- Follow established operational procedures, change management processes, and governance standards.

Role Requirements:***Experience***

- Minimum 1 to 3 years' professional experience supporting network or IT infrastructure in an enterprise or comparable environment.
- Exposure to working in live production environments with an understanding of operational impact.

Networking Fundamentals

- Basic practical knowledge of networking concepts, including TCP/IP, subnetting, VLANs, and routing principles.
- Understanding of switching and routing fundamentals in enterprise environments.
- Familiarity with network troubleshooting concepts and tools.

Network Infrastructure & Technologies

- Exposure to enterprise routing and switching technologies, including Cisco or equivalent platforms.
- Working understanding of wireless networking concepts and environments.
- Familiarity with network monitoring tools and basic diagnostics.

IP Telephony & Unified Communications

- Foundational understanding of IP telephony and voice technologies, including VoIP concepts.
- Exposure to unified communications platforms (e.g., CUCM, Webex, or equivalent) is desirable.
- Willingness to develop skills in voice and collaboration technologies.

Operational Support & Troubleshooting

- Ability to follow structured troubleshooting processes to resolve basic issues.
- Strong attention to detail when working in live environments.
- Ability to escalate issues appropriately based on severity and impact.

Operational Excellence & Risk Awareness

- Awareness of the importance of controlled changes and service continuity in production environments.
- Ability to follow change management processes and operational procedures.
- Willingness to learn and apply best practices in network operations.

Stakeholder Engagement & Delivery

- Ability to work as part of a technical team in delivering operational support and project tasks.
- Strong communication skills when interacting with technical colleagues and service users.
- Willingness to learn from senior engineers and contribute positively to team delivery.

Skills & Competencies:

- Strong interest in developing a career in networking and communications technologies.
- Analytical mindset with a structured approach to problem solving.
- Ability to learn quickly and apply new technical concepts in practice.
- Attention to detail and discipline when working in operational environments.
- Ability to work collaboratively within a team while developing independent capability.

Qualifications and Certifications:

Practical, hands-on experience is important. Candidates should be able to demonstrate experience supporting, maintaining, and troubleshooting network and ICT infrastructure services within enterprise or similar environments.

Professional certifications, formal training, and recognised vendor-accredited courses are desirable and will be considered as evidence of technical knowledge and commitment to professional development. Equivalent practical experience will also be considered.

Desirable Certifications (including but not limited to):

- Cisco Certified Network Associate (CCNA) or equivalent.
- Entry-level networking or IT infrastructure certifications.
- Training or certification exposure in networking technologies.

Candidates should be able to demonstrate practical experience and a willingness to develop their skills across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated technical capability, relevant experience, problem-solving skills, and the ability to support and maintain ICT infrastructure services, with certifications considered as supporting evidence of technical knowledge and professional development.

=====

Lot 2: Infrastructure Team

- 1 x Enterprise Infrastructure Architect - Senior Level
- 1 x ICT Infrastructure Engineer (SQL Server Design & DBA) - Senior Level
- 1 x ICT Infrastructure Engineer (Enterprise Services & Linux) - Senior Level
- 2 x ICT Infrastructure Engineer (Microsoft Cloud & Power Platform) - Senior Level
- 1 x ICT Infrastructure Engineer (SCCM Endpoint Configuration Manager) - Senior Level
- 2 x ICT Infrastructure Engineer (Microsoft Hybrid Cloud & Enterprise Services) - Senior Level
- 2 x ICT Infrastructure Engineer (Microsoft Hybrid Cloud & Enterprise Services) - Intermediate Level

=====

Job Title:

Enterprise Infrastructure Architect – Senior Level

Role Summary:

The Senior Enterprise Infrastructure Architect is responsible for the design, development, governance, and continuous evolution of the Department's enterprise ICT architecture. This role provides architectural leadership across infrastructure, cloud, identity, security, application, data, and technology domains, ensuring ICT strategy remains aligned with organisational objectives while maintaining a secure, coherent, and sustainable enterprise architecture.

This role is focused on hands-on architectural leadership within complex enterprise environments, ensuring that architecture standards, governance, and technology roadmaps support both operational requirements and long-term strategic objectives.

The successful candidate will demonstrate extensive professional experience and advanced hands-on expertise across enterprise infrastructure, hybrid environments, cloud platforms, security, identity, and business transformation initiatives.

The Senior Enterprise Infrastructure Architect will report to the Infrastructure Manager of the ICT Unit and support the coordination of ICT Infrastructure Engineers. The role is responsible for assigning duties and tasks based on skills, experience, and project requirements. The Senior Enterprise Infrastructure Architect will also act as Project Manager for major enterprise architecture and infrastructure initiatives within the ICT function.

Core Responsibilities:

- Develop, maintain, and govern enterprise ICT architecture models, standards, frameworks, and technology roadmaps.
- Ensure alignment between ICT strategy, technology platforms, and organisational objectives.
- Provide architectural leadership for business transformation, service improvement, and technology modernisation initiatives.
- Ensure consistency and integration across business, application, data, infrastructure, and technology domains.
- Provide technical oversight and architectural assurance for the design, implementation, and operation of enterprise ICT solutions.
- Lead the design and integration of hybrid environments, ensuring interoperability between on-premises and cloud-based platforms.
- Ensure enterprise solutions comply with security, regulatory, governance, and operational requirements.

- Contribute to the design and implementation of highly available, secure, resilient, and disaster-tolerant enterprise environments.

Role Requirements:

Experience

- Minimum 7+ years' demonstrable experience designing, implementing and supporting enterprise infrastructure solutions within large and complex ICT environments.
- Proven experience designing and delivering complex enterprise-scale ICT solutions within large or complex environments.
- Demonstrated experience aligning technology strategy, architecture, and investment with organisational objectives.
- Proven experience designing and delivering highly available, secure, and disaster-resilient enterprise environments.
- Ability to operate effectively at both strategic and technical levels, providing leadership while remaining technically engaged.
- Demonstrable experience delivering complex infrastructure, cloud, security, identity, and modernisation initiatives.

Enterprise Infrastructure Architecture & Governance

- Strong capability in enterprise architecture modelling, governance, standards development, and roadmap planning.
- Experience designing and integrating solutions across infrastructure, application, data, identity, security, and technology domains.
- Strong understanding of architectural governance, security requirements, regulatory obligations, and enterprise risk considerations.
- Ability to provide architectural assurance and technical leadership across complex programmes and projects.

Enterprise Infrastructure Technologies

- Advanced hands-on experience with Microsoft Active Directory, including high availability, replication, trusts, FSMO roles, and authentication design.
- Advanced experience with Hyper-V environments, including multi-site clustering, quorum and witness design, SAN integration, and networking.
- Extensive knowledge of Windows Server technologies, enterprise deployments, and associated infrastructure services.
- Advanced experience with SQL Server and Microsoft Exchange environments, including clustering, disaster recovery, availability, hybrid integration, and enterprise-scale design considerations.

Hosting, Virtualisation & Enterprise Platforms

- Experience designing secure hosting environments spanning both production and disaster recovery facilities.
- Advanced experience in enterprise virtualisation, network architecture, load balancing, redundancy, backup, and disaster recovery design.
- Advanced experience designing and supporting Citrix and Remote Desktop environments, including policies, security controls, capacity planning, and architecture design.

Cloud Technologies & Identity Services

- Advanced experience designing and deploying Microsoft 365 and Azure enterprise solutions.
- Extensive experience with Microsoft Entra ID (Azure AD), including hybrid identity, authentication, identity governance, and access management.
- Experience with Privileged Access Management (PAM) solutions, including general administration and architectural understanding of Delinea Secret Server.
- Experience implementing enterprise security controls including Multi-Factor Authentication, Conditional Access, and Zero Trust principles.
- Advanced experience with Exchange Online, Purview, eDiscovery, and enterprise compliance services.
- Experience with Azure services including Key Vault, DevOps, Front Door, Single Sign-On, and enterprise application integration.
- Experience with Azure AD B2C, External ID, and external authentication solutions.
- Working knowledge of Microsoft Power Platform technologies.
- Proven experience delivering integrated hybrid cloud solutions across on-premises and cloud platforms.

PKI, Security & Enterprise Protection

- Advanced experience designing and managing Public Key Infrastructure environments, including Microsoft and Entrust platforms.
- Experience integrating Hardware Security Modules, including nCipher, Thales, and cloud-based HSM technologies.
- Practical experience with 802.1x, SCEP, and NDES technologies.
- Experience implementing and managing enterprise anti-virus and endpoint protection solutions across multi-platform environments.

Infrastructure Resilience, Backup & Disaster Recovery

- Advanced experience with enterprise server and storage technologies, including SAN, DAS, and replication solutions.
- Advanced experience implementing and managing Commvault enterprise backup and recovery platforms.
- Demonstrated experience designing and implementing end-to-end disaster recovery solutions across enterprise systems and platforms.

Stakeholder Engagement & Technical Leadership

- Strong communication and stakeholder engagement skills, with the ability to influence architectural direction and decision-making at senior organisational levels.
- Ability to lead architectural discussions, provide technical leadership, and guide multidisciplinary teams through complex technical and organisational challenges.
- Ability to communicate complex technical concepts clearly to both technical and non-technical audiences.
- Proven ability to balance business requirements, operational constraints, risk, and technical considerations when developing solutions.

Skills & Competencies:

- Strong judgement in balancing strategic objectives, operational requirements, architectural standards, and organisational priorities.
- Strong analytical and problem-solving capability across infrastructure, cloud, security, identity, and enterprise technology domains.
- Ability to work independently and deliver effectively within a high-responsibility, outcome-focused role.
- Structured and disciplined approach to documentation, governance, architecture assurance, risk management, and project delivery.
- Strong focus on resilience, maintainability, security, and long-term operational supportability.

Qualifications and Certifications:

Depth of demonstrable, hands-on experience is essential. Candidates must demonstrate strong practical capability in designing, implementing, governing, and supporting enterprise-scale ICT solutions across complex environments.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for substantial practical experience and a proven track record of delivering enterprise-scale solutions.

Desirable Certifications (including but not limited to):

- Microsoft Certified: Windows Server Hybrid Administrator Associate.
- Microsoft Certified: Azure Administrator Associate.
- Microsoft Certified Systems Administrator (MCSA).
- Microsoft Certified: Azure Solutions Architect Expert.
- Microsoft Certified Systems Engineer (MCSE).

Candidates must be able to demonstrate substantial practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, and proven delivery of enterprise-scale ICT solutions, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

ICT Infrastructure Engineer (SQL Server Design & DBA) – Senior Level

Role Summary:

The Senior ICT Infrastructure Engineer (SQL Server Design & DBA) is responsible for the design, implementation, support, and continuous improvement of enterprise SQL Server environments across on-premises and cloud platforms. The role ensures the delivery and ongoing optimisation of secure, highly available, and high-performing database services supporting critical business applications within a complex, hybrid infrastructure.

SQL Server is a core component of the Department's ICT infrastructure, with multiple instances operating across varied platforms and configurations. The successful candidate will demonstrate extensive professional expertise and advanced hands-on experience in the design, administration, and optimisation of SQL Server environments, ensuring robust, scalable, and resilient database solutions with minimal downtime.

Core Responsibilities:

- Design, implement, administer, and support Microsoft SQL Server environments across on-premises and cloud platforms.
- Design and manage complex SQL Server environments, including multi-instance deployments, high availability, disaster recovery, backup, recovery, and security solutions.
- Monitor, manage, and proactively optimise database performance and overall environment stability.
- Identify and resolve performance bottlenecks, including advanced query tuning and resource optimisation.
- Perform database maintenance tasks including patching, upgrades, indexing, and integrity checks.
- Lead database capacity planning and design decisions, including storage, IOPS, and resource utilisation.
- Configure and manage SQL Server instances, including collation, authentication modes, and instance-level settings.
- Develop, support, and maintain T-SQL scripts and PowerShell automation for database administration and operational efficiency.
- Collaborate with infrastructure and application teams to design and support business-critical systems and integrations.
- Provide advanced troubleshooting and incident resolution across SQL Server platforms.
- Contribute to and maintain SQL Server architecture standards, documentation, best practices, and operational procedures.

Role Requirements:***Experience***

- Minimum 7+ years of demonstrated experience in SQL Server administration, database management, and solution design.
- Proven expertise in Microsoft SQL Server across enterprise environments.
- Extensive experience supporting enterprise SQL Server environments across complex and distributed infrastructures.
- Experience supporting hybrid environments (on-premises and cloud-based SQL services).
- Experience designing and delivering highly available, secure, and resilient database services.
- Strong experience in database performance tuning, optimisation, and troubleshooting.
- Experience working within large-scale, complex, and distributed environments.
- Ability to operate effectively across infrastructure, database, and application domains.

- Strong communication and stakeholder engagement skills.

Microsoft SQL Server (Core)

- Extensive experience installing, configuring, administering, and supporting enterprise SQL Server environments.
- Strong experience in database maintenance, backup, recovery, and operational management.
- Advanced knowledge of SQL Server security, authentication, and access control.

High Availability & Disaster Recovery

- Strong experience designing and implementing SQL Server clustering and availability groups.
- Experience implementing and supporting multi-site failover and disaster recovery solutions.
- Knowledge of replication and failover mechanisms for enterprise resilience.

Performance Tuning & Optimisation

- Proven ability to identify and resolve performance issues in SQL Server environments.
- Experience using monitoring tools to analyse query performance and system metrics.
- Ability to optimise queries, indexing strategies, and database structures.

Database Design & Capacity Planning

- Experience in database design, sizing, and capacity planning, including IOPS and storage considerations.
- Understanding of instance design, including collation, authentication modes, and configuration standards.
- Awareness of network and infrastructure considerations impacting database performance.

Scripting & Automation

- Strong working knowledge of T-SQL scripting and query optimisation.
- Experience with SQL Server PowerShell modules for automation and administration.
- Ability to develop scripts to improve operational efficiency and consistency.

Infrastructure Integration

- Understanding of how SQL Server integrates within wider ICT infrastructure.
- Experience collaborating with infrastructure, cloud, and application teams.
- Awareness of virtualisation, storage, and networking considerations impacting databases.

Microsoft Infrastructure & Platform Technologies (Advanced)

- Advanced to expert-level experience installing, administering, and maintaining Active Directory, including Group Policy, DNS, and DHCP design and configuration.
- Experience administering Delinea Secret Server, including privileged account management, credential vault administration, and access governance.
- Advanced to expert-level experience across Windows Server roles, features, and enterprise deployments.
- Extensive experience managing enterprise storage infrastructure, including SAN and geo-clustered environments.
- Advanced experience implementing and managing Commvault enterprise backup and recovery platforms.
- Experience designing, deploying, and supporting Work Folders solutions.
- Advanced experience administering SCCM, including OS deployment, patch management, and endpoint lifecycle control.

Skills & Competencies:

- Strong technical capability across SQL Server administration, database architecture, performance optimisation, high availability, disaster recovery, and infrastructure integration.
- Strong analytical and problem-solving capability across database, infrastructure, and application domains.
- Ability to operate effectively within complex enterprise environments while managing competing priorities.
- Strong communication and stakeholder engagement skills, with the ability to work effectively with technical teams, vendors, and business stakeholders.
- Ability to provide technical leadership, mentor junior staff, and contribute to knowledge sharing and capability development.
- Structured and disciplined approach to documentation, operational procedures, standards, and continuous service improvement.
- Strong focus on security, resilience, availability, performance, and operational reliability.

Qualifications and Certifications:

Depth of demonstrable, hands-on experience is essential. Candidates must demonstrate strong practical capability in designing, implementing, administering, supporting, and optimising SQL Server environments across complex enterprise infrastructures.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for substantial practical experience and a proven track record of delivering enterprise-scale solutions.

Desirable Certifications (including but not limited to):

- Microsoft Certified: Azure Database Administrator Associate.
- Microsoft Certified: Azure Data Engineer Associate.
- Microsoft Certified: Azure Administrator Associate.
- Microsoft Certified IT Professional (MCITP) Database Administrator (Associate level).
- Microsoft Certified Solutions Expert (MCSE) Data Management and Analytics (Expert level).

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, formal accreditation, and proven delivery of enterprise-scale SQL Server solutions, with certifications considered as evidence of professional development and technical competency.

=====

Job Title:

ICT Infrastructure Engineer (Enterprise Services & Linux) – Senior Level

Role Summary:

The Senior ICT Infrastructure Engineer (Enterprise Services & Linux) is responsible for the implementation, administration, support, and continuous improvement of enterprise ICT infrastructure across on-premises environments. The role ensures the delivery of secure, highly available, and performant systems supporting critical business operations within a complex enterprise environment.

The successful candidate will demonstrate extensive professional experience and advanced hands-on expertise across Microsoft enterprise services, Linux platforms, virtualisation, and infrastructure automation, ensuring the effective operation, optimisation, and resilience of core enterprise systems.

Core Responsibilities:

- Implement, support, and optimise enterprise ICT infrastructure across on-premises environments.
- Lead infrastructure initiatives, including system upgrades, migrations, and service deployments.
- Administer and maintain Microsoft enterprise platforms, including Windows Server and core infrastructure services.
- Manage enterprise identity services, including Active Directory, Group Policy, authentication, and directory services.
- Deliver and support core enterprise services such as DNS, DHCP, PKI, authentication, and file and print services.
- Administer and support enterprise Linux environments (e.g. SUSE, SLES, Ubuntu), including patching, performance tuning, and system optimisation.
- Implement and maintain high availability, backup, and disaster recovery solutions across infrastructure platforms.
- Manage virtualisation platforms, including VMware and Hyper-V environments, ensuring performance, resilience, and scalability.
- Implement infrastructure automation using scripting and configuration management tools, including PowerShell, Bash, Python, and Ansible.
- Support containerisation platforms, including OCI containers (Docker) and Kubernetes environments.
- Configure, administer, and support Synology DiskStation systems and Synology Active Backup for Microsoft 365.
- Experience administering Delinea Secret Server, including privileged account management, credential vault administration, and access governance.
- Apply security best practices across infrastructure platforms, including vulnerability management, access control, and compliance requirements.
- Monitor system performance, availability, and capacity, proactively identifying and resolving issues.
- Provide advanced troubleshooting, incident resolution, and root cause analysis across enterprise infrastructure services.
- Collaborate with internal teams and vendors to deliver integrated infrastructure solutions.
- Produce and maintain technical documentation, standards, and operational procedures.
- Provide technical leadership, mentoring junior staff, and contributing to knowledge sharing.

Role Requirements:

Experience

- Minimum 7+ years of demonstrated experience in enterprise ICT infrastructure roles.
- Proven experience managing complex on-premises infrastructure environments.
- Strong expertise in Microsoft enterprise technologies and identity services.
- Extensive experience administering Linux systems within production environments.
- Experience managing virtualisation platforms, including VMware and Hyper-V.
- Demonstrated experience implementing infrastructure automation using tools such as Ansible and scripting languages.
- Experience supporting container technologies, including Docker and Kubernetes.
- Experience delivering enterprise infrastructure projects, including upgrades, migrations, and deployments.
- Strong understanding of infrastructure security, compliance, and enterprise operational standards.
- Proven ability to troubleshoot complex technical issues and implement long-term solutions.
- Ability to operate effectively across multiple infrastructure domains.
- Strong communication and stakeholder engagement skills.

Microsoft Windows Server & Core Infrastructure

- Demonstrated advanced-level experience with Active Directory, including Group Policy, trusts, replication, ADMX/ADML, DNS, and DHCP.
- Advanced experience managing Windows Server roles, features, and enterprise deployments.
- Experience supporting identity, authentication, and core infrastructure services.

Linux Platforms & Open Systems

- Advanced experience administering GNU/Linux and SUSE Linux Enterprise Server (SLES).
- Experience implementing and supporting Linux-based services in production environments.
- Strong understanding of Linux system performance tuning, patching, and security.

Virtualisation & Containers

- Advanced experience managing virtualisation platforms, including VMware and Hyper-V (clustering, networking, failover).
- Experience working with OCI container platforms such as Docker.
- Working knowledge of Kubernetes for container orchestration and deployment.

Automation & Configuration Management

- Strong experience implementing automation using PowerShell, Bash, and Python.
- Advanced experience using configuration management tools such as Ansible.
- Ability to implement automated infrastructure deployment and management processes.

Storage, Backup & Platform Services

- Experience managing enterprise storage environments, including SAN and replicated storage solutions.
- Experience administering Synology Active Backup for Microsoft 365.
- Experience managing Synology DiskStation OS and associated storage services.
- Advanced experience implementing and managing Commvault enterprise backup and recovery platforms.
- Understanding of storage performance, resilience, and disaster recovery strategies.

Security & Access Management

- Strong understanding of enterprise security practices, including vulnerability management and compliance.
- Experience administering privileged access management solutions such as Secret Server PAM.
- Knowledge of authentication systems, PKI, and secure infrastructure design.

Networking & Infrastructure Integration

- Advanced knowledge of enterprise networking concepts and infrastructure integration.
- Experience supporting DNS, DHCP, and network-based services within enterprise environments.
- Ability to integrate infrastructure components across multiple platforms.

Infrastructure Operations & Support

- Experience monitoring and optimising infrastructure performance, availability, and reliability.
- Strong troubleshooting and problem-solving skills across infrastructure platforms.
- Ability to provide incident response and root cause analysis.

Skills & Competencies:

- Strong technical capability across Microsoft enterprise infrastructure, Linux platforms, virtualisation, automation, and container technologies.
- Strong analytical and problem-solving capability across multiple infrastructure domains.
- Ability to operate effectively within complex enterprise environments while managing competing priorities.
- Strong communication and stakeholder engagement skills, with the ability to work effectively with technical teams, vendors, and business stakeholders.
- Ability to provide technical leadership, mentor junior staff, and contribute to team capability development.
- Structured and disciplined approach to documentation, operational standards, and continuous service improvement.
- Strong focus on security, resilience, performance, and operational reliability.

Qualifications and Certifications:

Depth of demonstrable, hands-on experience is essential. Candidates must demonstrate strong practical capability in implementing, administering, supporting, and optimising enterprise infrastructure services across complex technology environments.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for substantial practical experience and a proven track record of delivering enterprise infrastructure solutions.

Desirable Certifications (including but not limited to):

- Microsoft Certified: Azure Administrator Associate.
- Microsoft Certified: Windows Server Hybrid Administrator Associate.
- Microsoft 365 Certified: Endpoint Administrator Associate.
- Microsoft Certified: Identity and Access Administrator Associate.
- Microsoft Certified Solutions Associate (MCSA) in technology relevant to the role (Associate level).
- Microsoft Certified Solutions Expert (MCSE) in technology relevant to the role (Expert level).
- RHCSA, RHCE, or equivalent Linux certifications.

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, and proven delivery of enterprise-scale ICT infrastructure solutions, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

ICT Infrastructure Engineer (Microsoft Cloud & Power Platform) – Senior Level

Role Summary:

The Senior ICT Infrastructure Engineer (Microsoft Cloud & Power Platform) is responsible for the implementation, administration, support, and continuous improvement of Microsoft cloud infrastructure and platform services across Azure and Power Platform technologies. The role ensures the delivery of secure, scalable, and high-performing solutions supporting critical business services within a modern, cloud-first environment.

The successful candidate will demonstrate extensive professional experience and advanced hands-on expertise across Microsoft Azure, Power Platform, application integration, and identity services, contributing to enterprise service delivery and digital transformation initiatives.

Core Responsibilities:

- Implement, configure, and support Microsoft Azure infrastructure and platform services.
- Implement, configure, and support solutions using Microsoft Power Platform, including Power Apps, Power BI, Power Automate, and Power Pages.
- Implement and support integrations between Power Platform and Azure services, including Azure Functions, Logic Apps, and Web Apps.
- Configure and manage Azure resources, including App Services, Function Apps, Storage Accounts, and networking components.
- Implement and manage Entra ID (Azure AD) application registrations and secure API integrations.
- Implement and maintain secure cloud solutions using Key Vault, managed identities, and role-based access control (RBAC).
- Support the development, deployment, and operation of web applications hosted in Azure environments.
- Support the implementation of scalable, secure, and maintainable cloud solutions aligned to business requirements.
- Monitor and optimise performance, availability, and security of cloud services.
- Develop and maintain automation for cloud deployment, configuration, and management using Infrastructure as Code and scripting tools.
- Provide advanced troubleshooting, incident resolution, and root cause analysis across cloud and platform services.
- Collaborate with internal stakeholders and external vendors to deliver integrated cloud and application solutions.
- Produce and maintain technical documentation, standards, and operational procedures.
- Provide technical guidance, mentoring, and knowledge transfer to team members.

Role Requirements:***Experience***

- Minimum 7+ years of demonstrated experience in ICT infrastructure and cloud engineering roles.
- Proven expertise in Microsoft Azure across enterprise environments.
- Demonstrated experience developing and supporting Microsoft Power Platform solutions.
- Experience integrating Power Platform solutions with Azure services and enterprise APIs.
- Strong understanding of cloud security principles, identity management, and access control.
- Proven experience delivering technical solutions through implementation and operational support.
- Experience working within large-scale, complex, and distributed environments.

- Strong troubleshooting capability across cloud platforms and application services.
- Ability to operate effectively across infrastructure, application, and platform domains.
- Strong communication and stakeholder engagement skills.

Microsoft Azure & Cloud Infrastructure

- Advanced knowledge of Microsoft Azure services, including compute, networking, and storage.
- Experience managing Azure resources, including Storage Accounts (Blob and Containers), App Services, and networking configurations.
- Strong experience with Azure Functions, serverless computing, and application hosting.
- Experience with Azure Front Door and Web Application Firewall (WAF) for secure application delivery.
- Experience using Azure logging, monitoring, and diagnostics (Log Analytics, Application Insights).
- Understanding of cloud architecture principles and enterprise deployment patterns.

Power Platform & Business Applications

- Advanced experience developing and supporting solutions using Power Platform, including Power Apps, Power Automate, Power BI, and Power Pages.
- Experience working with Microsoft Dynamics 365 and integration with Power Platform services.
- Familiarity with Microsoft Fabric for analytics and data platform capabilities.
- Strong understanding of low-code development, governance, and lifecycle management.

Integration & Application Services

- Experience implementing and supporting enterprise application integrations using Azure Functions, APIs, and web services.
- Experience integrating applications using Microsoft Graph API and application registrations.
- Strong understanding of enterprise application integration patterns and service-to-service communication.
- Experience integrating third-party platforms such as Cloudmersive.

Identity, Security & Access Management

- Strong knowledge of Entra ID (Azure AD), including application registrations and identity governance.
- Experience implementing Entra External ID and B2C identity solutions.
- Experience using Azure Key Vault for secure secrets, certificates, and key management.
- Understanding of RBAC, managed identities, and secure access control models.
- Familiarity with compliance and privacy tools such as Microsoft Purview and OneTrust.

Automation, DevOps & Scripting

- Experience with DevOps practices and tools for CI/CD pipelines and deployment automation.
- Proficiency in PowerShell scripting and automation.
- Experience with Infrastructure as Code (ARM, Bicep, Terraform).
- Ability to automate cloud provisioning, configuration, and operational processes.

Cloud Operations, Monitoring & Support

- Experience monitoring and optimising cloud performance, availability, and reliability.
- Strong troubleshooting and problem-solving skills across cloud, application, and integration layers.
- Ability to provide incident response, diagnostics, and root cause analysis.

Skills & Competencies:

- Strong technical capability across Microsoft Azure, Power Platform, identity services, application integrations, and cloud infrastructure technologies.
- Strong analytical and problem-solving capability across cloud, application, integration, and platform domains.
- Ability to operate effectively within complex enterprise environments while managing competing priorities.
- Strong communication and stakeholder engagement skills, with the ability to work effectively with technical teams, vendors, and business stakeholders.
- Ability to provide technical guidance, mentor team members, and contribute to knowledge sharing and capability development.
- Structured and disciplined approach to documentation, operational standards, governance, and continuous service improvement.
- Strong focus on security, scalability, performance, reliability, and maintainability.

Qualifications and Certifications:

Depth of demonstrable, hands-on experience is essential. Candidates must demonstrate strong practical capability in implementing, administering, supporting, and optimising Microsoft cloud, platform, and integration services across complex enterprise environments.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for substantial practical experience and a proven track record of delivering enterprise-scale Microsoft cloud and platform solutions.

Desirable Certifications (including but not limited to):

- Microsoft Certified: Azure Administrator Associate.
- Microsoft Certified: Azure Solutions Architect Expert.
- Microsoft Certified: Power Platform Developer Associate.
- Microsoft Certified: Power Platform Functional Consultant Associate.

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, and proven delivery of enterprise-scale Microsoft cloud and platform solutions, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

ICT Infrastructure Engineer (SCCM / Endpoint Configuration Manager) – Senior Level

Role Summary:

The Senior ICT Infrastructure Engineer (SCCM / Endpoint Configuration Manager) is responsible for the administration, support, and continuous improvement of enterprise endpoint management and associated infrastructure services across a complex ICT estate.

This role has a strong focus on Microsoft Endpoint Configuration Manager (SCCM/MECM), including operating system deployment, software distribution, patch management, and endpoint compliance. In addition, the role includes administration and support of Windows Server environments underpinning endpoint services.

The successful candidate will ensure endpoint devices and supporting infrastructure are secure, standardised, and efficiently managed in line with Government ICT policies, operating within a structured, security-focused, and compliance-driven environment.

They will demonstrate extensive professional experience and advanced hands-on expertise across endpoint management and supporting infrastructure technologies.

Core Responsibilities:

- Administer and maintain the SCCM/MECM environment to support enterprise endpoint management.
- Deliver and support operating system deployments.
- Manage software packaging and application deployment.
- Manage patching processes, including monthly updates, automatic deployment rules, and compliance monitoring.
- Monitor and maintain endpoint health, performance, and compliance across the ICT estate.
- Troubleshoot and resolve complex SCCM client, infrastructure, and deployment issues.
- Manage SCCM infrastructure components, including distribution points, management points, and content distribution.
- Administer and support Windows Server environments supporting endpoint services.
- Manage Windows Server operating systems, including patching, updates, and system health.
- Support Active Directory integration and Group Policy configuration.
- Support core infrastructure services, including DNS and DHCP, in collaboration with infrastructure teams.
- Perform server-side troubleshooting related to endpoint management services.
- Assist with capacity planning, performance tuning, and system reliability for SCCM-related servers.
- Implement endpoint and server security configurations in line with Government and NCSC standards.
- Support vulnerability remediation across endpoint and server environments.
- Develop and maintain PowerShell scripts to automate endpoint and server management tasks.
- Maintain technical documentation, including SOPs and operational procedures.
- Contribute to continuous improvement of endpoint and infrastructure services.

Role Requirements:

Experience

- Minimum 7+ years' experience in ICT infrastructure, with a strong focus on endpoint engineering and Windows Server administration.
- Proven experience administering SCCM/MECM in a large-scale enterprise environment.
- Experience supporting Windows Server infrastructure in production environments.
- Experience managing large-scale endpoint environments.
- Demonstrated experience in OS deployment, imaging, software packaging, and patch management.
- Strong experience troubleshooting complex endpoint and server-related issues.
- Experience working within structured, policy-driven environments (public sector or regulated industry desirable).
- Ability to operate across endpoint, server, and infrastructure domains.
- Strong communication and stakeholder engagement skills.

Endpoint Management (SCCM/MECM)

- Advanced experience administering Microsoft Endpoint Configuration Manager (SCCM/MECM).
- Expertise in OS deployment, application packaging, and patch management.
- Strong understanding of endpoint compliance, monitoring, and lifecycle management.

Windows Server & Core Infrastructure

- Advanced experience managing Windows Server environments (2016/2019/2022+).
- Strong knowledge of Active Directory, Group Policy, DNS, and DHCP.
- Experience supporting infrastructure services underpinning endpoint platforms.

Automation & Scripting

- Strong PowerShell scripting capability for automation and system administration.
- Ability to develop scripts for deployment, monitoring, and reporting.

Security & Compliance

- Understanding of endpoint and server security best practices.
- Experience supporting vulnerability remediation and compliance requirements.
- Support audit requirements, reporting, and compliance activities.

Skills & Competencies:

- Strong technical capability across endpoint management, Windows Server infrastructure, automation, and supporting enterprise technologies.
- Strong analytical and problem-solving capability across endpoint, server, and infrastructure domains.
- Ability to operate effectively within complex enterprise environments while managing competing priorities.
- Strong communication and stakeholder engagement skills, with the ability to work effectively with technical teams, vendors, and business stakeholders.
- Ability to provide technical leadership, mentor junior staff, and contribute to knowledge sharing and capability development.
- Structured and disciplined approach to documentation, operational procedures, compliance, and continuous service improvement.
- Strong focus on security, reliability, standardisation, and operational effectiveness.

Qualifications and Certifications:

Depth of demonstrable, hands-on experience is essential. Candidates must demonstrate strong practical capability in administering, supporting, and optimising enterprise endpoint management and supporting infrastructure services across complex ICT environments.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for substantial practical experience and a proven track record of delivering enterprise-scale endpoint management solutions.

Desirable Certifications (including but not limited to):

- Microsoft Certified: Azure Administrator Associate.
- Microsoft Certified: Windows Server Hybrid Administrator Associate.
- Microsoft 365 Certified: Endpoint Administrator Associate.
- Microsoft Certified Solutions Associate (MCSA) in technology relevant to the role (Associate level).
- Microsoft Certified Solutions Expert (MCSE) Cloud Platform and Infrastructure includes SCCM competencies (Expert level).

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, and proven delivery of enterprise-scale endpoint management and supporting infrastructure solutions, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

ICT Infrastructure Engineer (Microsoft Hybrid Cloud & Enterprise Services) – Senior Level

Role Summary:

The Senior ICT Infrastructure Engineer is responsible for the implementation, support, and continuous improvement of enterprise ICT infrastructure across on-premises and cloud platforms. The role ensures the delivery and ongoing optimisation of secure, highly available, and performant services across Microsoft technologies, supporting critical business operations within a complex, hybrid environment.

The successful candidate will demonstrate extensive professional experience and advanced hands-on technical expertise across enterprise infrastructure, cloud services, identity, and endpoint management.

Core Responsibilities:

- Implement, support, and maintain enterprise Microsoft infrastructure across on-premises and cloud environments.
- Administer and support Active Directory services, including Group Policy, DNS, DHCP, trusts, and identity management.
- Manage Windows Server environments, including roles, features, patching, and lifecycle management.
- Support and maintain Hyper-V and virtualised environments, including clustering and high availability.
- Administer Microsoft 365 services, including Exchange Online, Teams, SharePoint, and OneDrive.
- Support Exchange Server (on-premises and hybrid), including DAGs, backup and recovery, and troubleshooting.
- Manage Azure environments, including subscriptions, resource groups, identity services, and access control.
- Implement and manage Intune for endpoint configuration, compliance, software deployment, and device lifecycle.
- Ensure security best practices, including Conditional Access, MFA, PKI, and threat protection.
- Implement and support disaster recovery, backup, and high availability solutions.
- Manage and maintain UPS systems and power infrastructure, ensuring monitoring, testing, and resilience for critical ICT services.
- Manage storage infrastructure, including SAN environments and backup platforms.
- Develop automation scripts using PowerShell to improve operational efficiency.
- Monitor and optimise infrastructure performance, availability, and capacity.
- Provide advanced troubleshooting and incident resolution across infrastructure services.
- Collaborate with internal stakeholders and external vendors to deliver infrastructure solutions.

Role Requirements:***Experience***

- Minimum 7+ years of demonstrated experience in enterprise ICT infrastructure environments.
- Proven expertise across Microsoft server, cloud, and enterprise platform technologies.
- Demonstrated experience supporting hybrid environments integrating on-premises and cloud-based services.
- Strong experience in infrastructure implementation and advanced troubleshooting.
- Experience working within large-scale, complex, and distributed environments.

- Ability to operate effectively across multiple technical domains in parallel.
- Demonstrated experience delivering secure, highly available, and resilient infrastructure solutions.
- Ability to provide detailed examples of advanced technical expertise across listed technologies.

Microsoft Windows Server Technologies

- Demonstrated advanced-level experience in Active Directory (Group Policy, trusts, replication, ADMX/ADML, DNS, DHCP).
- Demonstrated advanced-level experience in Hyper-V (clustering, virtual networking, replication, failover).
- Demonstrated advanced-level experience in Windows Server roles, features, and enterprise deployments.

Microsoft Exchange & SQL

- Exchange (On-prem and Online): DAG administration, hybrid configuration, backup and restore, troubleshooting.
- SQL Server: general administration, maintenance, and performance support.

General Infrastructure & Systems Administration

- Server hardware installation, configuration, and lifecycle management.
- Disaster recovery, high availability, clustering, and incident response.
- Enterprise PKI infrastructure and certificate management.
- Storage and SAN management, preferably including Dell PowerStore.
- Advanced networking knowledge across enterprise environments.
- Scripting and automation using PowerShell and related technologies.
- UPS technologies and infrastructure resilience solutions.
- Enterprise backup and anti-virus platforms.
- Mobile device management platforms including Microsoft Intune and legacy platforms such as MobileIron.

Cloud Technologies (Microsoft 365, Azure, Intune)

- Demonstrated advanced-level experience in Microsoft 365 administration (Exchange Online, Teams, SharePoint, OneDrive).
- Demonstrated advanced-level experience in Entra ID, identity and access management, and hybrid identity.
- Experience administering Delinea Secret Server, including privileged account management, credential vault administration, and access governance.
- Demonstrated advanced-level experience in Intune (endpoint management, compliance, Autopilot, device deployment).
- Demonstrated advanced-level experience in Azure (subscriptions, resource groups, identity, application registration).
- Experience managing Conditional Access, MFA, PIM, licensing, and tenant administration.
- Understanding of Microsoft 365 security (Defender, threat policies, compliance, eDiscovery).
- Experience deploying and managing Windows 11 devices in hybrid environments.
- General Power Platform administration knowledge.

Hosting, Backup & Citrix

- Support of web hosting technologies including IIS.
- Experience managing Commvault enterprise backup and recovery platforms.
- Demonstrated experience in Citrix environments (XenApp, Virtual Apps, Storefront, Studio, Director, licensing).

Skills & Competencies:

- Strong technical capability across Microsoft enterprise infrastructure, cloud services, identity platforms, endpoint management, and hybrid technologies.
- Strong analytical and problem-solving capability across multiple infrastructure domains.
- Ability to operate effectively within complex enterprise environments while managing competing priorities.
- Strong communication and stakeholder engagement skills, with the ability to work effectively with technical teams, vendors, and business stakeholders.
- Ability to provide technical leadership, mentor junior staff, and contribute to knowledge sharing.
- Structured and disciplined approach to documentation, operational standards, and continuous service improvement.
- Strong focus on security, resilience, availability, performance, and operational reliability.

Qualifications and Certifications:

Depth of demonstrable, hands-on experience is essential. Candidates must demonstrate strong practical capability in implementing, supporting, administering, and optimising enterprise Microsoft infrastructure services across complex hybrid environments.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for substantial practical experience and a proven track record of delivering enterprise-scale ICT infrastructure solutions.

Desirable Certifications (including but not limited to):

- Microsoft Certified: Azure Administrator Associate.
- Microsoft Certified: Windows Server Hybrid Administrator Associate.
- Microsoft 365 Certified: Endpoint Administrator Associate.
- Microsoft Certified Solutions Associate (MCSA) in technology relevant to the role (Associate level).
- Microsoft Certified Solutions Expert (MCSE) in technology relevant to the role (Expert level).

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, and proven delivery of enterprise-scale ICT infrastructure solutions, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

ICT Infrastructure Engineer (Microsoft Hybrid Cloud & Enterprise Services) – Intermediate Level

Role Summary:

The ICT Infrastructure Engineer is responsible for the support, maintenance, and ongoing improvement of enterprise ICT infrastructure across on-premises and cloud platforms. This role focuses on delivering secure, reliable, and high-performing Microsoft-based services in a hybrid environment while supporting day-to-day operations.

This position will also act as a key escalation point for the Help Desk, ensuring timely resolution of complex technical issues while maintaining a strong customer service focus.

The successful candidate will demonstrate a minimum of 4 years of relevant experience, solid technical capability across Microsoft technologies, and a proactive approach to service delivery and continuous improvement.

Core Responsibilities:

- Support, maintain, and enhance Microsoft infrastructure across on-premises and cloud environments.
- Act as a Level 2/3 escalation point for Help Desk issues, ensuring effective and timely resolution.
- Provide excellent customer-focused support, communicating clearly with end users and stakeholders.
- Administer Active Directory services, including Group Policy, DNS, DHCP, and identity management.
- Support Windows Server environments, including patching, updates, and lifecycle management.
- Assist in managing virtualised environments (Hyper-V), including high availability and performance monitoring.
- Support Microsoft 365 services, including Exchange Online, Teams, SharePoint, and OneDrive.
- Assist with Exchange (on-premises and hybrid) administration and troubleshooting.
- Support Azure environments, including user access, resource management, and adherence to governance controls.
- Manage endpoint devices using Microsoft Intune (configuration, compliance, and deployments).
- Implement and support security measures such as MFA, Conditional Access, and endpoint protection.
- Assist in backup, disaster recovery, and business continuity processes.
- Support and maintain UPS systems and related power infrastructure to ensure availability and resilience of ICT services.
- Monitor infrastructure performance and respond to incidents and alerts.
- Develop and maintain basic automation scripts (e.g., PowerShell) to improve efficiency.
- Support the implementation of security, governance, and compliance controls across infrastructure and cloud services.
- Work collaboratively with senior engineers, vendors, and internal teams on infrastructure improvements and small-scale projects.
- Contribute to documentation, knowledge base articles, and process improvements.

Role Requirements:

Experience

- Minimum 4+ years' experience in ICT infrastructure or systems administration roles.
- Strong hands-on experience with Microsoft server and cloud technologies.
- Experience supporting hybrid environments (on-premises and cloud).
- Proven experience in troubleshooting infrastructure and end-user issues.
- Experience working with service desks and handling escalations.
- Experience supporting end users and stakeholders within a customer-focused ICT environment.
- Ability to prioritise and manage multiple tasks in a fast-paced environment.

Microsoft Windows Server & Core Infrastructure

- Solid experience with Active Directory (Group Policy, DNS, DHCP, user & group management).
- Experience supporting Windows Server roles and services.
- Working knowledge of Hyper-V and virtualisation concepts.

Microsoft 365 & Cloud Technologies

- Experience administering Microsoft 365 (Exchange Online, Teams, SharePoint, OneDrive).
- Basic to intermediate knowledge of Entra ID (Azure AD) and identity management.
- Experience administering Delinea Secret Server, including privileged account management, credential vault administration, and access governance.
- Experience with Microsoft Intune for device and policy management.
- Familiarity with Azure fundamentals (subscriptions, access control, resource basics).
- Understanding of security features such as MFA, Conditional Access, and Defender.

General Infrastructure & Systems Support

- Experience with server hardware and general system administration.
- Understanding of backup, recovery, and high availability concepts.
- Exposure to Commvault enterprise backup and recovery platforms.
- Basic networking knowledge (TCP/IP, VLANs, switching fundamentals).
- Scripting experience (PowerShell preferred, at a practical level).

Customer Service & Support

- Demonstrated ability to handle help desk escalations professionally and efficiently.
- Strong problem-solving and troubleshooting skills.
- Ability to translate technical issues into user-friendly language.
- Commitment to delivering high-quality customer service.

Skills & Competencies:

- Proactive and methodical approach to diagnosing and resolving technical issues.
- Ability to manage competing priorities and deliver effective outcomes in a fast-paced environment.
- Strong communication and interpersonal skills, with the ability to work effectively with end users, technical teams, and vendors.
- Commitment to continuous improvement, knowledge sharing, and maintaining high-quality documentation.
- Strong focus on service reliability, security, and customer satisfaction.

Qualifications and Certifications:

Depth of demonstrable, hands-on experience is essential. Candidates must demonstrate strong practical capability in supporting, maintaining, and improving Microsoft-based infrastructure services across hybrid environments.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for practical experience and a proven track record of supporting enterprise ICT environments.

Desirable Certifications (including but not limited to):

- Microsoft Certified: Azure Administrator Associate.
- Microsoft Certified: Windows Server Hybrid Administrator Associate.
- Microsoft 365 Certified: Endpoint Administrator Associate.
- Microsoft Certified: Identity and Access Administrator Associate.
- Microsoft Certified Solutions Associate (MCSA) in technology relevant to the role (Associate level).

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, and proven support and delivery of ICT infrastructure services, with certifications considered as supporting evidence of professional development and technical competency.

=====

Lot 3: SharePoint Team

- 1 x SharePoint Programme Manager - Senior Level
- 1 x SharePoint Technical Project Manager - Senior Level
- 1 x SharePoint Infrastructure Engineer - Senior Level
- 1 x SharePoint Solutions Designer (Forms & Business Solutions) - Senior Level
- 1 x Power Platform Developer - Senior Level
- 1 x SharePoint Testing & Quality Assurance Specialist - Intermediate Level
- 1 x SharePoint Administrator - Junior Level

=====

Job Title:

SharePoint Programme Manager – Senior Level

Role Summary:

The Senior SharePoint Programme Manager is responsible for the leadership, governance, and delivery of enterprise SharePoint programmes across on-premises and cloud platforms. The role ensures the successful coordination of multiple inter-related initiatives, including legacy stabilisation, modernisation, migration, and ongoing service improvement, supporting critical business services within a complex enterprise environment.

The successful candidate will demonstrate extensive professional experience and advanced capability in managing large-scale technology programmes, with a strong focus on benefits realisation, stakeholder engagement, and strategic alignment. The role includes overseeing the transition from legacy SharePoint platforms to modern solutions while ensuring continuity of business-critical services and effective management of programme risks and dependencies.

Core Responsibilities:

- Provide programme-level leadership across the SharePoint portfolio, coordinating legacy support, modernisation, migration, and operational improvement initiatives.
- Build and resource the programme delivery team, defining roles, responsibilities, and the overall working arrangements and ways of working.
- Source and onboard new team members as programme needs evolve, and maintain resourcing and continuity plans, including contingency for replacing staff with minimal disruption.
- Lead and coordinate project managers and cross-functional delivery teams, enabling them by removing blockers, resolving areas of confusion, and bringing clarity to programme goals and priorities.
- Define, maintain, and oversee the programme roadmap, timelines, and deliverables, aligned to organisational ICT strategy.
- Manage cross-project dependencies, risks, and issues across multiple delivery streams.
- Establish and maintain programme governance frameworks, controls, and reporting standards.
- Lead engagement with senior stakeholders, including executive sponsors, business owners, and vendors, and report progress, risk, and benefits realisation to governance bodies.

Role Requirements:

Experience

- Minimum 7+ years' demonstrable experience managing complex ICT or digital programmes in large, complex enterprise or public sector environments.
- Proven experience delivering programmes involving SharePoint or comparable enterprise collaboration platforms, evidenced by specific delivered programmes.

Team Formation, Resourcing & Continuity

- Proven experience building and standing up multi-disciplinary delivery teams, defining roles, responsibilities, and working arrangements.
- Demonstrable experience sourcing, onboarding, and integrating new team members as programme needs change.
- Proven experience maintaining resourcing and continuity plans, including contingency and succession arrangements for replacing staff with minimal disruption to delivery.
- Experience leading and coordinating project managers and cross-functional teams across multiple delivery streams.

Programme Delivery & Governance

- Demonstrable experience managing multi-stream programmes with complex cross-project dependencies, risks, and issues.
- Strong experience working within structured programme governance frameworks (such as MSP or equivalent), including controls, reporting, and benefits realisation.
- Proven ability to engage and influence stakeholders at senior and executive level, including sponsors and governance bodies.

Technical Awareness & Oversight

- Strong understanding of legacy platform risks across SharePoint 2013, SPSE, and SharePoint Online, sufficient to evaluate and challenge programme-level technical and migration approaches.
- Awareness of business-critical platform dependencies, including solutions built on InfoWise Ultimate Forms and Sintel Forms.
- Familiarity with OGCI0 / Build to Share guidance and the Public Service ICT Strategy.

Skills & Competencies:

- Facilitative leadership style that builds cohesive teams and keeps cross-disciplinary delivery aligned to shared goals.
- Sound judgement balancing programme pace, scope, and delivery risk across multiple streams.
- Ability to constructively challenge programme-level technical and migration approaches.
- Ability to influence decision-making at senior and executive level.
- Ability to work independently and deliver consistently in an outcome-focused environment.

Qualifications & Certifications:

Depth of demonstrable practical experience is essential. Candidates must demonstrate strong capability in leading, governing, and delivering complex enterprise-scale ICT and SharePoint programmes, ensuring effective stakeholder engagement, programme governance, benefits realisation, and successful delivery across multiple workstreams and organisational functions.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for substantial practical experience and a proven track record of delivering enterprise-scale solutions.

Desirable Certifications (including but not limited to):

- PRINCE2 Practitioner Certificate in Project Management.
- Project Management Professional (PMP).
- Agile Project Management Practitioner (AgilePM).
- Microsoft 365 Certified: Administrator Expert.
- Microsoft 365 Certified: Teams Administrator Associate.
- Microsoft Certified: Information Protection and Compliance Administrator Associate.

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, programme leadership expertise, governance capability, stakeholder engagement, and proven delivery of complex enterprise-scale ICT programmes, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

SharePoint Technical Project Manager – Senior Level

Role Summary:

The Senior SharePoint Technical Project Manager is responsible for the delivery, governance, and successful execution of enterprise SharePoint projects across on-premises and cloud platforms. The role ensures the effective management of complex initiatives, including legacy stabilisation, modernisation, migration, and coexistence, supporting critical business services within a complex enterprise environment.

The successful candidate will demonstrate extensive professional experience and advanced capability in managing large-scale technical projects, with strong emphasis on delivery assurance, risk management, and stakeholder engagement. The role requires sufficient technical depth to evaluate and challenge solution approaches, ensuring that delivery decisions are aligned with platform constraints, business requirements, and operational realities.

The Senior SharePoint Technical Project Manager reports to the SharePoint Manager of the ICT Unit and supports the coordination of the SharePoint team. The role includes assigning tasks based on individual skills, experience, and project requirements, and leading major technical projects as Project Manager within the ICT function.

Core Responsibilities:

- Take ownership of enterprise SharePoint projects spanning legacy stabilisation, modernisation, migration, and coexistence.
- Plan and deliver complex, multi-phase, and multi-year SharePoint roadmaps.
- Manage technical dependencies, risks, issues, and constraints across the project lifecycle and across multiple workstreams.
- Lead stakeholder engagement across ICT teams, business units, vendors, and external service providers.
- Establish and maintain project governance, including reporting, change control, and decision traceability, aligned to organisational ICT strategy.
- Coordinate delivery teams across multiple areas of technical and business expertise, including engineers, developers, testers, infrastructure and solution specialists, and business teams.
- Support and enable delivery teams by removing blockers, resolving areas of confusion, and bringing clarity to goals and priorities.
- Assure delivery in live operational environments, minimising disruption to business-critical services.
- Report progress, performance, and risk to senior sponsors and governance bodies, and support benefits realisation and post-implementation review.

Role Requirements:***Experience***

- Minimum 7+ years' demonstrable experience delivering complex ICT or technical projects in large, complex enterprise or public sector environments.
- Proven experience delivering projects on SharePoint platforms or comparable enterprise collaboration systems, evidenced by specific delivered projects.

Project & Delivery Expertise

- Proven delivery of upgrade, migration, and coexistence initiatives across legacy and modern platforms.
- Demonstrable management of multi-phase delivery with dependencies across multiple workstreams and delivery teams.
- Proven ability to coordinate teams across multiple areas of expertise on large-scale SharePoint migration projects.
- Experience delivering in live operational environments where service continuity is critical, using controlled change to minimise disruption.
- Strong experience working within structured governance, change control, and delivery frameworks
- Practical experience of Agile or hybrid delivery alongside structured, stage-gated delivery.
- Familiarity with OGCIO / Build to Share guidance and the Public Service ICT Strategy.

Technical Awareness & Oversight

- Sufficient technical depth in SharePoint 2013, SPSE, and SharePoint Online to evaluate and challenge solution, upgrade, and migration approaches, including their operational constraints and risks.
- Awareness of business-critical platform dependencies, including environments with solutions built on InfoWise Ultimate Forms and Sintel Forms.

Stakeholder Engagement & Communication

- Proven senior and executive stakeholder engagement, including reporting to governance boards and sponsors.
- Experience managing vendors and external service providers within a delivery project.

Skills & Competencies

- Sound judgement balancing delivery pace, scope, and operational risk in live, business-critical environments.
- Ability to constructively challenge technical, upgrade, and migration proposals on their merits.
- Ability to influence decision-making at senior and executive level.
- Disciplined governance, reporting, and decision-traceability practice.
- Facilitative leadership style that keeps cross-disciplinary teams unblocked, aligned, and focused on shared goals.
- Ability to work independently and deliver consistently in a contract, outcome-focused environment.

Qualifications & Certifications:

Depth of demonstrable practical experience is essential. Candidates must demonstrate strong capability in leading, governing, and delivering complex enterprise-scale ICT and SharePoint projects, ensuring effective stakeholder engagement, project governance, benefits realisation, and successful delivery across multiple workstreams and organisational functions.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for substantial practical experience and a proven track record of delivering enterprise-scale solutions.

Desirable Certifications (including but not limited to):

- PRINCE2 Practitioner Certificate in Project Management.
- Project Management Professional (PMP).
- Agile Project Management Practitioner (AgilePM).
- Microsoft 365 Certified: Administrator Expert.
- Microsoft 365 Certified: Teams Administrator Associate.
- Microsoft Certified: Information Protection and Compliance Administrator Associate.

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, project leadership expertise, governance capability, stakeholder engagement, and proven delivery of complex enterprise-scale ICT projects, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

SharePoint Infrastructure Engineer – Senior Level

Role Summary:

The Senior SharePoint Infrastructure Engineer is responsible for the implementation, administration, support, and continuous improvement of enterprise SharePoint environments across on-premises and cloud platforms. The role ensures the stability, availability, and performance of SharePoint 2013, SharePoint Server Subscription Edition (SPSE), and SharePoint Online environments supporting critical business services within a complex enterprise infrastructure.

The successful candidate will demonstrate extensive professional experience and advanced hands-on expertise across SharePoint platforms, hybrid environments, and enterprise content services. The role includes maintaining legacy SharePoint systems as live production environments while supporting modernisation, upgrade, and coexistence strategies across all platforms.

Core Responsibilities:

- Provide hands-on technical ownership of SharePoint 2013, SPSE, and SharePoint Online across on-premises, hybrid, and cloud platforms.
- Implement, configure, and support SharePoint farms, service applications, and site architecture across all environments.
- Perform advanced administration, maintenance, and troubleshooting across legacy and modern SharePoint platforms.
- Maintain high availability, performance, and reliability, including monitoring, optimisation, and remediation.
- Support business-critical legacy solutions, including those built on InfoWise Ultimate Forms and Sintel Forms.
- Deliver upgrade initiatives from SharePoint 2013 to SPSE and migration initiatives to SharePoint Online, using tools such as Sharegate.
- Manage hybrid and coexistence environments operating multiple SharePoint platforms in parallel.
- Implement and maintain backup, restore, recovery, and rollback procedures for all SharePoint platforms.
- Develop and maintain PowerShell automation for platform administration and operational efficiency.
- Apply structured change control across high-impact production environments, and provide advanced incident management, troubleshooting, and root cause analysis.
- Provide technical leadership through engineering standards, automation, and documentation, producing work that keeps the estate supportable by others.

Role Requirements:***Experience***

- Minimum 7+ years' demonstrable hands-on experience engineering and administering SharePoint platforms in large, complex enterprise environments, evidenced by specific delivered work.
- Advanced hands-on administration of SharePoint 2013, including service applications, site architecture, search, user profiles, security, permissions, and troubleshooting.
- Hands-on administration of SharePoint Server Subscription Edition (SPSE), including upgrade and migration scenarios from SharePoint 2013.
- Demonstrable management of SharePoint Online, including tenant configuration, governance, and hybrid connectivity.

- Proven experience designing and operating hybrid and coexistence environments that run on-premises and cloud SharePoint platforms in parallel.

Legacy Environment Expertise

- Deep, demonstrable knowledge of legacy SharePoint 2013 and SPSE environments maintained as live production systems.
- Experience supporting business-critical legacy solutions, including InfoWise Ultimate Forms and Sintel Forms, with a clear understanding of the hidden dependencies and failure modes of legacy platforms.

Platform Operations & Resilience

- Strong, specific experience of backup, restore, recovery, and rollback scenarios for SharePoint platforms.
- Strong PowerShell scripting capability for SharePoint automation and administration.
- Experience using migration and assessment tools, including, but not limited to, Sharegate.
- Understanding of how SharePoint integrates with wider ICT infrastructure, including identity, networking, and storage services.
- Experience operating within structured, change-controlled, and compliance-driven production environments.
- Experience integrating SharePoint with Azure-based infrastructure and services.

Skills & Competencies:

- Strong analytical and diagnostic capability in high-availability production environments.
- Sound judgement balancing legacy platform stability with modernisation and migration.
- Disciplined change-control and operational rigour in high-impact environments.
- Disciplined documentation and standards practice, keeping the estate supportable by others.
- Ability to work independently and deliver consistently in a contract, outcome-focused environment.

Qualifications & Certifications:

Depth of demonstrable practical experience is essential. Candidates must demonstrate strong capability in implementing, administering, supporting, troubleshooting, and optimising enterprise SharePoint environments across on-premises, hybrid, and cloud platforms.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for substantial practical experience and a proven track record of delivering enterprise-scale solutions.

Desirable Certifications (including but not limited to):

- Microsoft 365 Certified: Teamwork Administrator Associate.
- Microsoft Certified: Collaboration Communications Systems Engineer Associate.
- Microsoft 365 Certified: Enterprise Administrator Expert.
- Microsoft Certified Solutions Associate (MCSA): SharePoint.
- Microsoft Certified Solutions Expert (MCSE): Productivity.

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, and proven delivery, administration, support, and optimisation of enterprise

SharePoint environments, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

SharePoint Solutions Designer (Forms & Business Solutions) – Senior Level

Role Summary:

The Senior SharePoint Solutions Designer (Forms & Business Solutions) is responsible for the design, maintenance, and continuous improvement of enterprise SharePoint-based business solutions across on-premises and cloud platforms. The role ensures the stability, integrity, and evolution of solutions built on SharePoint 2013, SharePoint Server Subscription Edition (SPSE), and SharePoint Online, supporting critical business processes within a complex enterprise environment.

The successful candidate will demonstrate extensive professional experience and advanced hands-on expertise in designing and supporting SharePoint solutions, with particular focus on legacy forms and workflow technologies. The role includes maintaining continuity of long-standing solutions built on InfoWise Ultimate Forms and Sintel Forms while supporting the development of modern equivalents that preserve data integrity and business logic.

Core Responsibilities:

- Design, build, and maintain complex SharePoint forms and workflow solutions across SharePoint 2013, SPSE, and SharePoint Online, including multi-stage approvals, data capture, and conditional logic.
- Take operational ownership of the existing Sintel Forms and InfoWise Ultimate Forms portfolio, ensuring continuity of business-critical processes.
- Analyse and safely modify live solutions with embedded business rules, dependencies, and integrations, making controlled changes with minimal regression risk.
- Diagnose and resolve production issues such as workflow failures, data inconsistencies, and form performance problems, identifying root causes and implementing stable fixes.
- Work with legacy forms and workflow technologies, including InfoPath and SharePoint Designer workflows.
- Deliver incremental improvements or partial redesigns where full replacement is not feasible, and implement modern equivalents (Power Apps, Power Automate) where appropriate, preserving existing business logic and data structures.
- Engage stakeholders to elicit and clarify requirements, particularly where processes are undocumented, and produce clear, structured solution and operational handover documentation.

Role Requirements:***Experience***

- Minimum 7+ years' demonstrable experience delivering SharePoint-based forms and workflow solutions in large, complex enterprise or public sector environments.
- Demonstrable delivery across SharePoint 2013, SPSE, and SharePoint Online, including the edition and behaviour differences that affect form configurations between on-premises and online.

Forms Platform Expertise: Sintel Forms & InfoWise Ultimate Forms

- Proven, hands-on, expert-level experience with both products, evidenced by specific solutions personally designed, configured, and supported.
- Design of complex multi-tab and multi-section forms with conditional visibility, dynamic layouts, and responsive grid layouts.
- Authoring of declarative business logic (validation rules, calculated fields, mandatory or show and hide behaviour) across both products' rules engines.

- Custom JavaScript extension, notably in Sintel Forms, for behaviour beyond the native engine, including dynamic validation and character and word-limit enforcement on rich-text fields.
- Configuration of automation and Actions (InfoWise), cross-list relationships, lookups, cascading dropdowns, repeating tables, alerts, and print and export.
- Practical understanding of both products' limitations, failure modes, and behaviour under change in live environments.
- Ability to reverse-engineer undocumented legacy configurations and preserve business logic and data integrity during change.

Wider Technical & Delivery Experience

- Expert working knowledge of InfoPath and SharePoint Designer workflows.
- Evidence of resolving production issues on business-critical, high-dependency systems, including root-cause diagnosis and stable remediation.
- Sound assessment of the risks of partial redesign and platform coexistence in interdependent solutions, with practical mitigation.
- Proven ability to engage business users, interpret unclear requirements, and deliver working solutions without full specifications.
- Practical working knowledge of modern alternatives (Power Apps, Power Automate, modern SharePoint) and phased modernisation approaches.
- Familiarity with OGCIO / Build to Share guidance and the Public Service ICT Strategy.

Skills & Competencies:

- Sound judgement on when to retain, modify, or partially replace existing components.
- Ability to make safe, controlled changes to live systems with minimal regression risk.
- Ability to work independently and deliver consistently in a contract, outcome-focused environment.
- Structured documentation discipline, ensuring solutions remain supportable and maintainable by others.

Qualifications & Certifications:

Depth of demonstrable practical experience is essential. Candidates must demonstrate strong capability in designing, configuring, supporting, troubleshooting, and modernising enterprise SharePoint forms, workflows, and business solutions across on-premises and cloud platforms.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for substantial practical experience and a proven track record of delivering enterprise-scale solutions.

Desirable Certifications (including but not limited to):

- Microsoft Certified: Power Platform Functional Consultant Associate.
- Microsoft Certified: Power Platform Developer Associate.
- Microsoft 365 Certified: Enterprise Administrator Expert.
- Microsoft certifications relevant to SharePoint, Power Platform, collaboration, or administration.

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, and proven delivery, support, modernisation, and optimisation of enterprise

SharePoint forms, workflows, and business solutions, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

Power Platform Developer – Senior Level

Role Summary:

The Senior Power Platform Developer is responsible for the design, development, and continuous improvement of enterprise business solutions using Microsoft Power Platform technologies. The role ensures the delivery of secure, scalable, and well-governed solutions utilising Power Apps, Power Automate, Dataverse, and Power BI, supporting critical business processes within a modern Microsoft 365 environment.

The successful candidate will demonstrate extensive professional experience and advanced hands-on expertise across Power Platform development, application integration, and solution governance. The role includes modernising legacy SharePoint forms and workflows, including solutions built on InfoWise Ultimate Forms and Sintel Forms, while ensuring continuity of business logic, data integrity, and service reliability.

Core Responsibilities:

- Design, develop, and maintain enterprise Power Platform solutions using Power Apps (canvas and model-driven), Power Automate, Dataverse, and Power BI.
- Replace and modernise legacy SharePoint forms and workflow solutions, including those built on InfoWise Ultimate Forms and Sintel Forms, preserving business logic and data integrity.
- Integrate Power Platform solutions with SharePoint Online, SPSE, SharePoint 2013 where required, and broader Microsoft 365 and Azure services.
- Implement Application Lifecycle Management (ALM) practices, including solution packaging, source control, and environment management.
- Define and apply governance, security, and Data Loss Prevention (DLP) policies across the Power Platform.
- Develop integrations using custom connectors, REST APIs, and Azure-based services.
- Engage business stakeholders to gather requirements and translate business processes into secure, performant, and maintainable solutions.
- Provide advanced troubleshooting, incident resolution, and performance optimisation for production solutions.
- Provide technical leadership through standards, reusable patterns, and Centre of Excellence (CoE) practices, and produce clear documentation so solutions can be maintained and extended by others.

Role Requirements:

Experience

- Minimum 7+ years' demonstrable experience in software or application development, including significant hands-on Power Platform delivery in large, complex, and governed enterprise environments.
- Proven delivery of enterprise Power Platform solutions, evidenced by specific delivered applications and integrations.

Power Platform Development Expertise

- Advanced hands-on experience with Power Apps (canvas and model-driven), Power Automate, Dataverse, and Power BI.
- Proven experience integrating Power Platform with SharePoint Online and Microsoft 365 services, and developing integrations using REST APIs, custom connectors, and Azure services.
- Experience modernising legacy SharePoint-based solutions, including InfoPath, SharePoint Designer workflows, InfoWise Ultimate Forms, and Sintel Forms, while preserving business logic and data integrity.
- Strong command of Power Platform governance, ALM, environment strategy, and security, including DLP policies.
- Strong data modelling, application design, and solution architecture skills.

Wider Development & Delivery Experience

- Advanced troubleshooting and performance optimisation across application and integration layers, including support of production systems.
- Proven ability to engage stakeholders and translate business processes into robust technical solutions.
- Experience contributing to a Power Platform Centre of Excellence (CoE).
- Familiarity with OGCIO / Build to Share guidance and the Public Service ICT Strategy.

Skills & Competencies:

- Sound judgement balancing low-code and pro-code approaches for scalable, maintainable solutions.
- Strong analytical and problem-solving capability across application and integration layers.
- Ability to balance modernisation with business continuity.
- Disciplined documentation and standards practice, ensuring solutions remain supportable by others.
- Ability to work independently and deliver consistently in a contract, outcome-focused environment.

Qualifications & Certifications:

Depth of demonstrable practical experience is essential. Candidates must demonstrate strong capability in designing, developing, integrating, securing, and supporting enterprise Power Platform solutions, including Power Apps, Power Automate, Dataverse, and Power BI, within complex and governed enterprise environments.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and will be considered as evidence supporting and validating technical knowledge and expertise. However, certifications do not replace the requirement for substantial practical experience and a proven track record of delivering enterprise-scale solutions.

Desirable Certifications (including but not limited to):

- Microsoft Certified: Power Platform Developer Associate (PL-400).
- Microsoft Certified: Power Platform Functional Consultant Associate (PL-200).
- Microsoft Certified: Power Platform Solution Architect Expert (PL-600).
- Microsoft Certified: Power Platform Fundamentals (PL-900).

Candidates must be able to demonstrate practical experience across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, depth of experience, technical expertise, solution development skills, stakeholder engagement, and proven delivery of enterprise Power Platform solutions, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

SharePoint Testing & Quality Assurance Specialist – Intermediate Level

Role Summary:

The SharePoint Testing & Quality Assurance Specialist is responsible for providing structured, risk-based testing and assurance across enterprise SharePoint environments spanning SharePoint 2013, SharePoint Server Subscription Edition (SPSE), and SharePoint Online. The role ensures that changes, upgrades, and migrations are validated effectively to protect the integrity, reliability, and continuity of business-critical services.

The successful candidate will demonstrate professional experience and strong technical capability in testing SharePoint-based solutions across legacy and modern platforms. This includes supporting assurance activities for solutions built on InfoWise Ultimate Forms and Sintel Forms, where complex dependencies and legacy behaviours introduce elevated risk. It contributes to ensuring quality, stability, and confidence in delivery across change and operational activities.

Core Responsibilities:

- Plan, design, and execute structured, risk-based testing across SharePoint 2013, SPSE, and SharePoint Online.
- Validate the functionality, resilience, and accessibility of forms solutions built on InfoWise Ultimate Forms and Sintel Forms, including the forms and customisations produced by development teams.
- Design and execute regression testing for legacy SharePoint forms and workflow solutions before and after change.
- Test forms behaviour, validation rules, permissions, access controls, and data integrity across the change lifecycle.
- Test integrations between SharePoint and modern solutions, including Power Platform replacements.
- Support and coordinate user acceptance testing (UAT) for business-critical forms and systems.
- Develop and maintain test plans, test cases, traceability matrices, and defect records, and verify data integrity through pre- and post-migration checks.
- Provide independent, evidence-based assurance reporting, and collaborate with development, infrastructure, and business teams on issue resolution.

Role Requirements:***Experience***

- Minimum 4+ years' demonstrable experience in testing or quality assurance within enterprise ICT environments.
- Proven experience testing SharePoint solutions across SharePoint 2013, SPSE, and SharePoint Online, evidenced by specific testing engagements.

Forms Testing & Assurance: InfoWise Ultimate Forms & Sintel Forms

- Hands-on experience testing solutions built on InfoWise Ultimate Forms and Sintel Forms, including the forms, rules, validation, and customisations produced by a forms development function.
- Functional testing of complex forms behaviour, including conditional logic, validation rules, calculated fields, and repeating or multi-section structures.
- Resilience testing of forms, including failure modes, error handling, edge-case validation, and behaviour under change in live environments.
- Accessibility testing of forms against recognised standards such as WCAG, including keyboard navigation, focus visibility, colour contrast, and screen-reader compatibility.

Wider Testing & Delivery Experience

- Strong understanding of SharePoint forms, workflows, permissions, and data structures, and the risks introduced by fragile, business-critical legacy solutions.
- Experience designing and executing regression and integration testing, including SharePoint-to-Power Platform integrations.
- Demonstrable experience supporting upgrade and migration testing, including pre- and post-migration data validation.
- Experience using test management and defect tracking tools, with structured test planning, traceability, and defect management.
- Familiarity with OGCIO / Build to Share guidance and the Public Service ICT Strategy.

Skills & Competencies:

- Strong analytical, risk-based approach to prioritising test coverage for high-risk and complex scenarios.
- Methodical attention to detail and documentation discipline.
- Disciplined adherence to structured change control and quality assurance processes.
- Clear, evidence-based reporting of findings and risks to technical and business audiences.
- Ability to work independently and deliver consistently in a contract, outcome-focused environment.

Qualifications & Certifications:

Depth of demonstrable testing and quality assurance experience is strongly preferred. Candidates must demonstrate practical capability in planning, executing, and reporting structured testing activities across enterprise SharePoint environments, including regression testing, migration assurance, forms testing, integration testing, and user acceptance testing support.

Professional certifications, formal accreditation, and recognised vendor-certified training are desirable and may be considered as supporting evidence of knowledge and professional development. However, certifications are not mandatory and do not replace the requirement for relevant practical experience and a proven ability to deliver effective testing and quality assurance outcomes.

Desirable Certifications (including but not limited to):

- ISTQB Certified Tester Foundation Level (CTFL).
- ISTQB Advanced Level certifications.
- Microsoft 365 certifications relevant to SharePoint, collaboration, or administration.

Candidates must be able to demonstrate practical experience across the technologies, testing methodologies, and quality assurance disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated capability, relevant experience, testing and quality assurance expertise, problem-solving ability, and proven delivery of effective testing outcomes within enterprise SharePoint environments, with certifications considered as supporting evidence of professional development and technical competency.

=====

Job Title:

SharePoint Administrator – Junior Level

Role Summary:

The SharePoint Administrator provides operational support for enterprise SharePoint environments across on-premises and cloud platforms. The role supports the day-to-day administration of SharePoint 2013, SharePoint Server Subscription Edition (SPSE), and SharePoint Online environments, ensuring the effective operation of business-critical collaboration services.

The successful candidate will demonstrate early professional experience and developing technical capability across SharePoint platforms and Microsoft 365 services. Experience supporting forms solutions, including InfoWise Ultimate Forms and Sintel Forms, is a particularly strong attribute and the role provides structured exposure to legacy and modern SharePoint environments, supporting skills development through operational support activities.

Core Responsibilities:

- Support senior engineers and administrators in the day-to-day operation and maintenance of SharePoint platforms.
- Perform routine administration tasks across SharePoint 2013, SPSE, and SharePoint Online.
- Manage user permissions and access requests in line with established processes and governance controls.
- Provide first-line and second-line support for SharePoint incidents, service requests, and user queries.
- Support business-critical solutions, including those built on InfoWise Ultimate Forms and Sintel Forms.
- Assist with testing, data validation, and post-change verification during migration and upgrade activities.
- Monitor system performance, availability, and service health, perform troubleshooting, and escalate complex issues to senior engineers.
- Support hybrid environments running multiple SharePoint platforms in parallel.
- Contribute to technical documentation, operational procedures, and knowledge base articles.
- Follow structured change control and operational processes within a regulated environment.

Role Requirements:

- Minimum 1 to 3 years' professional experience supporting SharePoint or Microsoft 365 environments.
- Solid working knowledge of SharePoint Online and on-premises SharePoint (2013 or SPSE), including site administration, permissions, and access control, at a level approaching intermediate.
- Sound understanding of the wider Microsoft 365 ecosystem, including Teams, OneDrive, and Power Platform.
- Experience supporting forms and business solutions, including InfoWise Ultimate Forms and Sintel Forms (a particularly strong attribute).
- Experience of testing, data validation, and post-change verification during migration or upgrade activities.
- Working understanding of SharePoint infrastructure and operations, including service monitoring, availability, and troubleshooting.
- Sound understanding of SharePoint governance, security, and compliance concepts.
- Working knowledge of PowerShell scripting for administrative tasks, or the ability to extend scripting capability under guidance.

- Ability to follow structured change control and operational processes, and to work effectively under the direction of senior engineers.
- Awareness of modernisation approaches, such as moving SharePoint forms and workflows to Power Platform.
- Familiarity with OGCIO / Build to Share guidance and the Public Service ICT Strategy.

Skills & Competencies:

- Methodical, detail-oriented approach to permissions, configurations, and troubleshooting.
- Sound judgement on when to resolve at first line and when to escalate to senior engineers.
- Clear communication and effective end-user support skills.
- Strong organisational and time-management skills.
- Ability to work reliably within established processes and under direction.

Qualifications & Certifications:

Practical, hands-on experience is important. Candidates should be able to demonstrate experience supporting, maintaining, and troubleshooting SharePoint and Microsoft 365 collaboration services within enterprise or similar environments.

Professional certifications, formal training, and recognised vendor-accredited courses are desirable and will be considered as evidence of technical knowledge and commitment to professional development. Equivalent practical experience will also be considered.

Desirable Certifications (including but not limited to):

- Microsoft 365 Certified: Fundamentals.
- Microsoft Certified: Azure Fundamentals.

Candidates should be able to demonstrate practical experience and a willingness to develop their skills across the technologies and disciplines listed within this specification.

Assessment of suitability will be based primarily on demonstrated technical capability, relevant experience, problem-solving skills, and the ability to support and maintain SharePoint and Microsoft 365 collaboration services, with certifications considered as supporting evidence of technical knowledge and professional development.

=====

RESOURCE MANAGEMENT

Where indicated in the TRD, Tenderers must submit a comprehensive Resource Management Proposal in respect of each Lot for which they are submitting a tender, outlining how they will recruit, assign, manage, and retain appropriately skilled personnel for the duration of the contract. Tenderers should provide sufficient detail to demonstrate the effectiveness, robustness and suitability of their proposed resource management arrangements for delivery of the services, and where appropriate, explain how the arrangements will be applied to each lot tendered for. This proposal must include:

- Workforce planning and resource allocation arrangements;
- Measures for retaining key personnel and reducing turnover in critical roles, including employee engagement, career development and succession planning arrangements;
- Measures to ensure continuity of service, including cover for planned and unplanned leave/absences;
- Strategies to maintain consistent service levels and minimise disruption;
- Mobilisation, onboarding and transition arrangements, including measures to minimise service disruption and maintain operational continuity;
- Processes for supervision, performance management, and ongoing professional development;
- Succession planning and contingency arrangements for replacement of personnel;
- Measures to ensure knowledge retention and effective transfer within the resource pool, including how technical knowledge, operational procedures, service history and business context will be documented, retained and transferred throughout the contract lifecycle.

The Department is open to innovative approaches to resource management and service continuity.

If bidding for multiple Lots, the Proposals must describe how the Tenderer will ensure that it has sufficient capacity, management capability and suitably qualified personnel to deliver all lots concurrently.

Resource Performance and Replacement

All proposed personnel will be subject to an initial probationary period of three (3) months. Where performance is deemed unsatisfactory, the Contracting Authority reserves the right to terminate the assignment. The successful Tenderer must be capable of proposing suitably qualified replacement candidates promptly for consideration.

The service provider must demonstrate capacity to respond to vacancies or additional resource requirements during the contract term. Replacement or additional personnel must:

- Possess the technical skills, and relevant experience that are equivalent to or exceed those specified for the role in this RFT;
- Demonstrate experience in comparable roles and environments of similar scale, complexity, and criticality;
- Be available for interview within five (5) working days of request;
- Successfully complete all required security clearance procedures; and
- Be capable of commencing duties within eight (8) weeks of notification.

The service provider will be responsible for the ongoing performance management of all assigned personnel, including regular performance reviews as agreed with the Department. Where performance is deemed unsatisfactory, the provider must promptly propose suitable replacement

personnel. No change shall be made to the identity of the Key Personnel without the prior written consent of the Contracting Authority.

Security and Compliance

All personnel must be willing to:

- Undergo Civil Service security clearance procedures;
- Sign the Official Secrets Act; and
- Comply with all relevant Departmental policies.

The service provider is responsible for conducting appropriate background checks prior to assignment. The Department reserves the right to refuse any candidate following clearance procedures and will not provide justification for such decisions.

Customer Service and Quality Assurance

Customer service is an essential requirement for all personnel, in addition to technical competence. Tenderers must outline their approach to ensuring personnel maintain a strong customer focus in all interactions with Department staff.

Tenderers must also demonstrate a commitment to delivering high-quality services and provide evidence of established service quality assurance frameworks and management systems.

Resource Stability and Continuity

The successful Tenderer must:

- Confirm that no assigned personnel will be withdrawn without the prior written agreement of the Department, and subject to a minimum notice period of one (1) month;
- Ensure that all personnel assigned under this contract provide a minimum of one (1) months' notice prior to cessation of duties to support service continuity.

Handover and Transition

At the conclusion of the contract, or in the event of transition to another provider, the successful Tenderer will be required to participate fully in a structured handover process. This process must be conducted in a professional manner, ensuring continuity of service and protecting the best interests of the Department.

The Contractor will be required to provide all reasonable assistance necessary to enable the continued delivery of the services following expiry or termination of the contract. The Contractor will be required to maintain appropriate documentation throughout the Contract to facilitate an efficient transition and shall not defer the preparation of handover documentation until the end of the Contract.

Tenderers must outline their proposed approach to knowledge transfer and transition management as part of their submission.

Employment Responsibilities

The employment relationship between the service provider and assigned personnel remains the sole responsibility of the provider. The provider must ensure compliance with all statutory employment obligations, including taxation, statutory deductions, and reporting requirements, and must confirm annually that these obligations have been met.

Data Protection

In performing the Services, the Contractor will be required to comply with all applicable data protection legislation and the data protection provisions of the contract.

Appendix 2: Pricing Schedule

Tenderers must complete the Pricing Schedule, set out in Appendix 2 Pricing Schedule, for each lot for which they are submitting a tender. (Attached separately in Excel format and available in the Tender Documents section of the CFT on www.eTenders.gov.ie).

All costs associated with the delivery of the services must be included, with reference to the Requirements and Specifications outlined in Appendix 1.

Tenderers should provide pricing for each role, within each Lot for which they are submitting a tender, based on an 8-hour working day, and 232 contract days for the initial 12-month period of the Contract, and the number of team members specified.

Tenderers should also provide an hourly rate for any additional services required outside normal office hours, and details of any other relevant costs not included elsewhere in the pricing schedule.

All prices must be quoted in euro (€), exclusive of VAT.

Tenderers must complete every mandatory pricing field. Blank cells may be treated as non-compliant unless otherwise stated.

No minimum volume of work is guaranteed under the contract.

Appendix 3: Tenderers' Statement

[Tenderers shall complete and return the following form of Tenderers' Statement printed on the Tenderers' headed notepaper and signed by the Tenderer.]

TENDERERS' STATEMENT

TO: Minister for Foreign Affairs and Trade (the "Contracting Authority")

RE: Request for Tenders for the Supply of External ICT Technical Support Services

Having examined your Request for Tenders (the "RFT") including the Instructions to Tenderers, the Selection and Award Criteria, the Requirements and Specifications, and the Terms and Conditions of the Services Contract, we hereby agree and declare the following:

1. We understand the nature and extent of the Services required to be delivered as described in Requirements and Specifications at Appendix 1 to the RFT.
2. We accept all of the Terms and Conditions of the RFT, the Services Contract and the Confidentiality Agreement and agree if awarded a Services Contract to execute the Services Contract at Appendix 5 to the RFT and the Confidentiality Agreement at Appendix 6 to the RFT.
3. We accept all the Selection and Award Criteria as set out in Part 3 of the RFT.
4. We agree to provide the Contracting Authority with the Services in accordance with the RFT and our Tender.
5. We agree that, if awarded any Services Contract, we shall, in the performance of such contract, comply with all applicable obligations in the field of environmental, social and labour law.
6. We confirm that we have complied with all requirements as set out at Part 2 of the RFT.
7. We confirm that all prices quoted in our Tender will remain valid for the period of time commencing from the Tender Deadline, as specified at paragraph 2.10.3 of the RFT.
8. We shall, if awarded any Services Contract under the RFT, have in place on the Effective Date of the Services Contract all insurances (if any) as required by paragraph 2.21.1 of the RFT.
9. We confirm that all Data Subjects whose Personal Data is provided in our Tender have consented to the processing of such Personal Data by us, the Contracting Authority, the Evaluation Team and the supplier of the etenders.gov.ie website, for the purposes of our participation in this Competition or that we otherwise have a legal basis for providing such Personal Data to the Contracting Authority for the purposes of our participation in this Competition and that we will provide evidence of such consent and / or legal basis to the Contracting Authority upon request.

10. We do not within the category of prohibited economic operators identified in Regulation (EU) No 833/2014 of 31 July 2014 (as amended by EU Regulation 2022/576 or any subsequent amendments to same).
11. The origin of goods connected to our tender, if any, are not subject to the prohibitions set out in Regulation (EU) No 833/2014 (as amended by EU Regulation 2022/576 or any subsequent amendments to same).
12. The subcontractor(s) on whose capacity we rely as part of our Tender (where the value of that subcontract exceeds 10% of the value of the Services Contract) does not come within the category of prohibited economic operators identified in Regulation (EU) No 833/2014 of 31 July 2014 (as amended by EU Regulation 2022/576 or any subsequent amendments to same).

SIGNED

Company

(Authorised Signatory)

Print name

Address

Date

Appendix 4: Declaration as to Personal Circumstances of Tenderer

Re: Request for Tenders for the Provision of External ICT Technical Support Services

NAME: [Click here and insert name]

ADDRESS: [Click here and insert address]

I, [Click here and insert name of Declarant], having been duly authorised by [Click here and insert name of entity] sincerely declare that [Click here and insert name of entity] itself or any person who has is a member of the administrative, management or supervisory body of [Click here and insert name of entity] or has powers of representation, decision or control in [Click here and insert name of entity]:

- (a) Has never been the subject of a conviction for participation in a criminal organisation, as defined in Article 2 of Council Framework Decision 2008/841/JHA.
- (b) Has never been the subject of a conviction for corruption, as defined in Article 3 of the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union and Article 2(1) of Council Framework Decision 2003/568/JHA as well as corruption as defined in the national law of the Contracting Authority or [Click here and insert name of entity].
- (c) Has never been the subject of a conviction for fraud within the meaning of Article 1 of the Convention on the protection of the European Communities' financial interests.
- (d) Has never been the subject of a conviction for terrorist offences or offences linked to terrorist activities, as defined in Articles 1 and 3 of Council Framework Decision 2002/475/JHA respectively, or for inciting or aiding or abetting or attempting to commit an offence, as referred to in Article 4 of that Framework Decision.
- (e) Has never been the subject of a conviction for money laundering or terrorist financing, as defined in Article 1 of Directive 2005/60/EC of the European Parliament and of the Council.
- (f) Has never been the subject of a conviction for child labour and other forms of trafficking in human beings as defined in Article 2 of Directive 2011/36/EU of the European Parliament and of the Council.
- (g) Is not in breach and has not breached its obligations relating to the payment of taxes or social security contributions.

I understand and acknowledge that the provision of inaccurate or misleading information in this declaration may lead to my business/firm/company/partnership being excluded from participation in this or future tenders, and I make this solemn declaration conscientiously believing the same to be true and by virtue of the Statutory Declarations Act, 1938. This declaration is made for the benefit of the Contracting Authority.

Signature of Declarant

Name of Declarant in print or block capitals

Declared before me by _____ who is personally known to me

(or who is identified to me by _____ who is personally known to me)

at _____ this _____ day of _____ 20__

(signed)

Practising Solicitor/Commissioner for Oaths

Appendix 5: Services Contract

Minister for Foreign Affairs and Trade

and

[Insert successful Tenderer's full legal name]

AGREEMENT

Relating to the provision of Services pursuant to

Request for Tenders for the provision of External ICT Technical Support Services

THIS AGREEMENT IS MADE ON THE [DATE E.G. 2ND] DAY OF [MONTH] 20[YEAR] BETWEEN:

Minister for Foreign Affairs and Trade, of [address] (“the Client”);

and

[Contractor's full legal name], of [address] (“the Contractor”)

(each a “Party” and together “the Parties”).

WHEREAS:

- A. By Request for Tender entitled “Insert title of RFT” advertised in the supplement to the Official Journal of the European Union, OJEU Notice Number [] of [] dated insert date of RFT (“the RFT”) the Contracting Authority invited tenders from economic operators (“Tenderers”) for the provision of the services described in Appendix 1 to the RFT (the “Services”). References to the RFT shall include any clarifications issued by the Contracting Authority via the messaging facility on www.etenders.gov.ie between [insert date] and [insert date] (the “RFT Clarifications”). The RFT (including the RFT Clarifications) is hereby incorporated by reference into this Agreement.
- B. The Contractor submitted a response to the RFT dated [insert date of Tender] (“the Submission”). References to the Submission shall include any clarifications issued by the Contractor in writing to the Contracting Authority between [insert date] and [insert date] (the “Submission Clarifications”). The Submission (including the Submission Clarifications) is hereby incorporated by reference into this Agreement.

IT IS HEREBY AGREED AS FOLLOWS:

1. This Agreement consists of the following documents, and in the case of conflict of wording, in the following order of priority:
 - i. This Agreement and Schedules A to E attached hereto;
 - ii. The RFT;
 - iii. The Submission.
2. The Contractor agrees to provide the Services described in Schedule B (“the Services”) to the Client in accordance with this Agreement (“Agreement”). Schedule B details the nature, quality, time of delivery, key personnel and functional specifications of the Services in accordance with the RFT and the Submission (“the Specification”).
3. Subject to the terms and conditions of this Agreement, the Client agrees to pay to the Contractor the charges as stipulated in Schedule C (“the Charges”). The Charges are exclusive of VAT which shall be due at the rate applicable on the date of the VAT invoice.

4. For the purposes of this Agreement, the Client's Contact is [name of contact person] of [address of contact person]; the Contractor's Contact is [Contractor contact name] of [Contractor contact address].
5. This Agreement shall take effect on the date of this Agreement ("the Effective Date") and shall expire on [Insert date], unless it is otherwise terminated in accordance with the provisions of this Agreement or otherwise lawfully terminated or otherwise lawfully extended as agreed between the Parties ("the Term").

The Client reserves the right to extend the Term for a period or periods of up to 12 months with a maximum of two such extensions permitted subject to its obligations at law
6. Unless otherwise specified herein, a defined term used in this Agreement shall have the same meaning as assigned to it in the RFT.
7. Headings are included for ease of reference only and shall not affect the construction of this Agreement.
8. Unless the context requires otherwise, words in the singular may include the plural and vice versa.
9. References to any statute, enactment, order, regulation or other legislative instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended, unless specifically indicated otherwise.
10. In the event that any ambiguity or question of intent or interpretation arises in relation to this Agreement, this Agreement shall be construed as if drafted jointly by the Parties and no presumption or burden of proof shall arise favouring or disfavouring any Party by virtue of the authorship of any of the provisions of this Agreement.

SIGNED for and on behalf of the Client _____ (being a duly authorised officer)	SIGNED for and on behalf of the Contractor _____
Witness	Witness

Schedule A: Terms and Conditions

1. CONTRACTOR'S OBLIGATIONS

- A. The Contractor undertakes to act with due care, skill and diligence in the provision of the Services and generally in the carrying out of its obligations under this Agreement and in the appointment, monitoring and retention of its agents and Subcontractors. The Contractor shall require its agents and Subcontractors to exercise due care, skill and diligence in the provision of the Services and generally in the carrying out of obligations allocated by the Contractor to its agents and Subcontractors under this Agreement.
- B. In consideration of the payment of the Charges and subject to clause 3 the Contractor shall:
1. provide the Services in accordance with the Specification, the RFT, the Client's directions and the terms of this Agreement;
 2. comply with and implement any policies, guidelines and/or any project governance protocols issued by the Client from time to time and notified to the Contractor in writing;
 3. comply with all local security and health and safety arrangements as notified to it by the Client; and
 4. provide the Services in accordance with good industry practice and comply with all applicable laws including but not limited to all obligations in the field of environmental, social and labour law that apply at the place where the Services are provided, that have been established by EU law, national law, collective agreements and by international, environmental, social and labour law listed in Schedule 7 of the European Union (Award of Public Authority Contracts) Regulations 2016 (Statutory Instrument 284 of 2016) (the "Regulations") . The Contractor shall be responsible for compliance with all statutory requirements of an employer and without prejudice to the generality of the foregoing shall be solely responsible in law for the employment, remuneration, taxes, immigration and work permits of all personnel retained for the purposes of complying with this Agreement.
- C. The Contractor is deemed to be the prime contractor under this Agreement and the Contractor assumes full responsibility for the discharge of all obligations under this Agreement and shall assume all the duties, responsibilities and obligations associated with the position of prime contractor. The Contractor as prime contractor under the Submission hereby assumes liability for its Subcontractors and shall ensure that its Subcontractors shall comply in all respects with the relevant terms of this Agreement, including but not limited to clause 1B(4) above, to the extent that it or they are retained by the Contractor. Subject to clause 14, the Contractor shall notify the Client as soon as possible of any changes to the name, contact details and legal representatives of its Subcontractors.
- D. Without prejudice to clause 1C, where the Client becomes aware that any of the exclusion grounds set out in Regulation 57 of the Regulations apply to any Subcontractor, the Client reserves the right to require the Contractor to immediately replace such Subcontractor and the Contractor shall comply with such requirement. The Contractor shall include in every sub-contract a right for the Contractor to terminate the sub-contract where any of the

exclusion grounds apply to the Subcontractor and a requirement that the Subcontractor, in turn, includes a provision having the same effect in any sub-contract which it awards.

- E. During this Agreement the Contractor shall be an independent contractor and not the employee of the Client. Neither Party shall have any authority to bind or commit the other. Nothing herein shall be deemed or construed to create a joint venture, partnership, and/or fiduciary or other relationship between the Parties for any purpose. The officers, employees or agents of the Contractor are not and shall not hold themselves out to be (and shall not be held out by the Contractor as being) servants or agents of the Client for any purposes whatsoever.
- F. The Client acknowledges that the Contractor may from time to time be dependent on the Client to facilitate the Contractor in the carrying out of its duties under this Agreement. The Client agrees to use its reasonable endeavours to so facilitate the Contractor within the timescales and in the manner agreed by it in writing in accordance with clause 10.
- G. The Contractor agrees that any information relating to this Agreement and / or the performance of this Agreement may be passed by the Client to the Office of Government Procurement (“OGP”) and that the OGP may use this information in the analysis and reporting of spend data including the preparation and publishing of reports.
- H. The Contractor shall comply with all applicable obligations arising pursuant to the European Communities (Protection of Employees’ Rights on Transfer of Undertakings) Regulations 2003 (S.I. No. 131 of 2003) and Council Directive 2001/23/EC (together the “TUPE Regulations”) and failure to so comply shall constitute a serious breach of this Agreement. The Contractor shall indemnify, save harmless and keep the Client indemnified from and against any claim arising or loss or costs incurred as a result of its failure or incapacity to fulfil its obligation under the said TUPE Regulations.
- I. In the case of public procurement procedures which are subject to an IPI measure within the meaning of Regulation (EU) 2022/1031, the Contractor shall comply with the following obligations:
 - i. Not to subcontract more than 50% of the total value of the contract to economic operators originating in a third country which is subject to an IPI measure.
 - ii. For contracts whose subject matter covers the supply of goods, to ensure for the duration of the contract that goods or services supplied or provided in the execution of the contract and originating in a third country which is subject to the IPI measure represent no more than 50% of the total value of the contract, irrespective of whether such goods or services are supplied or provided directly by the successful tenderer or by a subcontractor.
 - iii. To provide the Client, upon request, adequate evidence corresponding to point (i) or (ii) above.
 - iv. To pay a proportionate charge, in the event of non-observance of the obligations referred to at point (i) or (ii) above, of between 10% and 30% of the total value of the contract.

2. KEY PERSONNEL

The Contractor undertakes and acknowledges that it is responsible for ensuring that all key personnel as specified in the Submission ("Key Personnel"), assigned by it to provide the Services shall be available for the Term of this Agreement. The Contractor acknowledges that the Key Personnel are essential to the proper provision of the Services to the Client. In the event that any of the Key Personnel assigned by the Contractor to provide the Services under this Agreement becomes unable to provide the Services for whatever reason then, the Contractor acknowledges and undertakes that it shall immediately notify the Client in writing of the inability of any Key Personnel and replace that person with a person of equivalent experience and expertise ("Replacement Personnel"). The Contractor shall provide to the Client such details as the Client may reasonably require in writing regarding any Replacement Personnel. The Client shall have absolute discretion as to the suitability of any proposed Replacement Personnel.

3. PAYMENT

- A. Subject to the provisions of this clause 3 the Client shall pay and discharge the Charges (plus any applicable VAT), in the manner specified at Schedule C. Invoicing arrangements shall be on such terms as may be agreed between the Parties.
- B. Discharge of the Charges is subject to:
 - 1. Compliance by the Contractor with the provisions of this Agreement including but not limited to any milestones, compliance schedules and/or operational protocols in place pursuant to clause 10A from time to time;
 - 2. The furnishing by the Contractor of a valid invoice and such supporting documentation as may be required by the Client from time to time. Any Contractor pre-printed terms and conditions are hereby disallowed;
 - 3. Invoices being submitted to the Client's Contact (as set out in this Agreement or such other alternative contact as may be agreed between the Parties). All and any queries relating to the invoice and/or the Services for any billing period (including whether or not Services have been accepted, rejected, satisfactorily re-performed or as the case may be) must be raised by the Client's Contact within 14 calendar days of receipt of invoice. In circumstances where no queries are raised within the said 14 day period the invoice shall be deemed accepted. Upon resolution of any queries on the invoice to the satisfaction of the Client or upon such deemed acceptance the invoice shall be payable by the Client. Payment is subject to any rights reserved by the Client under any other provision of this Agreement; and
 - 4. The Client being in possession of the Contractor's current Tax Clearance Certificate. The Contractor shall comply with all applicable EU and domestic taxation law and requirements.
- C. The European Communities (Late Payment in Commercial Transactions) Regulations, 2012 shall apply to all payments. Incorrect invoices will be returned for correction with consequential effects on the due date of payment.
- D. Wherever under this Agreement any sum of money is recoverable from or payable by the Contractor (including any sum which the Contractor is liable to pay to the Client in respect of any breach of this Agreement), the Parties may agree to deduct that sum from any sum

then due, or which at any later time may become due to the Contractor under the Agreement or under any other agreement or contract with the Client. Any overpayment by either Party, whether of the Charges or of VAT or otherwise, shall be a sum of money recoverable by the Party who made the overpayment from the Party in receipt of the overpayment.

- E. The Charges shall include any and all costs or expenses incurred by the Contractor, its employees, servants and agents in the performance of its obligations under this Agreement.
- F. The Charges shall be discharged as provided for in this clause subject to the retention by the Client in accordance with section 523 of the Taxes Consolidation Act, 1997 of any Professional Services Withholding Tax payable to the Contractor. Any and all taxes applicable to the provision of the Services will be the sole responsibility of the Contractor and the Contractor so acknowledges and confirms.

4. WARRANTIES, REPRESENTATIONS AND UNDERTAKINGS

- A. The Contractor acknowledges, warrants, represents and undertakes that:
 1. it has the authority and right under law to enter into, and to carry out its obligations and responsibilities under this Agreement and to provide the Services hereunder;
 2. it is entering into this Agreement with a full understanding of its material terms and risks and is capable of assuming those risks;
 3. it is entering into this Agreement with a full understanding of its obligations with regard to taxation, employment, social and environmental protection and is capable of assuming and fulfilling those obligations;
 4. it has acquainted itself with and shall comply with all legal requirements or such other laws, recommendations, guidance or practices as may affect the provision of the Services as they apply to the Contractor;
 5. it has taken all and any action necessary to ensure that it has the power to execute and enter into this Agreement;
 6. the status of the Contractor, as declared in the "Declaration as to Personal Circumstances of Tenderer" dated [insert date] , which confirms that none of the excluding circumstances listed in Regulation 57 of the Regulations apply to the Contractor, remains unchanged;
 7. it owns, has obtained or is able to obtain, valid licences for all Intellectual Property Rights (as defined in clause 6 below) that are necessary for the performance of its obligations under this Agreement and for the Client to obtain the benefit of the Services for its business purposes;
 8. Not Used.

9. it retains and shall maintain for the Term insurances for the nature and amount specified in the RFT. The Contractor undertakes to advise the Client forthwith of any material change to its insured status, to produce proof of current premiums paid upon written request and where required produce valid certificates of insurance for inspection. The Contractor shall carry out all directions of the Client with regard to compliance with this clause 4A.9; and
 10. the Client shall be under no obligation to purchase any minimum number or value of Services.
- B.** The Contractor undertakes to notify the Client forthwith of any material change to the status of the Contractor with regard to the warranties, acknowledgements, representations and undertakings as set out at clause 4A and to comply with all reasonable directions of the Client with regard thereto which may include termination of this Agreement.

5. REMEDIES

- The Contractor shall be liable for and shall indemnify the Client for and in respect of all and any losses, claims, demands, damages or expenses which the Client may suffer due to and arising directly as a result of the negligence, act or omission, breach of contract, breach of duty, insolvency, recklessness, bad faith, wilful default or fraud of the Contractor, its employees, Subcontractors or agents or any of them or as a result of the Contractor's failure to exercise skill, care and diligence as outlined in clause 1. The terms of this clause 5A shall survive termination of this Agreement for any reason.
- A.**
- B.** Save in respect of fraud (including fraudulent misrepresentation), personal injury or death or in respect of the Contractor's indemnity under clause 6(G), neither Party will be liable for any indirect losses (including loss of profit, loss of revenue, loss of goodwill, indirectly arising damages, costs and expenses) of any kind whatsoever and howsoever arising even if such Party has been advised of their possibility.
- C.** Should the Client find itself obliged to order elsewhere in consequence of the failure of the Contractor to deliver Services, the Client shall be entitled to recover from the Contractor any excess prices which may be paid by the Client.
- D.** Except as otherwise expressly provided by this Agreement, all remedies available to either Party for breach of this Agreement are cumulative and may be exercised concurrently or separately, and the exercise of any one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.
- E.** Save in respect of fraud, personal injury or death or in respect of the Contractor's indemnity under clause 6(G) (for which no limit applies), the limit of the Contractor's aggregate liability to the Client under this Agreement whatsoever and howsoever arising shall not under any circumstances exceed 100 per cent of the charges paid or projected to be paid (whichever is higher) by the Contractor to the Client in any 12 month period under this Agreement regardless of the number of claims and in any event shall not be for the sum more than the maximum limit of the Contractor's insurance cover.
- F.** Not Used.

- G. Time of delivery shall be of the essence and if the Contractor fails to deliver the Services within the time period promised or specified in the Specification, the Client may by notice in writing to the Contractor's Contact release itself from any obligation to accept and pay for the Services and / or terminate this Agreement in either case without prejudice to any other rights and remedies of the Client.
- H. Not Used.

6. INTELLECTUAL PROPERTY

- A. Intellectual Property Rights ("IPR") means all patents and patent rights, trademarks and trademark rights, trade names and trade name rights, service marks and service mark rights, service names and service name rights, brand names, copyrights and copyright rights, trade dress, business and product names, logos, slogans, trade secrets, industrial models, utility models, design models, designs, rights in confidential information, know-how, rights in the nature of unfair competition rights and rights to sue for passing off, and all pending applications for and registrations of patents, trademarks, service marks, and copyrights together with all connected and similar or analogous rights in any country or jurisdiction for the full term thereof.
- B. Pre-existing IPR means all IPR existing prior to the date of this Agreement and all IPR in any materials, acquired or developed by or for Contractor or Client independently of this Agreement, and any IPR in Contractor's standard hardware and software products or modifications or updates to such products.
- C. All IPR title and interest in all reports, data manuals and/or other materials (other than software) (including without limitation all and any audio or audio visual recordings, transcripts, books, papers, records, notes, illustrations, photographs, diagrams) produced for the purposes of this Agreement (collectively "the Materials") (or any part or parts thereof) shall vest in the Client and the Contractor so acknowledges and confirms. For the avoidance of doubt the Contractor hereby assigns all Intellectual Property Rights, title and interest in the Materials (including by way of present assignment of future copyright) to the extent that any such Intellectual Property Rights title or interest may be deemed by law to reside in it in the Materials to the Client absolutely.
- D. The Client grants to the Contractor a royalty-free non-exclusive licence to use the Client's Pre-existing IPR for the Term to the extent necessary to enable the Contractor to fulfil its obligations under this Agreement. Save as expressly set out in this clause 6 all Pre-Existing IPR shall remain the sole property of the party who owned, acquired or developed such intellectual property.
- E. The Contractor shall waive or procure a waiver of any moral rights subsisting in copyright produced under or in performance of this Agreement.
- F. Nothing in this Agreement shall prohibit or be deemed to prohibit the Contractor from providing services similar to the Services to any party other than the Parties hereto. In no event shall the Contractor be precluded from independently developing for itself, or for others, materials which are competitive with, or similar to, the Services and to use its

general knowledge, skills and experience, and any ideas, concepts, know-how, formats, templates, methodologies and techniques that are acquired or used in the course of providing the Services.

- G.** The Contractor shall ensure that all and any necessary consents and/or licences for any software, instrument, modality or methodology are obtained and in place before use for the purposes of this Agreement (to include but not be limited to ensuring that the Client shall be vested with all necessary rights so as to enable the Client to enjoy the benefit of the Services for its business purposes). The Contractor hereby indemnifies the Client and shall keep and hold the Client harmless from and in respect of all and any losses (whether direct, indirect or consequential) liability, damages, claims, costs or expenses which arise by reason of any breach of third-party Intellectual Property Rights in so far as any such rights are used for the purposes of this Agreement.

At the request of the Client for and in respect of any such breach, the Contractor shall at its expense and option:

- (i) procure the necessary rights for the Client to continue use;
- (ii) replace the relevant deliverable with a non-infringing equivalent;
- (iii) replace the relevant deliverable to make it non-infringing while giving equivalent performance; or
- (iv) if the Contractor cannot obtain the remedies in (i), (ii) or (iii) above, it may direct the return of the deliverable and refund to the Client Charges paid for such deliverable less a reasonable amount for the Client's use of the deliverable up to the time of return, provided such reasonable amount is due to the owner of the said deliverable, TOGETHER with all losses (whether direct, indirect or consequential) thereby accruing to the Client as a result of the breach.

- H.** Upon the termination of this Agreement for whatever reason, the Contractor shall immediately deliver up to the Client all the Materials prepared up to the date of termination. The provisions of this clause 6 will survive the expiration or termination of this Agreement for any reason.

7. CONFIDENTIALITY

- A.** Each of the Parties to this Agreement agrees to hold confidential all information, documentation and other material received, provided or obtained arising from their participation in this Agreement ("Confidential Information") and shall not disclose same to any third party except to:-
- 1. its professional advisers subject to the provisions of this clause 7; or
 - 2. as may be required by law; or
 - 3. as may be necessary to give effect to the terms of this Agreement subject to the provisions of this clause 7; or
 - 4. in the case of the Client by request of any person or body or authority whose request the Client or persons associated with the Client (including but not limited to the

Legislature and/or the Executive and/or the Civil Service) considers it necessary or appropriate to so comply.

- B. The Contractor undertakes to comply with all reasonable directions of the Client with regard to the use and application of all and any of its Confidential Information and shall comply with the confidentiality agreement as exhibited at Appendix 6 to the RFT (“the Confidentiality Agreement”).

The obligations in this clause 7 will not apply to any Confidential Information:

1. in the receiving Party’s possession (with full right to disclose) before receiving it from the other Party; or
2. which is or becomes public knowledge other than by breach of this clause; or
3. is independently developed by the disclosing Party without access to or use of the Confidential Information; or
4. is lawfully received by the disclosing Party from a third party (with full right to disclose).

- C. The Contractor acknowledges that the security of the State and its information is of paramount importance to the Client. Accordingly, the Contractor confirms that it will, if requested by the Client, from time to time, submit full personal details (including those of Subcontractors) who are assigned to provide the Services (or any part thereof) under this Agreement. The Contractor further acknowledges that checks may be carried out in relation to all such personnel by police authorities and the Contractor shall comply with all reasonable directions of the Client arising therefrom.

- D. In circumstances where the Client is subject to the provisions of the Freedom of Information Act 2014 or the European Communities (Access to Information on the Environment) Regulations 2007 to 2014, then in the event of the Client receiving a request for information related to this Agreement, the Client shall consult with the Contractor in respect of the request. The Contractor shall identify any information that is not to be disclosed on grounds of confidentiality or commercial sensitivity and shall state the reasons for this sensitivity. The Client will consult the Contractor about this confidential or commercially sensitive information before making a decision on any request received under the above legislation. The Contracting Authority accepts no liability whatsoever in respect of any information provided which is subsequently released (irrespective of notification) or in respect of any consequential damage suffered as a result of such obligations.

- E. The terms of this clause 7 shall survive expiry, completion or termination for whatever reason of this Agreement.

8. FORCE MAJEURE

- A. A 'Force Majeure Event' means an event or circumstance or combination of events and/or circumstances not within the reasonable control of the Affected Party (as defined in clause 8B below) which has the effect of delaying or preventing that Party from complying with its obligations under this Agreement including but not limited to acts of God, war, out-break of disease, insurrection, riot, civil disturbance, rebellion, acts of terrorism, government regulations, embargoes, explosions, fires, floods, tempests, or failures of supply of electrical power, or public telecommunications equipment or lines, excluding industrial action of whatever nature or cause (strikes, lockouts and similar) occurring at the Contractor (or Subcontractor or agent) places of business.
- B. In the event of any failure, interruption or delay in the performance of either Party's obligations (or of any of them) resulting from any Force Majeure Event, that Party ("the Affected Party") shall promptly notify the other Party in writing specifying:
1. the nature of the Force Majeure Event;
 2. the anticipated delay in the performance of obligations;
 3. the action proposed to minimise the impact of the Force Majeure Event;
- and the Affected Party shall not be liable or have any responsibility of any kind for any loss or damage thereby incurred or suffered by the other Party, provided always that the Affected Party shall use all reasonable efforts to minimise the effects of the same and shall resume the performance of its obligations as soon as reasonably possible after the removal of the cause.
- C. If the Force Majeure Event continues for 90 calendar days either Party may terminate at 14 days' notice.
- D. In circumstances where the Contractor is the Affected Party, the Client shall be relieved from any obligation to make payments under this Agreement save to the extent that payments are properly due and payable for obligations actually fulfilled by the Contractor in accordance with the terms and conditions of this Agreement.

9. TERMINATION

- A. This Agreement may be terminated by the Client, without liability for compensation or damages, by serving 30 days written notice to the Contractor. This Agreement may be terminated by the Contractor, without liability for compensation or damages, by serving 90 days written notice to the Client.
- B. Either Party shall have the right (in addition to its rights under clause 9(a) and any other rights which it has at law) to terminate this Agreement immediately and without liability for compensation or damages on the happening of any of the following:
1. if the other Party commits any serious breach or a series of breaches of any provision of this Agreement and fails to remedy such breach(es) (if the breach(es) are capable of remedy) within 30 days after receipt of a request in writing from the other Party;

2. if the other Party becomes insolvent, becomes bankrupt, enters into examinership, is wound up, commences winding up, has a receiving order made against it, makes any arrangement with its creditors generally or takes or suffers any similar action as a result of debt, or an event having an equivalent effect;
 3. in circumstances where the Client becomes aware of any conflict of interest on the part of the Contractor which cannot, in the opinion of the Client, be removed by other means; and
 4. in circumstances where the Client becomes aware of any registrable interest on the part of the Contractor.
- C. The Client shall have the right, in addition to any other rights which it has at law, to terminate this Agreement immediately and without liability for compensation or damages in circumstances where the Client becomes aware that any of the exclusion grounds set out in Regulation 57 of the Regulations apply to the Contractor.
- D. Termination of this Agreement shall not affect any antecedent and accrued rights, obligations or liabilities of either Party, nor shall it affect any provision of this Agreement which is expressly or by implication intended to come into or continue in force on or after such termination.
- E. If requested by the Client, the Contractor shall promptly furnish such anonymised information relating to the terms and conditions of the employment of all persons providing the Services as may be required by the Client ("Employment Information"). The Contractor agrees that the Client may release the Employment Information to third parties for the purposes of any procurement competition for the provision of the Services upon expiry of the Term or earlier termination of this Agreement for whatever cause.

10. CONTRACT MANAGEMENT

- A. The Client's Contact and the Contractor's Contact shall liaise on a regular basis to address any issues arising which may impact on the performance of this Agreement and to agree milestones, compliance schedules and operational protocols as required by the Client from time to time. If requested in writing by the Client the Contractor shall meet formally with the Client to report on progress and shall comply with all written directions of the Client.
- B. The Contractor agrees to:
1. liaise with and keep the Client's Contact fully informed of any matter which might affect the observance and performance of the Contractor's obligations under this Agreement;
 2. maintain such records and comply with such reporting arrangements and protocols as required by the Client from time to time;
 3. comply with all reasonable directions of the Client; and
 4. comply with the service levels and performance indicators set out in Schedule D.
- C. The Client or its authorised representative may inspect the Contractor's premises, lands and facilities (or such part or parts thereof relating solely to this Agreement) with due access to

relevant personnel and records upon reasonable notice in writing to ensure compliance with the terms of this Agreement. The Contractor shall comply with all reasonable directions of the Client thereby arising. The cost of inspection shall be borne by the Client.

11. DISPUTES

- A. In the event of any dispute arising out of or relating to this Agreement (the “Dispute”), the Parties shall first seek settlement of the Dispute as set out below.
- B. The Dispute shall be referred as soon as practicable to [insert Contractor contact] within the Contractor and to [insert Client contact] within the Client respectively.
- C. If the Dispute has not been resolved within fifteen (15) Business Days (or such longer period as may be agreed in writing by the Parties) of being referred to the nominated representatives, then either Party may refer the Dispute to an independent mediator, the identity of whom shall be agreed in advance by the Parties.
- D. If the Parties are unable to agree on a mediator or if the mediator agreed upon is unable or unwilling to act, either Party may within twenty-one (21) days from the date of the proposal to appoint a Mediator or within twenty-one (21) days of notice to either Party that the mediator is unable to act, apply to Mediator’s Institute of Ireland to appoint a mediator.
- E. Any submissions made to and discussions involving the mediator, of whatever nature, shall be treated in strict confidence and without prejudice to the rights and/or liabilities of the Parties in any legal proceedings and, for the avoidance of doubt, are agreed to be without prejudice and legally privileged. The Parties shall make written submissions to the mediator within ten (10) Business Days of his/her appointment.
- F. The Parties shall share equally the cost of the mediator. The costs of all experts and any other third parties who, at the request of any Party, shall have been instructed in the mediation, shall be for the sole account of, and shall be discharged by that Party.
- G. For the avoidance of doubt, the obligations of the Parties under this Agreement shall not cease, or be suspended or delayed by the reference of a dispute to mediation. The Contractor shall comply fully with the requirements of the Agreement at all times.

12. GOVERNING LAW, CHOICE OF JURISDICTION AND EXECUTION

- A. This Agreement shall in all aspects be governed by and construed in accordance with the laws of Ireland and the Parties hereby agree that the courts of Ireland have exclusive jurisdiction to hear and determine any disputes arising out of or in connection with this Agreement.
- B. This Agreement shall be executed in duplicate and each copy of the Agreement shall be signed by all the Parties hereto. Each of the Parties to this Agreement confirms that this Agreement is executed by their duly authorised officers.

13. NOTICES

- A. Any notice or other written communication to be given under this Agreement shall either be delivered personally or sent by registered post or email. The Parties will from time to time agree primary and alternative contact persons and details for the purposes of this clause 13.
- B. All notices shall be deemed to have been served as follows:
 - 1. if personally delivered, at the time of delivery;
 - 2. if posted by registered post, at the expiration of 48 hours after the envelope containing the same was delivered into the custody of the postal authorities (and not returned undelivered); and
 - 3. if communicated by email, on the next calendar day following transmission.

14. ASSIGNMENT AND SUBCONTRACT

- A. Subject to a Party's obligations at law, any assignment to a third party or other transfer of a Party's rights or obligations under this Agreement (the "Assignment") requires the prior written consent of the other Party. Prior to any such Assignment, the assignee will be obliged to sign an undertaking to comply with all obligations under this Agreement. Any attempted Assignment not complied with in the manner prescribed herein shall be null and void.
- B. Subject to a Party's obligations at law, any sub-contract of a Party's rights or obligations under this Agreement requires the prior written consent of the other Party, such consent not to be unreasonably withheld or delayed. Any attempted subcontract not complied with in the manner prescribed herein shall be null and void.

15. ENTIRE AGREEMENT

This Agreement constitutes the entire agreement and understanding of the Parties, and any and all other previous agreements, arrangements and understandings (whether written or oral) between the Parties with regard to the subject matter of this Agreement (save where fraudulently made) are hereby excluded.

16. SEVERABILITY

If any term or provision herein is found to be illegal or unenforceable for any reason, then such term or provision shall be deemed severed and all other terms and provisions shall remain in full force and effect.

17. WAIVER

No failure or delay by either Party to exercise any right, power or remedy shall operate as a waiver of it, nor shall any partial exercise preclude further exercise of same or some other right, power or remedy.

18. NON-EXCLUSIVITY

Nothing in this Agreement shall preclude the Client from purchasing services (or Services) from a third party at any time during the currency of the Agreement.

19. MEDIA

No media releases, public announcements or public disclosures relating to this Agreement or its subject matter, including but not limited to promotional or marketing material, shall be made by the Contractor without the prior written consent of the Client.

20. CONFLICTS, REGISTRABLE INTERESTS AND CORRUPT GIFTS

- A. The Contractor confirms that it has carried out a conflicts of interest check and is satisfied that neither it nor any Subcontractor nor agent as the case may be has any conflicts in relation to the Services and its obligations undertaken under this Agreement. The Contractor hereby undertakes to notify the Client immediately should any conflict or potential conflict of interest come to its attention during the currency of this Agreement and to comply with the Client's directions in respect thereof. In the event of such notification, the Client shall have the right (in addition to any other rights which it has at law) to terminate this Agreement immediately and without liability for compensation or damages.
- B. Any registrable interest involving the Contractor (and any Subcontractor or agent as the case may be) and the Client, the Ceann Comhairle (Speaker), or any member of the Government, or any member of the Oireachtas, or their relatives must be fully disclosed to the Client immediately upon such information becoming known to the Contractor (Subcontractor or agent as the case may be) and the Contractor shall comply with the Client's directions in respect thereof, to the satisfaction of the Client. In the event of such disclosure, the Client shall have the right (in addition to any other rights which it has at law) to terminate this Agreement immediately and without liability for compensation or damages. The terms "registrable interest" and "relative" shall be interpreted as per section 2 of the Ethics in Public Office Act, 1995 (as amended) a copy of which is available on request.
- C. The Contractor shall not offer or agree to give any public servant or civil servant any gift or consideration or commission of any kind as an inducement or reward for doing or forbearing to do or for having done or forborne to do any action in relation to the obtaining or execution of this or any other public contract. Any breach of this clause 20C or the commission of any offence by the Contractor, any Subcontractor, agent or employee under the Criminal Justice (Corruption Offences) Act 2018 shall entitle the Client to terminate this Agreement immediately and without liability for compensation or damages and to recover the amount of any loss resulting from such cancellation, including but not limited to recovery from the Contractor of the amount or value of any such gift, consideration or commission.

21. ACCESS TO PREMISES

- A. Any of the Client's premises made available from time to time to the Contractor by the Client in connection with this Agreement, shall be made available to the Contractor on a non-exclusive licence basis and shall be used by the Contractor solely for the purpose of performing its obligations under this Agreement. The Contractor shall have use of such premises as licensee and shall vacate the same on completion, termination or abandonment of this Agreement.

- B. The Contractor shall upon reasonable notice by the Client allow the Client access to its premises (including the premises of any Subcontractor or agent) where the Services are being performed for the Client under this Agreement.

22. EQUIPMENT

- A. The Contractor shall provide all equipment and materials necessary for the provision of the Services ("Equipment").
- B. All Equipment brought onto the Client's premises shall be at the Contractor's own risk and the Client shall have no liability for any loss of, caused by or damage to any Equipment. The Contractor shall provide for the haulage or carriage thereof to the Client's premises and the removal of Equipment when no longer required at its sole cost. Unless otherwise agreed, Equipment brought onto the premises will remain the property of the Contractor.
- C. The Contractor shall maintain and store all items of Equipment within the Client's premises in a safe, serviceable and clean condition.
- D. The Contractor shall, at the Client's written request, at its own expense and as soon as reasonably practicable:
 - i. remove from the Client's premises any Equipment which in the reasonable opinion of the Client is either hazardous, noxious or not in accordance with this Agreement; and
 - ii. replace such item with a suitable substitute item of Equipment.
- E. On completion of the Services the Contractor shall remove the Equipment used by the Contractor to provide the Services and shall leave the Client's premises in a clean, safe and tidy condition. The Contractor is solely responsible for making good any damage to the Client's premises or any objects contained thereon, other than fair wear and tear, which is caused by the Contractor or any of its employees or Subcontractors.

23. NON SOLICITATION

- A. For the Term and for a period of 12 months thereafter (and save in respect of publicly advertised posts) neither the Client nor the Contractor shall employ or offer employment to any of the other Party's employees without that other Party's prior written consent.

24. CHANGE CONTROL PROCEDURE

- A. At any time during the Term of this Agreement, either Party may propose a change or changes to any part or parts of this Agreement.
- B. The change control procedures set out in this Schedule will apply to all changes irrespective of whether the Contractor or the Client proposes the change.
- C. A change control notice ("Change Control Notice") shall be prepared for all change requests. The Change Control Notice will provide an outline description of the change requested, the rationale for the change, the effect that the change will have on the Services (where known)

and an estimate of the effort and cost required to prepare an impact assessment (“Impact Assessment”).

- D. All Change Control Notices proposing changes to this Agreement must be submitted for review to the other Party’s Contact.
- E. The Parties must indicate their acceptance or rejection of the change control request and/or Impact Assessment within a reasonable timeframe of its completion and Tender Submission for review, subject to a maximum of twenty (20) calendar days or such other period agreed between the Parties.
- F. On approval of an Impact Assessment, this Agreement and/or the Schedules should be updated and revised as appropriate and in writing.
- G. In the event that either Party rejects the Impact Assessment, the change(s) shall not take place and the Parties shall continue to perform their obligations under this Agreement.
- H. The Contractor and the Client will agree a reasonable charge in advance for investigating each proposed variation and preparing each estimate, whether or not the variation is implemented. If the Client’s request for any variation is subsequently withdrawn but results in a delay in the performance of the Services then the Contractor will not be liable for such delay and will be entitled to an extension of time equal to not less than the period of the delay.

25. DATA PROTECTION AND SECURITY

- A. In this Agreement the following terms shall have the meanings respectively ascribed to them:

“Data” means all Confidential Information, whether in oral or written (including electronic) form, created by or in any way originating with the Client (including but not limited to his employees, agents, independent contractors and/or Sub-contractors) and all information that is the output of any computer processing, or other electronic manipulation of any information that was created by or in any way originating with the Client provided under this Agreement and includes any Personal Data;

“Data Controller” has the meaning given under the Data Protection Laws;

“Data Processor” has the meaning given under the Data Protection Laws;

“Data Protection Laws” means all applicable national and EU data protection laws, regulations and guidelines, including but not limited to Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the “General Data Protection Regulation”), and any guidelines and codes of practice issued by the Office of the Data Protection Commissioner or other supervisory authority for data protection in Ireland.

“Data Subject” has the meaning given under the Data Protection Laws;

“Data Subject Access Request” means a request made by a Data Subject in accordance with rights granted under the Data Protection Laws to access his or her Personal Data;

“Personal Data” has the meaning given under Data Protection Laws;

“Processing” has the meaning given under the Data Protection Laws;

- B. The Contractor shall comply with all applicable requirements of the Data Protection Laws.
- C. The Parties acknowledge that for the purposes of the Data Protection Laws, the Client is the Data Controller and the Contractor is the Data Processor in respect of Data which is Personal Data. Schedule E sets out the scope, nature and purpose of Processing by the Contractor, the duration of the Processing and the types of Personal Data and categories of Data Subject.
- D. Without prejudice to the generality of clause 25B, the Contractor shall, in relation to any Personal Data processed in connection with the performance by the Contractor of its obligations under this Agreement:-

(1) process that Personal Data only on the written instructions of the Client;

(2) ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the Client, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

(3) ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential;

(4) not transfer any Personal Data outside of the European Economic Area unless the prior written consent of the Client has been obtained and the following conditions are fulfilled;

- i. appropriate safeguards are in place in relation to the transfer, to ensure that Personal Data is adequately protected in accordance with Chapter V of Regulation 2016/679 (General Data Protection Regulation);
- ii. the data subject has enforceable rights and effective legal remedies;
- iii. The Contractor complies with its obligations under the Data Protection Laws by providing an adequate level of protection to any Personal Data that is transferred; and
- iv. The Contractor complies with reasonable instructions notified to it in advance by the Client with respect to the processing of the Personal Data;

- E. The Contractor shall promptly notify the Client if it receives a Data Subject Access Request to have access to any Personal Data or any other complaint, correspondence, notice, request any order of the Court or request of any regulatory or government body relating to the Client’s obligations under the Data Protection Laws and provide full co-operation and assistance to the Client in relation to any such complaint, order or request (including, without limitation, by allowing Data Subjects to have access to their data).

- F. The Contractor shall without undue delay report in writing to the Client any data compromise involving Personal Data, or any circumstances that could have resulted in unauthorised access to or disclosure of Personal Data.
 - G. The Contractor shall assist the Client in ensuring compliance with its obligations under the Data Protection Laws with respect to security, impact assessments and consultations with supervisory authorities and regulators.
 - H. The Contractor shall at the written direction of the Client, amend, delete or return Personal Data and copies thereof to the Client on termination of this Agreement unless the Contractor is required by the laws of any member of the European Union or by the laws of the European Union applicable to the Contractor to store the Personal Data.
 - I. The Contractor shall permit the Client, the Office of the Data Protection Commissioner or other supervisory authority for data protection in Ireland, and/ or their nominee to conduct audits and or inspections of the Contractor's facilities, and to have access to all data protection, confidentiality and security procedures, data equipment, mechanisms, documentation, databases, archives, data storage devices, electronic communications and storage systems used by the Contractor in any way for the supply of the Goods. The Contractor shall comply with all reasonable directions of the Client arising out of any such inspection, audit or review.
 - J. The Contractor shall fully comply with, and implement policies which are communicated or notified to the Contractor by the Client from time to time.
 - K. The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this clause 25 and allow for inspections and contribute to any audits by the Client or the Client's designated auditor.
 - L. The Contractor shall:-
 - (1) take all reasonable precautions to preserve the integrity of any Personal Data which it processes and to prevent any corruption or loss of such Personal Data;
 - (2) ensure that a back-up copy of any and all such Personal Data is made weekly and this copy is recorded on media from which the data can be reloaded if there is any corruption or loss of the data; and
 - (3) in such an event and if attributable to any default by the Contractor or any Sub-contractor, promptly restore the Personal Data at its own expense or, at the Client's option, reimburse the Client for any reasonable expenses it incurs in having the Personal Data restored by a third party.
- The Client does not consent to the Contractor appointing any third party processor of Personal Data under this agreement
- M. Save for clauses 25B, 25C, 26D(4) and 25E, all the obligations on the Contractor in this clause 25 relating to the processing of Personal Data shall apply to the processing of all Data.
 - N. The provisions of this clause 25 shall survive termination and or expiry of this Agreement for any reason.

26. ADDITIONAL CONDITION(S)

Benchmarking prior to extension

Prior to exercising any option to extend the contract, the Contracting Authority may review and benchmark the Contractor's rates against prevailing market rates for comparable services.

Where the Contracting Authority considers that the Contractor's rates no longer represent value for money, the Parties may enter into discussions with a view to agreeing revised rates for the relevant extension period.

The Contracting Authority shall be under no obligation to exercise any extension option. Any extension shall be subject to the written agreement of the Parties, including agreement on any revised rates where applicable.

Schedule B: Services: The Specification

[Insert when completing contract]

Schedule C: Charges

[Insert when completing contract]

Schedule D: Service Levels

The Contracting Authority will monitor the Contractor's performance having regard to, as a minimum, the performance areas and expected standards listed below:

PERFORMANCE AREA	EXPECTED STANDARD
Resource availability	Agreed resource positions remain filled throughout the Contract.
Resource replacement	Suitable replacement resources are proposed within the agreed timeframe and approved by the Contracting Authority. No assigned personnel will be withdrawn without the prior written agreement of the Department, and subject to a minimum notice period of one (1) month; All personnel assigned under this contract will provide a minimum of one (1) months' notice prior to cessation of duties to support service continuity.
Quality of resources	Resources perform the duties assigned and possess the required skills and experience.
Resource management	Workforce planning, continuity arrangements and knowledge transfer are effectively maintained.
Security and confidentiality	Compliance with all contractual security, confidentiality and data protection obligations.

Schedule E: Data Protection

Processing, Personal Data and Data Subjects

1. Processing by the Contractor

1.1 Subject matter of processing

The Contractor will provide External ICT Technical Support Services to assist the Client's ICT Unit in supporting, maintaining, securing, administering, developing and managing the Client's ICT infrastructure, cloud services, business applications, collaboration platforms, communications systems and associated technologies.

1.2 Nature of processing

The Contractor will be engaged in the support, administration and maintenance of the Client's ICT environment, including on-premises, cloud and hybrid platforms. Activities may include system administration, identity and access management, incident resolution, cybersecurity operations, software deployment, monitoring, backup and recovery, migrations, SharePoint administration and Power Platform support.

All work will be carried out on the instructions of the Client's ICT Unit management. The Contractor will not process Personal Data except where necessary for the provision of the Services and will comply with the Client's Data Protection, Information Security and ICT policies.

With the exception of account creation and maintenance, the Contractor will typically be limited to servicing the ICT infrastructure. This will include running backups, restores and systems migrations but will generally not include processing of personal data held on the Client's systems directly.

1.3 Purpose of processing

The purpose of processing Personal Data is solely to facilitate the provision of the Services under the Contract and the support, maintenance, administration and security of the Client's ICT environment.

1.4 Duration of the processing

Data processing will be limited strictly to the duration required to perform the Services and shall be carried out only upon the instructions of the Client. Personal Data will not be processed outside of the Client's ICT systems.

2. Types of personal data

The Contractor may have access to ICT systems containing Personal Data in the course of providing the Services. Such Personal Data may include, but is not limited to:

- Personal data of employees, contractors and temporary staff;
- Personal data of service users and members of the public;

- User account, authentication and access control information;
- Contact details including names, email addresses, telephone numbers and business addresses;
- System, audit, security and usage logs;
- Personal data contained within email, collaboration, document management and business application systems.

Where a particular support, maintenance or investigative activity requires access to Personal Data, such access shall be limited to that necessary to perform the relevant activity and shall be carried out only on the instructions of the Client.

3. Categories of data subject

The categories of Data Subjects whose Personal Data may be processed include:

- Employees and former employees of the Client;
- Contractors, consultants and agency personnel;
- Locally engaged staff and personnel at overseas missions;
- Service users and members of the public;
- Suppliers, service providers and business contacts;
- Any other individuals whose Personal Data is contained within systems supported by the Contractor in the course of delivering the Services.

Schedule F: Key Personnel

[Insert when completing contract]

Schedule G: Exit Management and Handover

[Insert when completing contract]

Appendix 6: Confidentiality Agreement

THIS AGREEMENT is made on the [date] day of [month] 20 [year] BETWEEN:

The Minister for Foreign Affairs and Trade, of [insert address] (hereinafter “the Contracting Authority”) of the one part;
and

[Contractor’s legal name: to be completed on signing.], of [address: to be completed on signing.]
(hereinafter called “the Contractor”) of the other part.

WHEREAS

- A. By Request for Tenders dated [insert date] entitled The Provision of External ICT Technical Support Services (the “RFT”) the Contracting Authority invited tenders (“Tenders”) for the provision of the Services described in Appendix 1 to the RFT (the “Services”) (“the Competition”). The Contractor submitted a response to the RFT dated the [insert date of Tender].

The Contractor has been identified as the preferred bidder in the Competition.

- B. For the purposes of the Competition and any subsequent contract awarded thereunder (if any) (“the Contract”), certain confidential information as defined at clause 2 of this Agreement, will be furnished to the Contractor. The Confidential Information is confidential to the Client.

NOW IT IS HEREBY AGREED in consideration of the sum of €2.00 (the receipt of which is hereby acknowledged by the Contractor) as follows:

1. The Contractor acknowledges that Confidential Information may be provided to them by the Contracting Authority and that each item of Confidential Information shall be governed by the terms of this Agreement.
2. For the purposes of this Agreement “Confidential Information” means:
 - 2.1 unless specified in writing to the contrary by the Contracting Authority all and any information (whether in documentary form, oral, electronic, audio-visual, audio-recorded or otherwise including any copy or copies thereof and whether scientific, commercial, financial, technical, operational or otherwise) relating to the Contracting Authority, the supply of Services under the Contract and all and any information supplied or made available to the Contractor (to include employees, agents, Subcontractors and other suppliers) for the purposes of the Contract(s) including personal data within the meaning of the Data Protection Laws; and
 - 2.2 any and all information which has been derived or obtained from information described in sub-paragraph 2.1.
3. For the purposes of this Agreement “Data Protection Laws” means all applicable national and EU data protection laws, regulations and guidelines, including but not limited to Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and

repealing Directive 95/46/EC (the “General Data Protection Regulation”), and any guidelines and codes of practice issued by the Office of the Data Protection Commission or other supervisory authority for data protection in Ireland from time to time

4. Save as may be required by law, the Contractor agrees in respect of the Confidential Information:

4.1 to treat such Confidential Information as confidential and to take all necessary steps to ensure that such confidentiality is maintained;

4.2 not, without the prior written consent of the Contracting Authority, to communicate or disclose any part of such Confidential Information to any person except:

- i to those employees, agents, Subcontractors and other suppliers on a need to know basis; and/or
- ii to the Contractor’s auditors, professional advisers and any other persons or bodies having a legal right or duty to have access to or knowledge of the Confidential Information in connection with the business of the Contractor

PROVIDED ALWAYS that the Contractor shall ensure that all such persons and bodies are made aware, prior to disclosure, of the confidential nature of the Confidential Information and that they owe a duty of confidence to the Contracting Authority; and shall use all reasonable endeavours to ensure that such persons and bodies comply with the provisions of this Agreement.

5. The obligations in this Agreement will not apply to any Confidential Information:

- i in the Contractor’s possession (with full right to disclose) before receiving it from the Contracting Authority; or
- ii which is or becomes public knowledge other than by breach of this clause; or
- iii is independently developed by the Contractor without access to or use of the Confidential Information; or
- iv is lawfully received from a third party (with full right to disclose).

6. The Contractor undertakes:

6.1 to comply with all directions of the Contracting Authority with regard to the use and application of all and any Confidential Information or data (including personal data as defined in the Data Protection Laws);

6.2 to comply with all directions as to local security arrangements deemed reasonably necessary by the Contracting Authority including, if required, completion of documentation under the Official Secrets Act 1963 and comply with any vetting requirements of the Contracting Authority including by police authorities;

6.3 upon termination of the Competition (or the Contract) for whatever reason to furnish to the Contracting Authority all Confidential Information or at the written direction of the Contracting Authority to destroy in a secure manner all (or such part or parts thereof as may be identified by the Contracting Authority) Confidential

Information in its possession and shall erase any Confidential Information held by the Contractor in electronic form. The Contractor will upon request furnish a certificate to that effect should the Contracting Authority so request in writing. For the avoidance of doubt “document” includes documents stored on a computer storage medium and data in digital form whether legible or not.

7. The Contractor shall not obtain any proprietary interest or any other interest whatsoever in the Confidential Information furnished to them by the Contracting Authority and the Contractor so acknowledges and confirms.
8. The Contractor shall, in the performance of the Contract, access only such hardware, software, infrastructure, or any part of the databases, data or ICT system(s) of the Contracting Authority as may be necessary for the purposes of the Competition (and obligations thereunder or arising therefrom) and only as directed by the Contracting Authority and in the manner agreed in writing between the Parties.
9. The Contractor agrees that this Agreement will continue in force notwithstanding any court order relating to the Competition or termination of the Contract (if awarded) for any reason.
10. The Contractor agrees that this Agreement shall in all aspects be governed by and construed in accordance with the laws of Ireland and the Contractor hereby further agrees that the courts of Ireland have exclusive jurisdiction to hear and determine any disputes arising out of or in connection with this Agreement.
11.
 - A. In this Agreement, the following terms shall have the meanings respectively ascribed to them:

“Data Controller” has the meaning given under the Data Protection Laws;

“Data Processor” has the meaning given under the Data Protection Laws;

“Data Subject” has the meaning given under the Data Protection Laws;

“Data Subject Access Request” means a request made by a Data Subject in accordance with rights granted under the Data Protection Laws to access his or her Personal Data;

“Personal Data” has the meaning given under Data Protection Laws;

“Processing” has the meaning given under the Data Protection Laws;
 - B. The Contractor shall comply with all applicable requirements of the Data Protection Laws.
 - C. The Parties acknowledge that for the purposes of the Data Protection Laws, the Client is the Data Controller and the Contractor is the Data Processor in respect of Confidential Information which is Personal Data. Schedule A sets out the scope, nature and purpose of Processing by the Contractor, the duration of the Processing and the types of Personal Data and categories of Data Subject.
 - D. Without prejudice to the generality of clause 10(B), the Contractor shall, in relation to any Confidential Information which is Personal Data:-
 - (1) process that Personal Data only on the written instructions of the Client;

- (2) ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the Client, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);
- (3) ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential;
- (4) not transfer any Personal Data outside of the European Economic Area unless the prior written consent of the Client has been obtained and the following conditions are fulfilled;
 - i. appropriate safeguards are in place in relation to the transfer, to ensure that Personal Data is adequately protected in accordance with Chapter V of Regulation 2016/679 (General Data Protection Regulation);
 - ii. the data subject has enforceable rights and effective legal remedies;
 - iii. The Contractor complies with its obligations under the Data Protection Laws by providing an adequate level of protection to any Personal Data that is transferred; and
 - iv. The Contractor complies with reasonable instructions notified to it in advance by the Client with respect to the processing of the Personal Data;
- E. The Contractor shall promptly notify the Client if it receives a Data Subject Access Request to have access to any Personal Data or any other complaint, correspondence, notice, request any order of the Court or request of any regulatory or government body relating to the Client's obligations under the Data Protection Laws and provide full co-operation and assistance to the Client in relation to any such complaint, order or request (including, without limitation, by allowing Data Subjects to have access to their data).
- F. The Contractor shall without undue delay report in writing to the Client any data compromise involving Personal Data, or any circumstances that could have resulted in unauthorised access to or disclosure of Personal Data.
- G. The Contractor shall assist the Client in ensuring compliance with its obligations under the Data Protection Laws with respect to security, impact assessments and consultations with supervisory authorities and regulators.

- H. The Contractor shall at the written direction of the Client, amend, delete or return Personal Data and copies thereof to the Client on termination of this Agreement unless the Contractor is required by the laws of any member of the European Union or by the laws of the European Union applicable to the Contractor to store the Personal Data.
- I. The Contractor shall permit the Client, the Office of the Data Protection Commission or other supervisory authority for data protection in Ireland, and / or their nominee to conduct audits and or inspections of the Contractor's facilities, and to have access to all data protection, confidentiality and security procedures, data equipment, mechanisms, documentation, databases, archives, data storage devices, electronic communications and storage systems used by the Contractor in any way for the provision of the services. The Contractor shall comply with all reasonable directions of the Client arising out of any such inspection, audit or review.
- J. The Contractor shall fully comply with, and implement policies which are communicated or notified to the Contractor by the Client from time to time.
- K. The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this clause 11 and allow for inspections and contribute to any audits by the Client or the Client's designated auditor.
- L. The Contractor shall:-
 - 1. take all reasonable precautions to preserve the integrity of any Personal Data which it processes and to prevent any corruption or loss of such Personal Data;
 - 2. ensure that a back-up copy of any and all such Personal Data is made [insert frequency] and this copy is recorded on media from which the data can be reloaded if there is any corruption or loss of the data; and
 - 3. in such an event and if attributable to any default by the Contractor or any Sub-contractor, promptly restore the Personal Data at its own expense or, at the Client's option, reimburse the Client for any reasonable expenses it incurs in having the Personal Data restored by a third party.
- M. The Client does not consent to the Contractor appointing any third party processor of Personal Data under this agreement.
- N. Save for clauses 11B, 11C, 11D(4) and 11E, all the obligations on the Contractor in this clause 11 relating to the processing of Personal Data shall apply to the processing of all Confidential Information.

SIGNED for and on behalf of the Contracting Authority _____ (being a duly authorised officer)	SIGNED for and on behalf of the Contractor _____
Witness	Witness

Schedule A to the Confidentiality Agreement: Data Protection

Processing, Personal Data and Data Subjects

1. Processing by the Contractor

1.1 Subject matter of processing

The Contractor will provide External ICT Technical Support Services to assist the Client's ICT Unit in supporting, maintaining, securing, administering, developing and managing the Client's ICT infrastructure, cloud services, business applications, collaboration platforms, communications systems and associated technologies.

1.2 Nature of processing

The Contractor will be engaged in the support, administration and maintenance of the Client's ICT environment, including on-premises, cloud and hybrid platforms. Activities may include system administration, identity and access management, incident resolution, cybersecurity operations, software deployment, monitoring, backup and recovery, migrations, SharePoint administration and Power Platform support.

All work will be carried out on the instructions of the Client's ICT Unit management. The Contractor will not process Personal Data except where necessary for the provision of the Services and will comply with the Client's Data Protection, Information Security and ICT policies.

With the exception of account creation and maintenance, the Contractor will typically be limited to servicing the ICT infrastructure. This will include running backups, restores and systems migrations but will generally not include processing of personal data held on the Client's systems directly.

1.3 Purpose of processing

The purpose of processing Personal Data is solely to facilitate the provision of the Services under the Contract and the support, maintenance, administration and security of the Client's ICT environment.

1.4 Duration of the processing

Data processing will be limited strictly to the duration required to perform the Services and shall be carried out only upon the instructions of the Client. Personal Data will not be processed outside of the Client's ICT systems.

2. Types of personal data

The Contractor may have access to ICT systems containing Personal Data in the course of providing the Services. Such Personal Data may include, but is not limited to:

- Personal data of employees, contractors and temporary staff;
- Personal data of service users and members of the public;

- User account, authentication and access control information;
- Contact details including names, email addresses, telephone numbers and business addresses;
- System, audit, security and usage logs;
- Personal data contained within email, collaboration, document management and business application systems.

Where a particular support, maintenance or investigative activity requires access to Personal Data, such access shall be limited to that necessary to perform the relevant activity and shall be carried out only on the instructions of the Client.

3. Categories of data subject

The categories of Data Subjects whose Personal Data may be processed include:

- Employees and former employees of the Client;
- Contractors, consultants and agency personnel;
- Locally engaged staff and personnel at overseas missions;
- Service users and members of the public;
- Suppliers, service providers and business contacts;
- Any other individuals whose Personal Data is contained within systems supported by the Contractor in the course of delivering the Services.

Appendix 7: European Single Procurement Document (ESPD)

Please see separate document available in the Tender Documents section of eTenders under this RFT.

Appendix 8: Tender Response Document (TRD)

Please see separate document available in the Tender Documents section of eTenders under this RFT.

Please note that the structure set out in the Tender Response Document must not be altered and should be maintained in ALL responses. Failure to do so will result in the response being disqualified.

END OF DOCUMENT