



NATIONAL TRANSPORT AUTHORITY

and

[•]

AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES

CONTENTS

CLAUSE	PAGE
1. Definitions and Interpretation	6
2. Duration	10
3. Obligations of the Parties	10
4. Service Levels	11
5. Change Control	11
6. Project Governance	11
7. Status of the Supplier and Employee Matters	11
8. Key Personnel	15
9. Maintenance of records	16
10. Payment	16
11. Title, Ownership and Licensing	18
12. Assignment, Sub-Contracting and Novation	19
13. Confidentiality	19
14. Conflict of Interest.....	20
15. Intellectual Property Indemnity	21
16. Warranties.....	22
17. Force Majeure	22
18. Termination.....	23
19. Transfer of Undertakings.....	25
20. Liability.....	28

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

21.	Insurance obligations	28
22.	Dispute Resolution.....	29
23.	Data Protection.....	30
24.	Authority Locations and Policies.....	32
25.	Notices	32
26.	Waiver, Delay and Remedies.....	33
27.	Amendment or variation	34
28.	Non-Exclusivity	34
29.	Severance	34
30.	Counterparts.....	34
31.	Entire Agreement	34
32.	Governing Law	34
33.	Third Party Agreement.....	34
	SCHEDULE 1 – Services Specification Document	37
	SCHEDULE 2 – Payments Schedule.....	59
	SCHEDULE 3 – Key Personnel.....	65
	SCHEDULE 4 – Service Level Agreement.....	75
	SCHEDULE 5 – Contract Change Control	95
	SCHEDULE 6 – Exit Management Plan.....	102
	SCHEDULE 7 – Data Processing Obligations	112
	Appendix A – Target Service Levels for KPIs	115

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Appendix B – Target Service Levels for Pls 129

Appendix C – Standard Reports 131

[•]

THIS AGREEMENT is made on [•] 20

BETWEEN:

- (1) **NATIONAL TRANSPORT AUTHORITY**, a statutory corporation established under the laws of Ireland pursuant to an Act of the Oireachtas, and having its principal office at National Transport Authority, Haymarket House, Smithfield, Dublin 7, D07 CF98 (the “**Authority**”); and
- (2) [•], a company incorporated under the laws of [•] with registration number [•] and having its registered office at [•] (the “**Supplier**”).

RECITALS

- A. The Authority has been established pursuant to the Dublin Transport Authority Act 2008 and has such powers, functions and responsibilities as are conferred on it by law and, in particular, the Dublin Transport Authority Act 2008 and the Public Transport Regulation Act 2009.
- B. The Authority requires the supply of the Services.
- C. The Authority has conducted a public tender competition in connection with such supply of the Services.
- D. The Supplier is engaged in the business of providing services of the type contemplated by this Agreement and has the necessary skill, knowledge, expertise and experience in the supply of the Services.
- E. The Supplier has submitted a tender for the supply of the Services and has been selected by the Authority as the successful tenderer.

NOW IT IS AGREED AS FOLLOWS

1. Definitions and Interpretation

1.1 Definitions

In this Agreement (including the Recitals), except where the context requires otherwise:

“Affected Party” has the meaning given to it in clause 18.1;

“Agreed Sub-Contractors” means [•] and any other sub-contractor agreed by the Authority in accordance with the provisions of clause 12.2;

“Applicable Law” means any law applicable in Ireland (without further enactment) or any other applicable jurisdiction and shall include without limitation, common law, statute, statutory instrument, proclamation, bye-law, directive, decision, regulation, rule, order, notice, code of practice, code of conduct, rule of court, instruments, or delegated or subordinate legislation;

“Associated Companies” means the Supplier and any undertaking which from time to time is a subsidiary undertaking of the Supplier or is the parent undertaking of the Supplier or ultimate parent undertaking of the Supplier or a subsidiary undertaking of any such parent undertaking and for the purposes of this definition “subsidiary undertaking” and “parent undertaking” shall have the meanings given to them in the European Communities (Companies: Group Accounts) Regulations 1992;

“Authority Locations” means the locations nominated by the Authority;

“Authority Policies” means all internal policies of the Authority which apply in the normal course to the Authority’s employees, agents and sub-contractors including, without limitation, policies relating to health and safety, IT security, data privacy and acceptable usage of e-mail, internet and intranet;

“Authority Project Manager” shall have the meaning set out in clause 6.1;

“CEDR” means the International Centre for Effective Dispute Resolution;

“Change Control Procedure” means the change control procedure set out in Schedule 5;

“Commencement Date” means the date of this Agreement;

“Confidential Information” means all information and knowledge received by a party (the **“Receiving Party”**) in the course of the Services or in connection with this Agreement which is the property of the other party (the **“Disclosing Party”**) or is in the control or possession of the Disclosing Party (whether or not the subject of a separate non-disclosure or confidentiality agreement between the Disclosing Party and any third party), whether verbal, written or existing, stored or communicated in any form or medium, together with all copies thereof, however and whenever made, and includes data, documents, reports, analysis, tests, specifications, charts, plans, drawings, models, ideas, schemes, correspondence, communications, lists, manuals, computer programs, software, technology, techniques, methods, processes, services, routines, systems, procedures, practices, operations, modes of operation, apparatus, equipment, business opportunities, financial information, and/or know-how and trade or other secrets, but excluding:

information or knowledge which is or hereafter becomes part of the public domain through no fault of the Receiving Party or its personnel;

information or knowledge which is, legally and as a matter of right, in the Receiving Party’s possession as of the date of this Agreement and not the subject of another non-disclosure or confidentiality agreement between the Disclosing Party and the Receiving Party;

information or knowledge which has been or is hereafter furnished or made known to the Receiving Party, legally and as a matter of right, by third parties without any restriction on use or disclosure; and

information or knowledge which is bona fide independently developed by the Receiving Party provided that such information or knowledge has been developed entirely without reference to, or consideration of, the information or knowledge referred to in clause 13;

“Customised Materials” shall have the meaning set out in clause 11.1;

“Data Protection Acts” means the Data Protection Act 2018, and Regulation (EU) 2016/679 (General Data Protection Regulation);

“Deliverables” means the deliverables to be provided by the Supplier as set out in the Services Specification Document;

“Employee Liabilities” means costs (including the cost of wages, salaries and other remuneration or benefits), taxation or other deductions required by law, PRSI payments, redundancy payments, levies, losses, claims, demands, actions, fines, penalties, awards, liabilities, expenses (including legal expenses on an indemnity basis), in each case howsoever arising;

“Exit Management Plan” shall have the meaning set out in Schedule 6;

“Farshore resources” means contractor personnel who are based outside the EU, EEA and the United Kingdom subject to compliance with Clause 23;

“Force Majeure” shall, in relation to either party, include any event beyond the reasonable control of that party including act of God, war, riot, civil commotion, malicious damage, national official strike or lock-out, accident, fire, flood or storm and which could not have been avoided by taking reasonable precautions;

“Index” means the consumer price index (all items) of Ireland published from time to time by the Central Statistics Office;

“Instructions to Tenderers” means the request for tender issued by the Authority on [•];

“Intellectual Property” means all intellectual and/or industrial property rights including copyright, patents, design rights, trade secrets, rights in confidential information, trade marks, trade names, domain names, service marks, utility models, moral rights, topography rights, rights in databases and know-how in all cases whether or not registered or registerable and including registrations and applications for registration of any of these rights to apply for the same, and all rights and forms of protection of a similar nature or having equivalent or similar effect to any of these anywhere in the world;

“Key Personnel” means the personnel set out in Schedule 3 of this Agreement;

“Mediation Notice” shall have the meaning set out in clause 23.2;

“Nearshore resources” means contractor personnel who are not based in Ireland but are based in the EU, EEA or the United Kingdom;

“New Contractor” has the meaning given to it in clause 20;

“Operational Services Start Date” means the date on which the Services are fully accepted by the Authority, including the completion of the transition of any services from any incumbent service provider to the ServiceNow instance;

“Other Suppliers” means suppliers or other parties who may be providing services to the Authority from time to time;

“Payments Schedule” means Schedule 2 of this Agreement;

“Performance Points” means the performance points set out in the Service Level Agreement;

“Personnel” means employees, partners or Agreed Sub-Contractors engaged by the Supplier in the performance of the Services;

“Project Manager” shall have the meaning set out in clause 6.1;

“Prospective Tenderer” means a person or company who has submitted, or has indicated an intention to submit, a tender or expression of interest in relation to the provision of works or services of a similar type to any of the Services under this Agreement;

“Services” means the services set out in the Services Specification Document and any services ancillary, incidental or necessary thereto;

“Service Level Agreement” means the service level agreement in Schedule 4 in which details of the Service Levels and Service Credits are set out;

“Service Levels” means the service levels, including response and resolution times, set out in the Service Level Agreement;

“Services Specification Document” means the services specification document set out in Schedule 1 of this Agreement which contains details of the Services to be provided under this Agreement;

“Supplier Project Manager” shall have the meaning set out in clause 6.1;

“Tender Submission” means the tender submission submitted by the Supplier and dated [•]; and

“Working Day” means a day other than a Saturday or Sunday in Ireland on which banks are generally open for business in Dublin.

1.2 Interpretation

In this Agreement:

- i. the headings and the table of contents in this Agreement are inserted only for convenience and shall not affect its construction;

any reference to this Agreement includes reference to the Schedules hereto;

reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or statutory instrument or as contained in any subsequent re-enactment and shall include, without limitation, any statutory instrument, proclamation, bye-law, directive, decision, regulation, rule, order, notice, codes of practice, code of conduct, rule of court, instrument or delegated or other subordinate legislation made under the relevant statute;

any reference to the Supplier shall include its servants, agents and Agreed Sub-Contractors, except where the context otherwise requires;

any reference to a person will be construed so as to include any individual, firm, company, government, state or agency of a state, local authority or government body or any joint venture, association or partnership (whether or not having separate legal personality) and a reference to a person (including a party to this Agreement) includes a reference to that person's legal personal representatives, successors and assigns;

words importing the singular shall include the plural and vice versa; words importing any gender shall include every gender;

the word **“including”** shall be construed as meaning including without limitation;

[•]

the Authority shall not be imputed with knowledge of any fact, matter or thing merely because that fact, matter or thing is within the knowledge of the State's servants or agents; and

- i. the rule known as the *ejusdem generis* rule shall not apply to the interpretation of this Agreement and accordingly general words, including those introduced by "**other**" shall not be given a restrictive meaning by reason of the fact that they are preceded by words indicating a particular class of acts, matters or things and general words shall not be given a restrictive meaning by reason of the fact that they are followed by particular examples intended to be embraced by general words; and
- ii. the words in this Agreement shall bear their natural meaning.

1.3 Contra Proferentum

The parties have had the opportunity to take legal advice on this Agreement and no terms shall therefore be construed *contra proferentum*.

1.4 Ambiguities

In the event of any conflict or inconsistency between the terms of this Agreement and any document or other agreement referred to herein, such conflict shall be resolved in the following order of priority:

- i. This Agreement (not including its Schedules);
- ii. Schedules to this Agreement;
- iii. Mandatory provisions of the Instructions to Tenderers; and
- iv. the Tender Submission,

save that, where in the reasonable opinion of the Authority and at the Authority's sole discretion, the Tender Submission with a higher standard of service than another provision of this Agreement, the Tender Submission shall prevail.

2. Duration

This Agreement shall commence on the Commencement Date and, subject to earlier termination in accordance with its terms, the Agreement shall continue in full force and effect for a period of two (2) years from the Operational Services Start Date. The Authority may extend the term for any period or succession of periods up to a further three (3) years. The option to extend rests solely with the Authority and will be based on service requirements, supplier performance and the availability of funding. The full term of the Contract shall not continue for more than five (5) years from the Operational Services Start Date.

3. Obligations of the Parties

- 3.1 In consideration of the award of this contract, and the payment by the Authority of the charges to the Supplier in accordance with clause 10 and the Payments Schedule, the Supplier agrees to supply the Services to the Authority in accordance with the terms of this Agreement.
- 3.2 While this Agreement is in force the Supplier shall give the Authority such time and attention as may be necessary for the proper exercise of its duties under the Agreement.
- 3.3 The Supplier agrees to provide the Services in a timely manner, in accordance with the timeframes set out in the Services Specification Document (if any). The Supplier shall co-operate with all the Authority personnel and any third parties involved in the provision of services to the Authority to the extent reasonably required to ensure that the Services are provided in accordance with any such timeframes set out in the Services Specification Document. In the event that the Supplier fails to meet any timeframe set out in the Services Specification Document, without prejudice to any other remedies which may be available to the Authority, the Supplier shall be obliged to pay the Authority the liquidated damages set out in the Services Specification Document.

4. Service Levels

- 4.1 Without prejudice to the generality of clause 3.1, the Supplier agrees to provide the Services in accordance with the Service Level Agreement.
- 4.2 Where the Supplier fails to provide the Services in accordance with the Service Levels, the Service Credits shall apply, without prejudice to any other right or remedy to which the Authority may be entitled.

5. Change Control

Any request for material changes to the Services will be dealt with in accordance with the Change Control Procedure.

6. Project Governance

- 6.1 The Authority and the Supplier shall each appoint a project manager for the purposes of this Agreement (respectively the "**Authority Project Manager**" and the "**Supplier Project Manager**" and the term "**Project Manager**" shall be construed accordingly) who shall act as the primary point of contact in respect of all matters relating to this Agreement. Subject to the terms of clause 8 (Key Personnel) each party shall notify the other of any change in the identity of its Project Manager from time to time.
- 6.2 The parties agree to participate in regular review meetings, including without limitation meetings with any Other Suppliers or any other third parties (together with, or in the absence of, the Authority) as required by the Authority (acting reasonably).

7. Status of the Supplier and Employee Matters

7.1 Status of the Supplier

Subject to clause 24, the parties agree that the Supplier is and shall be an independent supplier and not the servant, agent or employee of the Authority.

7.2 Provision of services to other persons

Subject to clause 14, nothing in this Agreement shall preclude the Supplier from providing similar or any other services to any other person or firm except where the Authority considers such provision may create a conflict of interest, in which case the Supplier may not provide the services without first obtaining the prior written consent of the Authority, not to be unreasonably withheld.

7.3 Responsibility for Employees

It is agreed and acknowledged that:

the Supplier is fully responsible for, and the Authority has no responsibility for or to, the Supplier's employees, servants or agents;

the Supplier's employees, servants or agents shall not be entitled to any salary, wages, overtime payments, sick or holiday pay, pension, bonus or additional or fringe benefits of any kind from the Authority and such are the responsibility of the Supplier;

the Supplier shall be responsible for income tax liabilities, PRSI contributions, levies or other deductions required by law in respect of itself or its employees, servants or agents (including, for the avoidance of doubt, all PAYE deductions for tax and universal social charge contributions from the remuneration which it pays to Personnel);

the Supplier shall be responsible for the day-to-day management and control of its employees, servants and agents and the Authority shall have no such responsibility or control; and

- i. the Supplier is responsible for providing and maintaining any equipment or resources to be used by its employees, servants or agents and the Authority shall have no such responsibility (unless agreed otherwise).

The Supplier shall indemnify and keep indemnified the Authority against any claim (including but not limited to a claim for income tax, PRSI, universal social charge, any other deductions required by law and any interest and penalties thereon) which may be made against the Authority by the Revenue Commissioners, the Department of Social Protection, the Supplier's employees or any third party, or any order or award made by any tribunal or court, relating to a determination or allegation that the Supplier's employees, servants or agents are employees of the Authority, together with all costs and expenses incurred by the Authority in connection with or arising out of any such claim, order or award (including reasonable legal costs in defending such claim if necessary).

The Supplier shall indemnify and keep indemnified the Authority against Employee Liabilities arising from death or personal injury suffered by the Supplier's employees, servants or agents in providing the Services, except to the extent that such arises due to any negligent act of the Authority.

7.4 No partnership

Subject to clause 24, nothing in this Agreement shall constitute a partnership or joint venture nor establish a relationship of agency between the parties or a relationship of employment between the Authority and the Supplier's servants or agents.

7.5 No authority

The Supplier shall have no power or authority to enter into any agreement, contract or commitment for or on behalf or in the name of the Authority in connection with, or pursuant to, the provision of the Services or otherwise without the prior specific consent in writing of the Authority.

7.6 Stand-Still Period

During the 6 (six) month period preceding the date of expiry of this Agreement, or at any time after either party has given notice to terminate this Agreement, the Supplier shall not, and shall procure that its Associated Companies, contractors or sub-contractors (of any tier) shall not, without the prior written consent of the Authority:

- i. amend, or offer, promise or agree for the future to amend, terms and conditions of employment including, without limitation, the rates of remuneration (including pensions and bonuses), working hours, holidays and sick pay, of any employee employed by the Supplier or by any of its Associated Companies, contractors or sub-contractors (of any tier) whose work (or any part of it) is work undertaken for the purposes of this Agreement; or
- ii. increase or decrease the number of employees whose work (or any part of it) is work undertaken for the purposes of this contract, or make offers of employment that would have the effect of increasing the number of such employees or give notice of termination of employment that would have the effect of decreasing the number of such employees.

7.7 Employee Information

1. At any time during the term of this Agreement where notified in writing by the Authority to do so, the Supplier shall provide Employee Information (as defined below) to the Authority within 10 (ten) business days of such notice.

2. It is agreed that the Authority may disclose Employee Information to any Prospective Tenderer, but that the Authority shall not disclose Employee Information (or any part of that information) to any other person without the Supplier's consent except where the Authority is required by law or under regulatory rules to disclose such information.
3. Where Employee Information has been provided by the Supplier to the Authority, the Supplier shall:
 - i. within 10 (ten) business days of any amendment to such information, or the discovery of new relevant information, inform the Authority of any change to the information provided and/or provide any new Employee Information not previously provided;
 - ii. use its best endeavours to clarify within 10 (ten) business days any matter upon which clarification is requested by the Authority; and
 - iii. use its best endeavours to co-operate with any other reasonable request made by the Authority concerning the Employee Information or concerning the Supplier's employees or the employees of its Associated Companies, contractors or sub-contractors (of any tier).

"Employee Information" means:

1. An overview of how the Services are provided, including but not limited to setting out the total number of persons engaged by the Supplier to provide the Services and indicating in each case whether those persons are employed by the Supplier, its Associated Companies or by any of its contractors or sub-contractors of any tier; and
2. In relation to employees of the Supplier or its Associated Companies who are wholly or mainly assigned to the provision of the Services, a spreadsheet containing the following:
 - i. employee's job title and staff number
 - ii. name and address of the applicable employer (i.e. whether employed by the Supplier or an Associated Company);
 - iii. date of birth;
 - iv. details of remuneration (including salary and all benefits, perquisites, bonuses, commission, share plans, overtime or other such payments);
 - v. details of any pension scheme contributions or entitlement;
 - vi. details of any other contractual entitlements (for example health insurance, permanent health insurance and company car);
 - vii. normal working hours;
 - viii. approximate percentage of the employee's working time spent on the Services (expressed as a percentage of the total work the employee carries out for his/her employer);
 - ix. contractual annual leave entitlements and accrued annual leave;

[•]

- x. details of whether employment is permanent, temporary, part-time or fixed-term;
- xi. length of service;
- xii. notice period;
- xiii. any amendments to terms and conditions of employment covering future dates which has already been agreed; and

any contractual redundancy or severance entitlement whether express or implied; and

In relation to each person mentioned in clause 2 above, the following:

- i. terms and conditions of employment (copy contracts of employment) including details of terms incorporated from any collective agreement or arising out of any custom or practice;
- ii. employee handbook and/or policies and procedures forming part of the employees' contracts;
- iii. workforce structure and lines of responsibility;
- iv. details of any outstanding or reasonably anticipated liability for past breaches of such employment contracts;
- v. details, including expected return dates, of any employee who is on sick leave, maternity leave or other statutory or contractual leave (other than normal holiday leave) whether paid or unpaid;
- vi. details of any outstanding or potential liability under statute or otherwise (for example, any claim for unfair dismissal or discrimination or wrongful dismissal);
- vii. details of any employee grievances or current disciplinary action;
- viii. details of trade union recognition, any collective agreements, any areas of industrial dispute and any decisions or recommendations of a court or otherwise affecting the workforce that are still in effect;
- ix. details of any employees currently serving a notice period or garden leave period prior to termination of their contract; and
- x. details of any other outstanding or potential contractual liability to be met by a new contractor were it to become employer of such persons;

In relation to any employees providing the Services, whether they be employees of the Supplier, an Associated Company or contractors or subcontractors of any tier, confirmation that any such employee would not reasonably be deemed to be an employee of another employer due to his working arrangement; and

Such other information as the Authority may reasonably require in relation to the Supplier's employees or the employees of its Associated Companies, contractors or subcontractors (of any tier).

8. Key Personnel

- 8.1 Unless the Key Personnel are removed in accordance with clause 8.2, or cease to be employed by or contracted to the Supplier, are taken ill, are injured or are on maternity or paternity leave, the Supplier will use all reasonable endeavours to ensure that the Key Personnel shall continue to provide the Services to the Authority until expiry or termination of this Agreement in accordance with its terms. Subject to clause 8.2, with the exception of a member of the Key Personnel who ceases to be employed by or contracted to the Supplier, who is taken ill, is injured or is on maternity or paternity leave, the Key Personnel may only be removed by the Supplier in advance of the completion of the Services with the prior written consent of the Authority, such consent not to be unreasonably withheld. In all cases the Key Personnel (whether removed with consent or otherwise pursuant to the terms of this clause) must be replaced with an employee, servant or agent of equal or higher ability. Prior to the removal of any Key Personnel in accordance with this clause, the Supplier shall (where possible in advance of any such removal) furnish the Authority with a copy of the proposed replacement's curriculum vitae and all details required to enable the Authority to satisfy itself that the employee, servant or agent is appropriately qualified for the provision of the Services.
- 8.2 If at any time during the term of this Agreement the Authority reasonably determines that any employees, servants or agents of the Supplier are not suitable for the provision of the Services, it shall notify the Supplier of its decision and the Supplier shall immediately remove the said person(s) from the Services and replace him/her in accordance with the procedures set out in clause 8.1. The Supplier shall indemnify and keep indemnified the Authority from any Employee Liabilities that may result from such action or that relate to the removal of that person from the Service(s).

9. Maintenance of records

The Supplier shall keep detailed records of all acts and things done by it in relation to the performance of the Services and at the Authority's request shall make them available for inspection and shall, at the Supplier's own expense, provide to the Authority copies of all documentation required by the Authority at any time.

10. Payment

10.1 Basis of payment

The Authority shall pay the Supplier in accordance with the Payments Schedule. The Supplier acknowledges that payments may be subject to retention provisions as set out in the Payments Schedule.

10.2 Notification

- i. The Supplier shall, on a monthly basis (or such other period as may be requested by the Authority), notify the Authority of the time spent in carrying out the Services over the course of that month and shall produce any such record, back-up or other evidence relating to the time spent as the Authority may require.

The Supplier shall maintain records of all fees incurred in respect of the Services in electronic format (or such other format specified by the Authority). The records maintained by the Supplier shall contain details of all Services undertaken, the dates and identities of the Personnel who carried out such Services and the identities of the personnel of the Authority who authorised the carrying out of such Services. The Authority shall be entitled to inspect the Supplier's fee records upon providing notice of such inspection to the Supplier.

10.3 Payment

- i. Invoices shall be submitted to the Authority in accordance with the Payments Schedule.
- ii. Payment of any sums due (including all legally demandable VAT, at the rate for the time being properly chargeable in respect of the supply of goods and services by the Supplier under this Agreement) shall be made on a net monthly account basis such that payment is made on the last business day of the month following the month of the invoice date, provided all monies specified in the Supplier's invoice raised are due and undisputed and the invoices are valid VAT invoices and are correctly addressed. The Supplier will be responsible for any VAT due in respect of fees received under this Contract.
- iii. The Authority shall be entitled to make deductions from the payments specified in this Agreement where it is required by law or otherwise entitled to make such deductions. In particular, Professional Services Withholding Tax will be deducted at source as directed by the Revenue Commissioner from the Supplier's payment and remitted to the Revenue, if the Supplier is providing professional services.
- iv. Payment of any monies under this Agreement does not give rise to an inference that the Supplier has fulfilled its obligations to the satisfaction of the Authority or is entitled to any such payment.

10.4 Right of set-off

Where, in any case, the Supplier is liable to make any payment to the Authority under this Agreement or otherwise, the Authority may set off any such payments due to it against any fees due by the Authority to the Supplier on this or any other contract between the parties.

10.5 Current tax clearance certificate

The Supplier shall not be entitled to any payment if at any time in response to a request from the Authority the Supplier does not produce a current tax clearance

certificate from the Revenue Commissioners of Ireland confirming suitability on tax grounds.

10.6 Indexation

The Daily Rates set out in the Daily Rate Table of Schedule 2 (Payments Schedule):

- i. are fixed for the period up to the second anniversary of the Commencement Date and shall not before that date be subject to any price adjustment or escalation formula to reflect variations in currency, exchange rates, taxation, the cost of labour, materials, overheads or any other expense; and
- ii. following the second anniversary of the Commencement Date and on each subsequent anniversary of the Commencement Date (a "Readjustment Date"), upon request, shall be adjusted by the percentage increase or decrease (if any) of the Index figure current at the Readjustment Date compared with the Index figure current on the previous Readjustment Date, or, in the case of the first readjustment, compared with the Index figure current on the Commencement Date. Between Readjustment Dates, the fees as adjusted will be fixed for the year following the Readjustment Date and shall not be subject to any further price adjustment or escalation formula to reflect variations in currency, exchange rates, taxation, the cost of labour, materials, overheads or any other expense until the next Readjustment Date.

11. Title, Ownership and Licensing

- 11.1 The Supplier agrees that all Intellectual Property Rights for the full terms thereof throughout the world arising in any works or material originated, conceived, written or created specifically for the Authority by the Supplier or the Personnel, in connection with the supply of the Services (the "**Customised Materials**"), shall vest in and be the absolute property of the Authority. The Intellectual Property rights in respect of any works or material supplied in connection with the Services, which are not Customised Materials, shall vest in and be the absolute property of the Supplier and the Supplier grants to the Authority a worldwide, non-exclusive, perpetual, sub-licensable, transferable and royalty-free licence to use such works and material. The Supplier shall, at the request and expense of the Authority, do all things necessary or desirable to substantiate the rights of the Authority under this clause.
- 11.2 The Supplier hereby waives, and shall procure that the Personnel waive, all current or future moral or similar rights arising in connection with the Customised Materials insofar as they may lawfully do so in favour of the Authority and for the avoidance of doubt this waiver shall extend to the licensees and successors in title to the Intellectual Property Rights in such Customised Materials.
- 11.3 The Supplier acknowledges that all rights in any materials (including without limitation any and all computer programs, data, diagrams, charts, reports, specifications, studies, and development tools) provided by the Authority to the Supplier ("**Authority Materials**") shall at all times vest in and be the absolute property of the Authority.

- 11.4 Title to any other goods or physical media of which the Deliverables are comprised shall vest in the Authority on the earlier of delivery to the Authority or payment of any relevant charges for them. The Supplier shall do all things necessary or desirable to substantiate the rights of the Authority under this clause.

12. Assignment, Sub-Contracting and Novation

12.1 Supplier

With the exception of the Agreed Sub-Contractors, the Supplier shall not be entitled to assign and/or sub-contract any of its rights and/or obligations under this Agreement without the prior written consent of the Authority.

- 12.2 The Supplier shall procure the compliance with the terms of this Agreement by the Agreed Sub-Contractors and by any sub-contractor, servant or agent appointed by the Supplier pursuant to clause 12.1, provided that the Supplier shall remain primarily liable to the Authority for the performance of the Supplier's obligations under this Agreement notwithstanding the appointment of the Agreed Sub-Contractors or any sub-contractor, servant or agent appointed by the Supplier pursuant to clause 12.1.

12.3 Authority

The Authority may transfer, assign or novate all or any part of the terms and conditions of this Agreement to any public sector body and shall give prompt notice to the Supplier of such transfer, assignment or novation. The Supplier agrees to do all acts, and execute all documents, necessary to give effect to such transfer, assignment or novation.

13. Confidentiality

13.1 Confidential

The parties agree and acknowledge that they will keep, and will ensure that their personnel shall keep, Confidential Information confidential, and shall not at any time for any reason whatsoever disclose or permit Confidential Information to be disclosed to any third party except as permitted hereunder to enable them to carry out their duties and obligations under the Agreement.

13.2 Third parties

1. The parties shall procure that each of their employees and any other personnel having access to Confidential Information shall be subject to the same obligations as set out in this clause 13 with respect to Confidential Information and shall enter into a suitable confidentiality agreement in a form agreed by the parties or, insofar as that is not reasonably practicable, they shall take all reasonable steps to ensure that their personnel and employees are made aware of and perform such obligations.

[•]

2. The Supplier further agrees and acknowledges that it and its Personnel are subject to, and to the extent applicable shall comply with, Section 38 of the Dublin Transport Authority Act 2008.

13.3 Permitted disclosure

Either party may disclose Confidential Information:

- i. if and to the extent required by law or for the purpose of any judicial inquiry or proceedings;
- ii. if and to the extent required by any securities exchange or regulatory or governmental body to which it is subject wherever situated, including (amongst other bodies) the Public Accounts Committee, any other Oireachtas Committee, and/or the Irish Stock Exchange, whether or not the requirement to disclose the Confidential Information has the force of law;
- iii. if and to the extent necessary or desirable to enable mediation under clause 23;
- iv. where necessary, to its professional advisers, auditors and bankers;
- v. if and to the extent that it is necessary to carry out its Services hereunder;
- vi. in the case of a disclosure by the Supplier, if and to the extent that the Authority has given prior written consent to the disclosure; or
- vii. in the case of the Authority, pursuant to an access request under the Freedom of Information Acts 2014 (the “**FOI Acts**”), subject where relevant to the Authority seeking submission from the Supplier in accordance with Section 38 of the FOI Acts.

14. Conflict of Interest

14.1 No conflict

The Supplier agrees and acknowledges that:

- i. it and its Personnel are subject to, and to the extent applicable shall comply with, Section 37 of the Dublin Transport Act 2008; and
- ii. without prejudice to the generality of clause 14.1(a), shall ensure that no conflict of interest arises in respect of its performance of the Services under this Agreement.

14.2 Disclosure

The Supplier shall disclose to the Authority, within forty-eight hours of it coming to its attention, any conflict of interest or potential conflict of interest which it, any of its affiliates, Associated Companies, or any of its Agreed Sub-Contractors may have in performing the Services.

14.3 Authority rights

In the event of any conflict or potential conflict of interest arising, the Supplier agrees and acknowledges that it is a matter for the Authority to decide the appropriate action to be taken (including termination of contract) in accordance with Section 37 of the Dublin Transport Act 2008 and the terms of this Agreement.

14.4 Supplier warranty

The Supplier hereby expressly agrees and warrants that for the duration of this Agreement neither the Supplier nor any of its Agreed Sub-Contractors shall, unless otherwise agreed in advance with the Authority, provide any advice to any person other than in accordance with this Agreement in connection with any matter connected with the Services.

14.5 Third parties

The Supplier shall ensure that its Personnel comply with this clause 14 and Section 38 of the Dublin Transport Authority Act 2008 as if they were a party to this Agreement.

15. Intellectual Property Indemnity

15.1 The Supplier shall indemnify the Authority against all damages, costs, charges and expenses arising from or incurred by reason of any infringement or alleged infringement of any third party Intellectual Property Rights in consequence of the use or possession of any Deliverables (or any part thereof) by the Authority and the supply of the Services (or any part thereof) by the Supplier under this Agreement, subject to the following:

- (a) the Authority shall promptly notify the Supplier in writing of any alleged infringement of which he has notice;
- (b) the Authority must make no admissions without the Supplier's prior written consent; and
- (c) the Authority, at the Supplier's request and expense, shall allow the Supplier to conduct any negotiations or litigation and/or settle any claim. The Authority shall give the Supplier all reasonable assistance. The costs incurred or recovered in such negotiations or settled claim shall be for the Supplier's account.
- (d) If at any time an allegation of infringement of Intellectual Property Rights is made in respect of the Services (or any part thereof) or, if in the Supplier's reasonable opinion such an allegation is likely to be made, the Supplier may at his own expense modify or replace the Services (or any part thereof) so as to avoid the infringement, without detracting from overall performance, the Supplier making good to the Authority any loss of use during modification or replacement.

15.2 Rights of Third Parties

Nothing in this Agreement confers or purports to confer on any third party any benefit or any right to enforce any term of this Agreement.

16. Warranties

- 16.1 The Supplier warrants that the Deliverables, and any other equipment or materials to be provided to the Authority under this Agreement, shall be fit for purpose and free from material defects in normal use.
- 16.2 The Authority shall give notice to the Supplier as soon as practicable upon becoming aware of any breach of the warranty in clause 16.1. Without prejudice to any other rights and remedies to which the Authority may be entitled under this Agreement or otherwise, the Supplier shall after receipt of notice of a breach of warranty remedy same by repair or replacement of the Deliverables, or the equipment or materials, in question without charge to the Authority so as to ensure that the item in question complies with the warranty in clause 17.1.
- 16.3 The Supplier warrants that the Services shall be provided by appropriately experienced, qualified and trained personnel and that the Services shall be rendered with all due skill, care and diligence.
- 16.4 The Supplier warrants that the provision of the Services will not infringe the Intellectual Property Rights of any third parties.
- 16.5 The Supplier warrants that it has the authority to enter into this Agreement and to perform its obligations under this Agreement and that no material conflict of interest shall arise for the Supplier by virtue of the Supplier entering this Agreement.
- 16.6 The Supplier warrants that all information supplied by the Supplier in the Tender Submission is true and accurate in all respects as at the date of this Agreement save as otherwise disclosed in writing to the Authority.
- 16.7 The Supplier warrants that it shall:
- iii. observe and comply with all Applicable Law to the extent that such laws are relevant to the performance of its obligations under this Agreement; and
 - iv. obtain at its own risk and expense from the appropriate authorities or any third parties all permits and licences necessary for the proper performance of its obligations under this Agreement.
- 16.8 The Supplier warrants that it is a company duly incorporated and validly existing under the laws of Ireland.

17. Force Majeure

17.1 Affected Party obligations

If a party is affected by a Force Majeure then the party so affected (the “**Affected Party**”) shall promptly notify the other party in writing of the nature and extent of the circumstances in question and both parties shall consult each other and make

every reasonable effort to mitigate the effect of such Force Majeure on the Affected Party's ability to perform its obligations under this Agreement.

17.2 Effect of Force Majeure

- (a) Notwithstanding any other provisions of this Agreement, but subject to clause 18.2(c), the Affected Party shall be deemed not to be in breach of this Agreement or otherwise be liable to the other party for any delay in performance or non-performance of its obligations under this Agreement arising from the operation of a Force Majeure which it has notified to the other party. The time for the performance of obligations affected by a Force Majeure which has been duly notified to the other party shall, subject to clause 18.2(c), be extended until such time as the Force Majeure ceases to exist.
- (b) The Affected Party shall notify the other party immediately in writing once the Force Majeure has ended and shall forthwith resume performance of its obligations under this Agreement.
- (c) If any circumstances of Force Majeure exist for a continuous period of six months then the Authority shall be entitled to terminate the Supplier's appointment under this Agreement forthwith by giving notice in writing to the Supplier.

18. Termination

18.1 Termination Events

This Agreement may be terminated by the Authority immediately in writing (without prejudice to any other rights and remedies which it may possess):

- (a) if in the reasonable opinion of the Authority there has been material breach, default or negligence by the Supplier or flagrant or persistent neglect by the Supplier of its obligations under this Agreement and, the Authority having served written notice on the Supplier notifying it of the breach, default or negligence, the Supplier has failed to remedy such breach, default or negligence within a period of ten Working Days of such notification;
- (b) if the Supplier (or, where the Supplier is a partnership, any partner in the Supplier) becomes bankrupt or compounds or makes any arrangement with or for the benefit of its creditors or (where the Supplier is a company) enters into compulsory or voluntary liquidation or amalgamation (other than for the purpose of a bona fide reconstruction or amalgamation without insolvency) or the Supplier has a receiver or manager appointed to its undertakings or if any security is enforced against any asset of the Supplier or any distress or execution shall be threatened or levied upon any asset of the Supplier or if the Supplier is unable to pay its debts in accordance with the law relating to this Agreement;

[•]

- i. if the Supplier has been guilty of conduct tending to bring itself or the Authority into disrepute;
- ii. if funding of the Authority in connection with the matter the subject of the Services shall cease; or
- iii. if the performance of the Supplier's duties hereunder is not satisfactory in the reasonable opinion of the Authority.

18.2 The Agreement may be terminated by the Authority immediately in writing where:

- (a) in the reasonable opinion of the Authority, the Agreement has been subject to substantial modification, which would require a new procurement procedure pursuant to Article 72 of Directive 2014/24/EU and/or Regulation 72 of the European Union (Award of Public Authority Contracts) Regulations 2016; or
- (b) the Supplier has, at the time of the award of the Agreement, been in one of the situations referred to in Article 57(1) of Directive 2014/24/EU of the European Parliament and of the Council, and/ or Regulation 57(1) or (2) of the European Union (Award of Public Authority Contracts) Regulations 2016 and should therefore have been excluded from the procurement procedure for this Agreement; or
- (c) the Agreement should not have been awarded to the Supplier in view of a serious infringement of the obligations under the Treaties governing the European Union and/or Directive 2014/24/EU and/or the European Union (Award of Public Authority Contracts) Regulations 2016, which infringement has been declared by the Court of Justice of the European Union in a procedure under Article 258 of the Treaty on the Functioning of the European Union

18.3 Authority voluntary right

This Agreement may be terminated by the Authority at any time on giving 3 months' written notice to the Supplier. In such circumstances the Authority shall pay the Supplier for all Services which have been performed in accordance with the terms of this Agreement up to and including the date of termination.

18.4 Supplier waiver

Without prejudice to any other clause of this Agreement, the Supplier waives any rights it may have under this Agreement, under statute, in equity or otherwise at law to seek compensation for loss of profit, loss of business or any indirect or consequential losses resulting from the Authority's termination of this Agreement, including, without limitation, pursuant to clause 19.1, 19.2 [or 19.3,].

18.5 Consequences of termination

The parties shall develop an Exit Management Plan in accordance with the provisions of Schedule 6. On termination of this Agreement for any reason, the provisions of the Exit Management Plan shall apply. For the avoidance of doubt, the Supplier shall have no lien on documents in its possession or under its control for payment due to it by the Authority.

18.6 Without prejudice

The provisions of this clause 19 are and shall be without prejudice to any other rights or remedies which the Authority may have.

19. Transfer of Undertakings

19.1 In this clause; 19

“Employee” means any employee of the Existing Contractor or of any third party whose terms and conditions of employment transfer to the Supplier under Regulation 4 of the Transfer Regulations;

“Existing Contractor” means [•], the contractor currently providing some or all of the services the subject of this Agreement;

“New Contractor” means the Authority or any third party that will provide some or all of the Services on the termination or expiry of this Agreement;

“Retransfer Date” means the date on which the relevant Retransferring Employee transfers to a New Contractor in accordance with the Transfer Regulations;

“Retransferring Employee” means any employee of the Supplier or of any third party whose terms and conditions of employment transfer to a New Contractor under Regulation 4 of the Transfer Regulations on the termination or otherwise of this Agreement;

“Transfer Date” means the date on which the Employees transfer to the Supplier in accordance with the Transfer Regulations; and

“Transfer Regulations” means the European Communities (Protection of Employees on Transfer of Undertakings) Regulations 2003, including any statute or statutory provision which amends, extends, consolidates or replaces the same.

19.2 The Parties acknowledge that the Transfer Regulations may apply on or following the commencement of this Agreement such that persons currently providing all or part of the Services would transfer to the Supplier and that, should the Transfer Regulations apply, the contracts of employment of the Employees (save insofar as excluded under Regulation 4 of the Transfer Regulations) will have effect from the Transfer Date as if originally made between the Supplier and the Employees. However, the Supplier acknowledges and agrees that it shall be liable for all Employee Liabilities resulting from the application or alleged application of the Transfer Regulations on, or following, commencement of this Agreement, that the Authority has made no representations regarding the Transfer Regulations and that the Authority has not provided any warranty or indemnity of any nature regarding the application of the Transfer Regulations or the identity of the persons who may transfer to the Supplier in accordance with the Transfer Regulations.

19.3 If the Transfer Regulations apply on or following commencement of this Agreement, it is agreed that:

- (a) the Supplier shall comply with its obligations under the Transfer Regulations;
- (b) the Authority shall provide information and assistance so far as it is reasonably able to do so in order to allow the Supplier to so comply with its obligations under the Transfer Regulations, including using reasonable endeavours to obtain from the Existing Contractor (or other applicable employer) details of the Employees' existing contractual rights and obligations. However, the Authority neither warrants, represents nor takes responsibility for the accuracy of information so obtained from the Existing Contractor and provided to the Supplier; and
- (c) the Supplier shall indemnify the Authority and keep the Authority indemnified on demand against any and all Employee Liabilities relating to Employees (or persons claiming to be Employees) arising from:
 - i. a refusal to employ such person;
 - ii. the employment or termination of such person's employment by the Supplier after the Transfer Date;
 - iii. any changes in such person's terms and conditions of employment after the Transfer Date;
 - iv. any failure by the Supplier to comply with the Transfer Regulations, including the information and consultation requirements in Regulation 8; and
 - v. any failure by the Supplier to comply with its obligations under this clause 19.3.

19.4 It is acknowledged and agreed that if, on the termination or expiry of all or part of this Agreement, the provision of some or all of the Services pursuant to it are transferred to a New Contractor and such transfer constitutes a transfer within the meaning of the Transfer Regulations, then the provisions of clauses 20.5 to 20.7 below shall apply.

19.5 The Supplier shall comply with its obligations under the Transfer Regulations, including its information and consultation obligations under Regulation 8 of the Transfer Regulations, and it shall provide any reasonably necessary information and assistance to a New Contractor to allow that party to comply with its obligations (including providing a list of Retransferring Employees together with their terms and conditions of employment and allowing the New Contractor to address Retransferring Employees as is reasonably necessary in the lead up to the Retransfer Date).

19.6 The Supplier shall indemnify the Authority and the New Contractor and keep the Authority and New Contractor indemnified on demand against any and all Employee Liabilities relating to Retransferring Employees (or a person claiming his employment should transfer to the New Contractor) arising from:

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICE NOW INSTANCES AGREEMENT

[•]

- (a) any claim which relates to such person's employment by the Supplier before the Retransfer Date;
- (b) the employment or termination of such person's employment by the Supplier before the Retransfer Date;
- (c) any changes in such person's terms and conditions of employment before the Retransfer Date;
- (d) any failure by the Supplier to comply with the Transfer Regulations, including the information and consultation requirements in Regulation 8;
- (e) a failure by the Supplier to provide an accurate list of Retransferring Employees together with their terms and conditions of employment; and
- (f) the non-disclosure or inaccurate disclosure of Employee Information.

19.7 If it is alleged that the provisions of the Transfer Regulations operate so as to transfer to the New Contractor a person other than a Retransferring Employee whose identity was notified to the New Contractor in accordance with clause 19.5 above:

- (a) the New Contractor shall, upon becoming aware of the alleged application of the Transfer Regulations to such person, inform the Supplier, and the Supplier shall within 5 (five) business days:
 - i. provide all relevant information to the New Contractor relating to such person and his employment as reasonably requested by the New Contractor; and
 - ii. consult with the New Contractor in good faith as to the appropriate steps to be taken in relation to that person;
- (b) the Supplier shall, within 10 (ten) business days, offer such person employment on their same terms and conditions of employment; and
- (c) the Supplier covenants to pay to the New Contractor on demand an amount equal to any and all Employee Liabilities arising out of such person's employment and/or the termination of such person's employment, so long as such termination takes place within 2 (two) months of the New Contractor becoming aware of such allegation.

19.8 The Authority holds the benefit of any indemnities, covenants, agreements or warranties provided under this clause 19 (or any sub-clauses hereof) for itself and in trust for any nominee or New Contractor, and the Supplier agrees that the Authority has the right at its sole discretion to assign the benefit of such indemnities to a New Contractor or that, when requested to do so by the Authority, the Supplier shall execute indemnities, covenants, agreements or warranties in similar terms as this clause 19 in favour of a New Contractor.

19.9 Where the Supplier chooses to provide all or any part of the Services through an Associated Company, contractor or subcontractor:

- (a) the term "Supplier" shall be interpreted where necessary as including such Associated Company; and
- (b) the Supplier shall ensure that any such Associated Company, and any contractors or subcontractors providing some or all of the Services, comply with the Transfer Regulations (if applicable) and any obligations to provide information or assistance to the Authority or a New Contractor in the same manner as such applies to the Supplier.

20. Liability

- 20.1 Save in respect of death or personal injury caused by the negligence of either party, breach of this Agreement by virtue of fraud or wilful default, or breach of any Intellectual Property Rights by the Supplier (including, for the avoidance of doubt, any liability under the indemnity at clause 15), each party's liability for any claim whether in contract, tort (including negligence) or otherwise, for any loss or damage, arising out of or in connection with this Agreement or otherwise shall in no case exceed 200% of sums paid and payable by the Authority under this Agreement in respect of any event or series of connected events.
- 20.2 In no event shall either party be liable for special, incidental, indirect or consequential damages.

21. Insurance obligations

- 21.1 The Supplier shall be required at all times during the term of this Agreement, and for a period of 2 years thereafter, to effect and maintain such levels of insurance with a reputable insurer as may be required to cover any potential liability of the Supplier under this Agreement.
- 21.2 Without prejudice to the generality of clause 22.1, the Supplier shall, as a minimum, carry throughout the term of this Agreement the levels and types of insurance set out below under forms of policy which are acceptable to the Authority, acting reasonably:
- i. Professional Indemnity: €6,500,000 per claim and unlimited in the aggregate
 - ii. Employer's Liability: €13,000,000 per claim and unlimited in the aggregate
 - iii. Public Liability: €6,500,000 per claim and unlimited in the aggregate
 - iv. Product Liability: €6,500,000 per claim and unlimited in the aggregate
- 21.3 The Supplier shall notify the Authority immediately in the event that any of the insurances described in clause 22.2 ceases to be available or maintained.

[•]

- 21.4 The insurance policies described in clause 22.2 shall include an indemnity to principals clause specifically indemnifying the Authority. None of the policies described in clause 22.2 shall include any terms or conditions to the effect that the Supplier must discharge any liability before being able to recover from the insurers.
- 21.5 If the Supplier fails to provide the insurance cover specified in clause 22.2, the Authority may do so for the whole or part of the period for which such cover is required, without being under any obligation so to do, and may deduct any costs it incurs in obtaining such cover from any sums due to the Supplier under this Agreement, or otherwise recover such sums from the Supplier.
- 21.6 The Supplier shall be liable to pay the full amount of any deductibles or excess amounts payable under the policies of insurance referred to in clause 22.2 in the event of a claim under any of the policies.

22. Dispute Resolution

- 22.1 The parties shall use all reasonable endeavours to settle any dispute that may arise in connection with this Agreement.
- 22.2 If any dispute cannot be settled amicably by the Authority Project Manager and the Supplier Project Manager within 10 Business Days, the dispute shall be referred to the Authority's [•] and the Supplier's [•]. The Authority's [•] and the Supplier's [•] will use all reasonable endeavours to resolve the dispute. If the dispute is not resolved by the Authority's [•] and the Supplier's [•] within 10 Business Days of the matter being referred to them, the parties will refer the dispute to mediation in accordance with the CEDR procedures then in force before resorting to litigation. The mediation process will be commenced by service by one party on the other of a written notice that the issue is to be referred to mediation (the "**Mediation Notice**"). The parties shall agree on a choice of mediator with sufficient knowledge and experience in the industry sufficient to comprehend the technical and economic issues raised. In the event that the parties are unable to agree on a choice of mediator within 10 Business Days of the date of service of the Mediation Notice, the parties shall accept a mediator nominated by CEDR. The costs of the mediation shall be shared equally between the parties.
- 22.3 Nothing contained in this clause 23 shall restrict either party's freedom to commence legal proceedings where such proceedings are required urgently to preserve any legal right or remedy, to protect any Intellectual Property Rights or rights in Confidential Information or to otherwise prevent irreparable harm.

23. Data Protection

23.1 The Service Provider acknowledges that in providing the Services under this Agreement the Service Provider will process personal data within the meaning set out in Data Protection Law on behalf of the Authority. In such circumstances, the Service Provider acknowledges that the Authority is the data controller and the Service Provider is the data processor, as each term is defined in the Data Protection Acts and the Service Provider agrees that:

- i. the Service Provider processes personal data on behalf of the Authority in the context of providing the services under this Agreement, for the duration of the Term. The obligations and rights of the Authority shall be as set out in this Agreement;
- ii. the Service Provider will only process such personal data in accordance with the documented instructions of the Authority, including with regard to transfers of personal data to a third country and solely as strictly necessary for the performance of its obligations under this Agreement;
- iii. the Service Provider shall ensure that the persons authorised by the Service Provider to process such personal data are bound by appropriate confidentiality obligations;
- iv. the Service Provider shall implement such technical and organisational security measures as are required to comply with the data security obligations under Data Protection Law;
- v. the Service Provider shall not engage any sub-processor without the prior written consent of the Authority and where the Authority has consented to the appointment of a sub-processor, the Service Provider must not replace or engage other sub-processors without the prior written consent of the Authority;
- vi. where any sub-contractor of the Service Provider will be processing such personal data on behalf of the Authority, the Service Provider shall ensure that a written contract exists between the Service Provider and the Sub-contractor containing clauses equivalent to those imposed on the Service Provider in this clause 24. In the event that any sub-processor fails to meet its data protection obligations, the Service Provider shall remain fully liable to the Authority for the performance of the sub-processors obligations;
- vii. the Service Provider shall inform the Authority immediately in the event of receiving a request from a data subject to exercise their rights under Data Protection Law and provide such co-operation and assistance as may be required to enable the Authority to deal with such request in accordance with the provisions of Data Protection Law;

- viii. the Service Provider shall assist the Authority by implementing appropriate technical and organisational measures to allow the Authority to comply with requests from data subjects to exercise their rights under Data Protection Law;
- ix. the Service Provider shall assist the Authority in ensuring compliance with its obligations in respect of security of personal data under Data Protection Law;
- x. the Service Provider shall: (i) at the choice of the Authority, delete or return all such personal data to the Authority when the Service Provider ceases to provide service relating to data processing; and (ii) save as required by Applicable Law, delete all existing copies of such personal data unless EU law or the laws of an EU Member State require storage of the personal data;
- xi. the Service Provider shall: (i) make available to the Authority all information necessary to demonstrate compliance with the obligations laid down in this clause 24; and (ii) allow for and assist with audits, including inspections, conducted by the Authority or another auditor mandated by the Authority, in order to ensure compliance with the obligations laid down in this clause 24, including its data security obligations under Data Protection Law provided however that the Authority shall be entitled, at its discretion, to accept adherence by the Service Provider to an approved code of conduct or an approved certification mechanism to aid demonstration by the Service Provider that it is compliant with the provisions of this clause 24;
- xii. the Service Provider shall inform the Authority immediately if, in its opinion, it receives an instruction from the Authority which infringes Data Protection Law;
- xiii. the Service Provider shall notify the Authority immediately after becoming aware of any personal data breach (as defined in Data Protection Law) and provide the Authority with such co-operation and assistance as may be required to mitigate against the effects of, and comply with any reporting obligations which may apply in respect of, any such breach; and
- xiv. no such personal data shall be transferred outside of the European Economic Area by the Service Provider or any of its agents or sub-processors without the prior written consent of the Authority which consent may be subject to terms and conditions (including, without limitation, that the data importer enters into model clauses in the form approved by the European Commission and, where relevant, complies with the provisions regarding sub-processors contained in such model contracts in respect of any sub-processors). The Service Provider shall comply with the requirements of Data Protection law in respect of transfers of such personal data outside of the European Economic Area, to the extent that the Authority consents to any such transfer.

23.2 For the purposes of this clause 24, but not for any other purpose under this Agreement, the Authority appoints the Service Provider as its agent.

24. Authority Locations and Policies

24.1 The Authority shall afford to appropriate personnel of the Supplier, and its sub-contractors, servants and agents, at all reasonable times and upon receipt of adequate prior notice, such access to the Authority Locations as may be necessary for the performance of the Supplier's obligations hereunder provided always that such personnel comply with the terms of any Authority Policies notified by the Authority to the Supplier from time to time. The Authority shall have the right to refuse admission to, or order the removal from, the Authority Locations of any person who is in breach of any rule relating to safety whilst at the Authority Locations where such rule has previously been brought to the attention of the Supplier or who, in the opinion of the Authority, is in breach of the Authority Policies or who is under the influence of alcohol or drugs whilst at the Authority Locations. The Authority shall confirm action taken pursuant to this clause forthwith in writing to the Supplier.

24.2 The Supplier shall use best endeavours to ensure that in performing its obligations under this Agreement it does not disrupt the operations of or, save as may be reasonably unavoidable, inconvenience the Authority, its employees, agents, customers or service providers, or any other persons, including at the Authority Locations.

25. Notices

25.1 Communications in writing

Any communication to be made under or in connection with this Agreement shall be made in writing and, unless otherwise stated, may be made by fax or letter.

25.2 Addresses

The address and fax number (and the department or officer, if any, for whose attention the communication is to be made) of each party for any communication or document to be made or delivered under or in connection with this Agreement is:

in the case of the Authority:

National Transport Authority
Address: National Transport Authority (NTA)
Haymarket House
Smithfield
Dublin 7
D07 CF98
Facsimile no: +353 (0)1 879 8333
Attention: [To be inserted]

in the case of the Supplier:

[name of Supplier]
Address: Facsimile no: Attention:

*[To be inserted]**[To be inserted]**[To be inserted]*

or such other address or facsimile number as may be notified to the other party to this Agreement, such notice to take effect not less than five Working Days' after the service of the notice.

25.3 Delivery

Subject to clause 26.3(b), a communication or document made or delivered by one person to another under or in connection with this Agreement will only be effective:

- (a) if by way of fax, when received in legible form; or
- (b) if by way of letter, when it has been left at the relevant address or five Working Days' after being deposited in the post postage prepaid in an envelope addressed to it at that address,
 - i. and, if a particular department or officer is specified as part of its address details provided under Clause 26.2, if addressed to that department or officer.
- (c) Any communication or document to be made or delivered to the Authority will be effective only when actually received by the Authority and then only if it is expressly marked for the attention of the department or officer identified with the Authority's signature below (or any substitute department or officer as the Authority shall specify for this purpose).

25.4 English language

- (a) Any notice given under or in connection with this Agreement must be in English.
- (b) All other documents provided under or in connection with this Agreement must be:
 - i. in English, or
 - ii. if not in English, and if so required by the Authority, accompanied by a certified English translation and, in this case, the English translation will prevail unless the document is a constitutional, statutory or other official document.

26. Waiver, Delay and Remedies

26.1 No waiver

The failure by either party to enforce any provision of this Agreement will in no way affect its right thereafter to require complete performance by the other party nor will the waiver of any breach of any provision be taken or held to be a waiver of any subsequent breach of any provisions or be a waiver of the provision itself.

26.2 Delay

No failure or delay by the Authority in exercising any claim, remedy, right, power or privilege under this Agreement shall operate as a waiver nor shall a single or partial exercise of any claim, remedy, right, power or privilege preclude any further exercise thereof or exercise of any other claim, remedy, right, power or privilege.

26.3 Remedies cumulative

Except where this Agreement provides otherwise, the rights and remedies contained in this Agreement are cumulative and not exclusive of rights or remedies provided by law.

27. Amendment or variation

An amendment or variation of this Agreement is valid only if it is in writing and signed by or on behalf of each party.

28. Non-Exclusivity

The Authority shall at all times be entitled to enter into separate contracts for the provision of any or all services the same as or similar to the Services with persons other than the Supplier. Nothing in this Agreement shall create an exclusive relationship between the Authority and the Supplier for the provision of Services.

29. Severance

Each of the provisions of this Agreement is severable and distinct from the others and if at any time one or more of such provisions become invalid, illegal or unenforceable then the validity and legality or enforceability of the remaining provisions hereof shall not in any way be affected or impaired thereby.

30. Counterparts

This Agreement may be executed in any number of counterparts and by different parties hereto on separate counterparts, each of which, when executed and delivered, shall constitute one and the same instrument.

31. Entire Agreement

This Agreement (including its Schedules) contains the entire agreement between the parties with respect to its subject matter, supersedes all previous agreements and understandings between the parties with respect to its subject matter, and may not be modified except in accordance with clause 28.

32. Governing Law

The laws of Ireland govern the construction, validity and performance of this Agreement.

33. Third Party Agreement

33.1 Third Party Agreement

The Supplier may arrange or procure on behalf of the Authority a separate agreement between any third party licensor of software or supplier of software-as-a service and the Authority, subject to Authority approval of the terms of the separate agreement in question and agreement of all parties that in the event of any conflict or inconsistency between the terms of this Agreement and the terms set out in any such separate agreement, that the terms of this Agreement shall take priority.

33.2 Terms of Third Party Agreement

The Supplier shall ensure that any separate agreement between any third party licensor of software or supplier of software-as-a-service services and the Authority that the Supplier arranges or procures on behalf of the Authority shall include, at least, the following provisions:

- i. a licence to use the software/system that permits use not only by Authority personnel but also by third party service providers acting on behalf of the Authority;
- ii. reasonable support and maintenance provisions, with appropriate service level arrangements including in respect of response times and resolution times;
- iii. appropriate security and confidentiality obligations on the third party licensor of software or supplier of software-as-a-service service;
- iv. appropriate service continuity and disaster recovery obligations on the third party licensor of software or supplier of software-as-a-service service;
- v. appropriate data protection provisions and obligations on the third party licensor of software or supplier of software-as-a-service service, to the extent that the supplier will process any personal data on behalf of the Authority;
- vi. an obligation on the third party licensor of software or supplier of software-as-a-service service to comply with all applicable laws;
- vii. on obligation on the third party licensor of software or supplier of software-as-a-service service to comply with any Authority policies to the extent relevant to the services to be provided by the third party licensor of software or supplier of software-as-a-service service;
- viii. appropriate warranties, including that the relevant software/system will operate materially in compliance with its applicable specifications and that any services will be provided with due skill, care, and diligence;

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICE NOW INSTANCES AGREEMENT

[•]

- ix. an intellectual property indemnity by the third party licensor of software or supplier of software-as-a-service service, covering any third party allegations or claims of intellectual property infringement arising from the authorised use of the relevant software or system by or on behalf of the Authority;
- x. reasonable audit rights for the Authority; and
- xi. reasonable exit management provisions, including in relation to any data migration that might be required.

IN WITNESS WHEREOF the parties hereto have executed this Agreement the day and year first written above.

SIGNED by [INSERT NAME OF _____
INDIVIDUAL] _____

a duly authorised representative of/for _____
and on behalf of the Authority

SIGNED by [INSERT NAME OF _____
INDIVIDUAL] _____

a duly authorised representative of/for _____
and on behalf of the Supplier

SCHEDULE 1 – Services Specification Document

1. Scope

The Supplier must be an experienced ServiceNow Elite Partner who can provide technical support and expertise to maintain and continue development of our full cloud based SAAS standalone dedicated instance of ServiceNow (including all hosting and storage) for the Authority.

The Authority has experienced a significant level of growth and activity with 3rd party systems engagements and integrations over the past number of years. The current ServiceNow setup includes an IT Service Management (ITSM) solution through ServiceNow, and with the growth in the organisation, an improved system, tailoring to improve usage and functionality for the relevant teams, is required.

1.1 Initial Scope

As the Authority's system responsibilities grow, it is the Authority's desire that the current ServiceNow instance be maintained and extended to the rest of the organisation, leveraging the current implementation and licencing model. This will facilitate centralised management, escalation, and reporting across the organisation. It will also help standardise processes in the organisation with minimal deviations e.g. different resolver groups, approvers, suppliers or departments in the Authority. The Supplier shall deliver the Authority's requirements using ServiceNow out-of-the-box (OOB) functionality as the primary approach, where OOB is considered configuration and not customisation, and will be done in accordance with ServiceNow's official documentation and guidance.

The Initial Scope is to develop and maintain the current implementations, supporting the current usage of system modules and integrations, including but not limited to the multiple portals currently in use. The vendor must support the current environment, which includes, but is not limited to the below:

- PROD, UAT, and Development environments
- Integrations including:
 - CI Synch (integration tool from different data sources into ServiceNow CMDB)
 - Logic monitor integration with incident tickets (integration with ICT monitoring tool for out of hours incident tickets from Logic monitor. Uses the ServiceNow store application.)
 - Jira integration with NGAVL = Integration with incident and request tickets between a 3rd party using Jira and integration hub.
 - Inbound email rules from different systems.
 - Integration hub workflows using Workflow Data Fabric.
- Data segregation framework using Business rules and ACLs.
 - Approval workflows.

- Catalogue workflows.
- Record producers.
- Other customisations

The supplier must maintain and support the Authority's current instances aligned with the NTA Polices and Governance requirements.

The Initial Scope of Services includes but is not limited to the following areas:

- Delivery of the service as outlined in the sections below;
- The Supplier shall operate the ServiceNow system with at least 99.9% planned availability
- Delivery of licenses for all Authority ServiceNow user types.
Current licences are ServiceNow standard level for the ITSM Module. For clarity, the NTA use these for
 - Incident Management – including Major Incident
 - Request Management
 - Change Management
 - Problem Management
 - Knowledge Management (Knowledgebase)
 - Service Portals including basic Employee Centre

The NTA currently have 132 ITIL fulfiller, and 134 Approver Users and use WDF and Automation Hub. A novation of existing licences from the current supplier may be required for the current year until May 2027. The NTA would prefer to stay on their existing licencing model for the next 3 years (from May 2027). It is appreciated that this may need a slightly early renewal of licence contract to enable this.

- Development, management and support of current instances of ServiceNow. Currently this includes 1 development (DEV) instance, 1 User Acceptance Testing (UAT) instance, 1 production (PROD) instance with the option to spin up temporary instances when this is required by the Authority. All these instances and any future instances must be fully supported.;
- System analysis, design, build, test and configuration of ServiceNow using a recognised implementation methodology to meet Authority's requirements;
- Provision and operation of a User helpdesk / Service Desk to support Authority's ServiceNow instances available during normal office hours (Monday-Friday 08:00-18:00 Irish time);
- Provision and operation of an out of hours support channel to manage P1 incidents in order to achieve the 99.9% availability of the application.
- Maintenance of service catalogue for ServiceNow to allow external and Authority staff open and monitor cases;

- Support for creation, configuration, and decommissioning of service catalogue items quickly, with routine configuration changes included in the service e.g. via request tickets, not treated as charged projects.
- Ensure the security and integrity of Authority's ServiceNow instances including change review, best practice implementations and governance processes.
- Support and upgrade to ServiceNow's annual global releases, including testing/regression testing for core functionalities.
- Regular IT strategic advice on the development and operation of the ServiceNow system including new features or module availability.
- Project management of ServiceNow enhancement projects as and when required;
- Direct support for new integrations with Next Generation Ticketing (NGT), Next Generation AVL (NGAVL) environments, and third-party engagement, with ongoing integration support and roadmap input.
- Ownership for regression testing of core functionality, and centralised documentation of use cases.
- System quality assurance; Provide a robust service to ensure sufficient testing and QA of the platform and any functionality implemented in the platform to meet the Authority's requirements.
- System documentation, including but not limited to how the system is used, as a reference for builds/changes, Configuration change documents, User stories documents based on NTA requirements, Design documents to NTA requirements and standards, Knowledge articles stored in ServiceNow outlining the support of the system, SOPs processes etc.
- Identification and action on opportunities for development of automated workflows and consolidating similar workflows/portals (e.g. bespoke CCC portal, transport/ICT portals, parliamentary questions portal) and have the ability to implement quickly if internal access/resources are available.
- Knowledge transfer including but not limited to, Transition of contracts, Project work to Run support teamwork, onboarding and off boarding of resources, any other scenarios where Knowledge regarding the NTA instances of ServiceNow needs to be shared or transferred;
- End-user training on any current or new system functionality, especially where a training requirement has been identified (tutorials, walk-throughs, suggestions on improving workflows and utilising new features etc.); and
- Delivery of improved reporting from ServiceNow to utilise new features like Platform analytics and other ServiceNow features
- Supply of 3rd party applications / utility software to support existing configuration e.g. CI Synchronizer from Synchfish. This tool is in an integration tool between NTA data sources and ServiceNow CMDB.
- Supply of Workflow Data Fabric from ServiceNow.

Workflow Data Fabric Licensing Alignment and Adaptability

- The Supplier shall provide the Authority (NTA) with a ServiceNow licensing model that fully meets the Authority's current and foreseeable functional, operational, and scalability requirements.
- The Supplier shall demonstrate that the proposed licensing model is sustainable and compatible with the Authority's use of the ServiceNow platform across existing and planned modules.

Change in ServiceNow Licensing Model

- In the event that ServiceNow amends, replaces, or materially changes its licensing model during the term of the contract, the Supplier shall adapt the licensing model provided to the Authority accordingly.
- Any such adaptation shall not result in:
 - an increase in cost to the Authority, or
 - a degradation or reduction in service capability, functionality, or licensed entitlements required to meet the Authority's business needs.
- The Supplier shall remain fully accountable for ensuring continued licensing compliance and uninterrupted service delivery in line with the Authority's requirements for the duration of the contract.

1.2 Future Scope

The Initial Scope set out above in Section 1.1 is limited to the existing business units within the Authority. During the term of the Contract, the Authority may at its sole discretion, decide to materially expand the scope of Services performed by the successful Tenderer, whereby the service elements as described below form the "Future Scope" of the Contract.

The decision to draw down any and/or all of these Future Scope service elements shall be at the sole discretion of the Authority during the term of the Contract and subject to the business needs of the Authority, the availability of funding and approval of all applicable internal governance processes. In the circumstance that the Authority decides to draw down any and/or all of the Future Scope service elements, the Authority shall notify the successful Tenderer in writing.

The expansion of the scope of Services may include but is not limited to the following:

- Expansion of the dedicated ServiceNow instance by enabling additional modules within ServiceNow such as but not limited to the following:
 - CSM
 - Finance and HR Modules
 - Test Management;
 - App Portfolio;

-
- Virtual Agent;
 - Automation capability
 - AI functionality (under the strict overview of the NTA Governance processes); and
 - Asset management
 - Integration of the dedicated ServiceNow instance with existing external supplier instances that support key business areas such as but not limited to the following;
 - TaxSaver system;
 - Leap card operations;
 - Mobile Ticketing system;
 - CABs Ticketing system;
 - Dedicated MSPs
 - CCC Ticketing system
 - Expansion of the dedicated ServiceNow instance to support the future systems that will be hosted or managed by the Authority and will serve the Transport Suppliers such as but not limited to the following;
 - Next Generation Ticketing;
 - Next Generation Automatic Vehicle Location Systems;
 - New Financial Management System; and
 - Consolidated Call Centre Programme;
 - Taxi Regulations system under the umbrella of CABS
 - Integration of the dedicated ServiceNow instance with the ServiceNow instance used by the Authority's strategic partners to form an integrated ITSM offering, in support of Transport Supplier use of the future systems outlined above;
 - Integration of the NTA ServiceNow instance with other (non-ServiceNow) systems used by Suppliers;
 - Integration with the BI stack (e.g. PowerBI, Tableau, etc.); and
 - Provision of in-house (on NTA premises) of an L3 engineer resource. This resource will maintain, document, and operate the NTA ServiceNow platform, at minimum have experience in the following in ServiceNow: Administration, Development, Testing (Automated Testing Framework), in order to reduce project costs and speed up delivery.
- The primary objective of this role is to ensure that critical internal knowledge of the NTA ServiceNow instance is retained within the organisation and not lost across project cycles

Any and/or all Future Scope service elements as contained within this Section 1.2, shall not be binding on the Authority and the Authority will engage the Supplier at its sole discretion. Should the Authority wish to draw down any and/or all of the Future Scope service elements, these will be subject to the change control procedure as set out in Schedule 5 – Change Control Procedure.

2. Services Specifications

The Supplier shall be required to provide the following categories of services:

- Service Category 1: ServiceNow Maintenance and Support: General Support and Maintenance.
- Service Category 2: ServiceNow Maintenance and Support: Development and Customisations;
- Service Category 3: Future Scope System Design, Development and Approach
- Service Category 4: ServiceNow Environment Migration.

2.1 Service Category 1: ServiceNow Maintenance and Support: General Support and Maintenance

Under this service category, Services under the following headings shall be provided by the Supplier, as further detailed below in this Section, which shall adhere to the Service Level Agreement as set out the Schedule 4 of this Agreement.

- Support & Maintenance and;
- IT Security & Compliance.

2.1.1 Support & Maintenance

- The Supplier must provide a helpdesk capability, with English speaking staff, from Monday-Friday 08:00-18:00 GMT time
- The helpdesk must be accessible via a dedicated email and static contact phone number.
- The helpdesk must provide adequate technical support for staff to operate ServiceNow support on general system use, administration, access and reporting.
- The Supplier must provide a dedicated Account Manager and Technical Manager as escalation points.
- The Supplier must provide an out of hours escalation path in the cases of a priority 1 incident and be prepared to work on the incident out of hours if required e.g. in the case of a malware or data breach incident.
- The Supplier must provide backup and disaster recovery functionality to meet the Authority's requirements and to support the current instance configuration. The supplier will give advice on how to improve the NTA instance in the context of Back up and Disaster recovery.
- The Supplier must be able to configure or confirm the data backup retention for ServiceNow of NTA data and configuration of 90 days e.g. 30 daily, 13 weekly, 3 monthly.
- The Supplier must have a Recovery Time Objective ("RTO") of 30 minutes and a Recovery Point Objective ("RPO") of 15 minutes after the discovery of a disaster.

- In the event of a disaster, the Supplier shall activate processes to recover the environment of the affected services in an alternative European Data Centre Region and will work to restore data from the most recent available backup made prior to the onset of the disaster.
- The Supplier must provide alerts to relevant stakeholders in response to events, trends and incidents detected by system monitoring.
- Users within the Authority shall be able to subscribe to alerts and configure by what means they receive them (e.g. email, text, dashboard).
- The Supplier shall notify the Authority of performance or service degradation in a timely manner which aligns with the SLAs defined in contract.
- The Supplier shall monitor and measure solution performance to ensure response times allow for efficient and effective use and maintenance of the entire solution and report on these.
- The Supplier shall operate within a robust patch management policy, and the ServiceNow environments must be regularly reviewed and patched with the latest hotfixes, service packs, updates and security definitions at all times.
- The Supplier shall provide the Authority with adequate prior notice of such patches and updates following the NTA Change Management processes. The Authority holds the right to reject or postpone such updates and patches based on a policy agreed with the Supplier.
- The Supplier shall manage configurations and promotions & roll backs between environments as per ServiceNow best practices.
- The Supplier shall manage all data in each environment as per ServiceNow best practices and to comply with GDPR and to align with all the Authority's compliance requirements.
- The Supplier shall be able to configure the ServiceNow instances with a data retention period as requested by the NTA with automatic deletion of data older than the retention period with auditing in place to prove this occurs.
- The Supplier shall not allow any enablement or activation of any AI elements within the ServiceNow environments without the express permission of the NTA and after following the NTA AI Governance process.

2.1.2 IT Security & Compliance Requirements

- The Supplier must run a regular automated job to purge data with Personally Identifiable Information ("PII") that has been held on the system for more than the configurable retention period.
- Only approved file types should be imported/exported, and all files shall be scanned for malware/viruses and integrity.
- The Supplier must align with the NISD2 cloud definition framework and follow the essential characteristics (On demand self-service, broad network access, rapid elasticity, resource pooling, measured service) during the term of the Contract.
- The data stored within ServiceNow must reside and transit through the European Economic Area ("EEA"). Data must not be replicated outside the EEA

-
- The Supplier must comply with ISO27001 (or equivalent to be agreed with the Authority) at all times during the term of the Contract.
 - The data at rest within ServiceNow system must be encrypted using industry standard encryption technologies and solutions.
 - The Supplier shall manage encryption keys however, the Authority must have the ability/access to manage, at its discretion.
 - All changes made to ServiceNow system must be fully auditable and provide an easily accessible audit trail - for all user, administrative and system configurations changes.
 - Only personnel authorised by the Authority shall have access to the data within the ServiceNow system.
 - The Supplier and any other parties involved in the systems ongoing availability must not have access to data within the system without express consent from the Authority.
 - The Supplier must ensure that the underlying infrastructure and platform of ServiceNow adheres to the relevant CIS standards (or equivalent). It is the full responsibility of the Supplier to ensure the infrastructure is patched and hardened to minimise IT security risk.
 - The Supplier must apply a robust antivirus/malware policy and have regularly updated adequate anti-virus/malware controls that encompass all solution components and security monitoring capability.
 - The Supplier shall support and employ User and Privileged User Access Management controls to support 'least privilege' security principles and enable regular User Access Management ("UAM") and /Privileged User Access Management ("PUAM") audit activities.
 - The Supplier shall provide security reports upon request from the Authority. The security reports that shall provide details and identify suspicious or potentially suspicious activity.
 - It must be possible to copy data from the production/live environment back to other environments.
 - It must be possible to anonymise such data.
 - The Supplier must be fully available to staff working from home to ensure that Business As Usual ("BAU") can continue to operate during a time of emergency (e.g. red weather events, pandemics etc.).
 - The Supplier must apply remote working security controls.
 - The Supplier must encrypt data in transit and while being processed utilizing the most current and secure industry standard encryption technologies and solutions (e.g. SSL/TLS, HTTPS) to provide the highest level of data security to meet all current data protection and General Data Protection Regulations ("GDPR") compliance.
 - The Supplier must ensure security of data including but not limited to the following:
 - Provision of a secure system for data and users;

-
- adequate measures to prevent malicious input such as but not limited to SQL injection; and
 - cross-site scripting, IFRAME-based attacks or spam.
 - The Supplier must ensure that measures are in places that will protect the system against the Top 10 Application Vulnerabilities identified by the OWASP online community.
 - The Supplier must employ and demonstrate Role Based Access Control (“RBAC”) controls and auditable granular user and privileged user role controls to both prevent Authority staff and third-party users from viewing or accessing data not associated to their role, in addition to following the 'least privilege', 'need to know' principles.
 - The Supplier must operate a session management policy and provide a configurable session management method that automatically logs users out after a pre-determined period (in minutes) of inactivity.
 - The Supplier shall ensure that the risks associated with access to ServiceNow are mitigated through a range of controls such as but not limited to example Identity Management (“IDM”) functionality that supports role-based access and conditional access such as IP Whitelisting, MFA, device type and location (“Geo-blocking”) for internal and external users.
 - In the circumstance that ServiceNow has system accounts that are not integrated with an identity management system, the Supplier shall ensure that the following measures are in place:
 - Password management and complexity must be in line with industry best practice including a self-service password reset facility;
 - ServiceNow shall manage the number of days to password expiration for the user base;
 - ServiceNow shall provide the ability to set criteria for password creation;
 - ServiceNow shall have the ability of controlling the management of usernames, passwords and other access control elements and should form part of the overall solution; and
 - ServiceNow shall lock an account after multiple, failed login attempts or following a suspicious login attempt.
 - In the circumstance that ServiceNow is integrated with MS Azure AD SSO, the above password management and account lock requirements are not applicable.
 - The Supplier must provide the functionality for each user within the system to assume one or many roles in line with a secure RBAC policy.
 - The Supplier must utilise strict RBAC controls to restrict certain functions to authorised personnel only, e.g. certain user groups have read-only access and different user groups may have the ability to edit/delete data.
 - The Supplier shall integrate/align these restrictions with the standard Authority user lifecycle management.
 - Beyond standard user operations, the Supplier must provide a mechanism allowing full traceability of all operations relating to but not limited to the following:

- User Management;
- System Configuration; and
- Report Generation.

2.2 Service Category 2: ServiceNow Maintenance and Support: Development and Customisations

The Supplier shall support, maintain, develop and operate the Authority's existing ServiceNow instance, including all current configurations, customisations, workflows, integrations, and security controls, in accordance with the Authority's governance, policies, and standards. No existing configuration or customisation shall be materially changed without prior Authority approval through the agreed change control process.

All items in this section shall fall under maintenance and support and will not incur additional project cost to the authority.

This service shall include, but is not limited to, the following ServiceNow capabilities:

- Call Management
- Incident Management
- Request Management
- Change Management
- Knowledge Base
- CMDB, Configuration Items and Asset Management
- Self-Service Portal(s)
- Reporting and Business Intelligence (BI)
- Microsoft Office 365 Integration
- Identity and Access Management
- Data Encryption and data protection.
- Implementation and Configuration Services

The Supplier shall proactively review and optimise the ServiceNow instance to ensure the Authority achieves best value from its existing configuration, customisations, and licensed functionality. This includes identifying improvement opportunities, promoting relevant ServiceNow features, and presenting upgrade-safe recommendations aligned to the Authority's business requirements. Any proposed changes shall be subject to Authority approval prior to implementation.

Core Service Management Capabilities

The Supplier shall support and maintain the Authority's existing Call, Incident, Request, Change, and Knowledge Management capabilities within the ServiceNow platform,

including all current configurations, workflows, integrations, and reporting. The Supplier shall ensure continuity of service and shall not materially alter or degrade existing functionality without prior Authority approval through the agreed change control process. In addition, the Supplier shall proactively review and assess these capabilities to identify opportunities to improve efficiency, usability, automation, and data quality, using existing or available ServiceNow features. Any proposed enhancements must be upgrade-safe, aligned to the Authority's business requirements, and approved by the Authority prior to implementation.

The supplier will develop new configurations and customisations as part of BAU activities and align with the existing processes and procedures in this context.

For the avoidance of doubt, BAU support includes activities required to maintain, support, enhance and continuously improve the Authority's existing ServiceNow platform and related operational processes, reflecting the nature and scope of services historically delivered as part of BAU support during the incumbent service arrangement. Such activities shall not be deemed out of scope, project work, or Future Scope solely because they require development, configuration, customisation, scripting, testing, or release effort.

Any activity that the Supplier considers to be outside BAU must be clearly identified by the Supplier in advance, with the rationale documented, and must be agreed in writing by the Authority before being treated as a separately chargeable project or Future Scope item.

2.2.1 CMDB / Configuration Items /Asset Management

- The Authority requires ServiceNow to communicate with and/or utilise external software and services (including but not limited to, JIRA, VMware, Azure, AWS, MS Dynamics and other instances of ServiceNow, etc.) for several purposes including but not limited to system integration, network software and hardware discovery, user management, etc. using manual and automated (.csv, system discovery, etc.) update processes.
- The supplier will work with current 3rd parties that engage with the Authority's ServiceNow CMDB based on the requirements of the authority.
- The Supplier shall support, maintain, and operate the Authority's existing Configuration Management Database (CMDB), including all current data models, configuration items (CIs), relationships, processes, and integrations. This includes ongoing support for integrations with internal systems, external platforms, and third-party suppliers, and active engagement with third parties where required.

- The Supplier shall facilitate and support updates to the CMDB, including the creation, modification, and lifecycle management of new and existing configuration items and assets, and the development of new or updated CMDB data models as required to meet the Authority's operational and business requirements.
- The Supplier shall ensure the integrity, accuracy, and completeness of CMDB data and its alignment with Incident, Request, Change, and Asset Management processes to support effective impact analysis and operational decision-making.
- In addition, the Supplier shall proactively invest in and improve the CMDB by identifying opportunities to enhance data quality, coverage, automation, and integration to strengthen the Authority's ITSM processes and procedures. Any proposed improvements must be upgrade-safe, aligned with Authority governance standards, and approved prior to implementation.

2.2.2 Self Service Portals

- The supplier shall support and maintain all the Authority's existing ServiceNow Service Portals, including current structure, catalogue items, forms, user criteria, and branding, without degrading existing functionality.
- The Supplier shall ensure that all the exiting Service Portals continue to meet the Authority's user experience, accessibility, and security requirements, including access for internal users and approved external parties.
- The Supplier shall proactively review and assess the Service Portals to identify opportunities to improve usability, automation, adoption, and service fulfilment using existing ServiceNow features.
- The Supplier shall proactively review and assess the Service Portals to identify changes required for regulatory purposes e.g. accessibility.
- Any proposed enhancements must be upgrade-safe, aligned with Authority governance standards, and approved prior to implementation.
- The supplier is expected to configure, customise and update the Service Portals as part of business as usual (BAU) activities to meet any NTA requirements. These updates and configurations and customisations must align with the existing processes and procedures in this context.

2.2.3 Reporting & Business Intelligence

- The Supplier shall support and maintain all existing reports, dashboards, and scheduled report outputs within the ServiceNow platform and shall ensure their continued operation and accuracy throughout the term of the Contract.
- Where ServiceNow functionality, features, or underlying report mechanisms are identified for deprecation or change (including through platform upgrades), the Supplier shall proactively assess the impact on existing reports and shall plan for

and deliver the migration or replacement of affected reports to an equivalent or improved solution.

- Any report migration or remediation must preserve existing business intent, data integrity, access controls, and reporting outcomes, and must be implemented in a controlled manner with prior Authority approval.
- Report generation and distribution must not compromise the privacy of the data and operate within the Role Based Access Control (“RBAC”) framework and within the existing Data segregation configuration in the NTA instance of ServiceNow.

2.2.4 Office 365 Integration

- The Supplier shall support and maintain the Authority’s existing integration between ServiceNow and Microsoft Office 365, including the ability for ServiceNow to connect to and retrieve emails from multiple mailboxes within the Authority’s Office 365 tenant.
- The integration shall support multiple email domains within the same tenant, including but not limited to @nationaltransport.ie and @transportforireland.ie, and shall ensure that incoming emails from different addresses are correctly routed to the appropriate queues or assignment groups.
- Outbound email communications from ServiceNow shall be sent using approved Authority email domains. The Supplier shall ensure continuity of existing email-based processes and shall not degrade current functionality without prior Authority approval.

2.2.5 Identity Access Management (IAM)

- The Supplier shall ensure that ServiceNow remains fully integrated with the Authority’s existing Single Sign On (SSO) solution, currently provided by Microsoft Azure Active Directory (Azure AD), and that SSO is consistently applied across all ServiceNow modules and capabilities.
- Any user within the Authority’s Azure AD tenant shall be automatically provisioned as a requester by default, enabling access to the ServiceNow self-service portal for the submission of requests and cases.
- The Supplier shall support and maintain the provisioning of external users to the ServiceNow self-service portal, including integration with Azure AD Guest Accounts, in accordance with the Authority’s security, access control, and governance standards.
- The supplier shall be responsible for IAM of their own staff for the purposes of support and this access shall be granted only after following the NTA approval processes.

2.2.6 Release management.

The Supplier shall provide and operate a fully managed Release Management and release to production approval (RTPA) process for the Authority's ServiceNow platform, aligned with ServiceNow best practice, ITIL5 (preferred) or ITIL4, and a formally defined Software Development Lifecycle (SDLC), covering all stages from demand intake through to deployment into Production.

All Business As Usual (BAU) development, configuration, enhancement and fix activity undertaken to meet NTA business requirements must be delivered strictly through this managed framework, with no ungoverned or ad-hoc changes permitted.

The Release and RTPA process must, at a minimum:

- Define and enforce controlled stages for design, build, testing (including system, integration and UAT support), release approval and production deployment using a recognised implementation methodology.
- Be fully integrated with ServiceNow Change and Release Management, ensuring end-to-end traceability of requirements, builds, tests and deployments.
- Ensure that all changes are appropriately categorised, risk-assessed, approved and auditable in line with NTA governance and policies.
- Support segregation of environments (e.g. Development, Test/UAT, Production) and controlled promotion between environments.
- Ensure that production releases are only executed following formal approval based on the Authority's requirements.
- Include clear ownership and accountability for release planning, coordination, execution and post-release validation.
- Provide release documentation and evidence (e.g. release notes, test evidence, approval records) suitable for audit purposes.

The Supplier shall not bypass, weaken or replace the Authority's governance requirements and must operate the Release and RTPA processes as the single authoritative mechanism for delivering all BAU platform changes.

2.3 Service Category 3: Future Scope System Design: Development and Approach

Under this service category, Services under the following headings shall be provided by the Supplier as further detailed below in this Section 2.5:

- System Architecture and Design;
- System Development;
- Testing;
- System Release Management;
- Project Management;
- Business Analysis; and
- Integration.
- [Multiple Identity Integration](#)

2.3.1 System Architecture and Design

- The Supplier shall provide architecture, migration, build, integration, and design services to assist the Authority with project design and roadmap planning using a recognised implementation methodology. These services shall include but are not limited to the following:
 - Architecture design and implementation;
 - Setup and configuration of integration and or E-Bonding integration of various ServiceNow instances and applications;
 - Workflow design optimisation;
 - Development and recommendation of SOPs conducive to an organisation of the Authority's size and standing whilst following ServiceNow good practice guidance;
 - Development and recommendation of good business practices, including but not limited to Custom Data Segregation Frameworks and Logic including ACLs and Business Rules and
 - Development and recommendation of test plans and procedures including automated testing where possible.

2.3.2 System Development

- The Supplier shall complete system development based on the requirements defined in the specifications including but not limited to the following:
 - All code changes and new development to be completed in secure development, QA and UAT environments; and
 - Complete bug fixing at QA and UAT stages.
- Complete quality assurance testing has been undertaken to ensure that all Authority requirements are satisfied and that the system is fully operational and free from known defects.
- Manage a solid QA process and provide details of same to the Authority.
- Use a set of functional test scripts for QA and provide same to the Authority.
- Ensure thorough testing to ensure all functionality issues are raised and resolved ahead of UAT.

2.3.3 Testing

- Each element of ServiceNow must be rigorously tested including functional, integration, UAT, performance, penetration, and regression testing, before it is implemented.
- The Supplier must provide a test strategy, test cases, scripts and test evidence to the Authority where required.
- Entry and exit criteria for each test phase are to be agreed with the NTA.
- The Supplier shall support the Authority in UAT by way of the following:
 - Delivering all system changes for UAT on schedule and in the manner preferred by the Authority, i.e. full release; sprint testing;

- Providing test scripts;
 - Providing data for testing;
 - Bug fixing; and
 - Liaising with the Authority to resolve issues raised.
- The Supplier shall work closely with the Authority to ensure the delivery of a high-quality system updated within agreed timeframes.

2.3.4 System Release Management

- The Supplier shall provide a detailed deployment plan, including plans for potential rollbacks at least 2 weeks before commencement of the project.
- The Supplier shall manage all changes to the systems within the Authority's Change Management policy and processes.
- The Supplier shall schedule system deployment in liaison with the Authority, outlining system downtime requirements.
- The Supplier shall complete deployment. Out of hours deployments shall be required (late evening/early morning) to ensure there is no impact on service delivery and as little impact as possible on front-facing modules/apps.
- The Supplier shall liaise with operational teams in the completion of go-live smoke tests and provide resources to close out issues where necessary.
- The Supplier shall complete system user guides.
- The Supplier shall complete user training on request.
- The Supplier shall work with the NTA Security teams to remediate identified security issues e.g. results from penetration testing or security reviews.

2.3.5 Project Management

- For every project, the Supplier shall assign project management resources to undertake the following activities as a minimum:
 - Oversee Supplier resources in managing the completion of each stage of the project;
 - Ensure timely commitment to projects and ensure resources can be assigned promptly;
 - Provide safeguards to ensure that the relevant expertise/experience is spread amongst resources, to avoid bottlenecks and single points of failure;
 - Provide Rough Orders of Magnitude estimates promptly on request;
 - Provide Statements of Work (SOWs) promptly on request and on a fixed cost basis;
 - Agree timeframes for completion and ensure these are not exceeded;
 - Agree project costs and ensure these are not exceeded;
 - Provide detailed status updates and reports to the Authority at agreed intervals;
 - Liaise closely with Authority operational and project teams;

- Provide deployment plan and liaise with the Authority to agree a schedule for deployment; and
- Ensure maintenance and delivery of updated technical documentation in liaison with the helpdesk.

2.3.6 Business Analysis

- For every development project, the Supplier shall assign a business analysis resources to undertake the following activities as a minimum:
 - Engage with the Authority's operational teams in designing functionality for new modules and applications;
 - Review requirements in a transparent manner, suggesting efficient and cost-effective solutions;
 - Complete impact analysis, ensuring the potential impact of changes proposed and all associated risks and are raised;
 - Provide prompt and detailed cost estimates (on a fixed cost basis) for any projects proposed;
 - Based on an agreed set of requirements, write a system requirements specification and provide to the Authority for review and sign off; and
 - Adhere to agreed project schedules and timeframes.

2.3.7 Integration

- ServiceNow must have the ability to integrate with the Authority's and third-party systems, as required. ServiceNow should allow for scalable integration with other solutions should it be required in the future to streamline and optimize processes.
- The Authority's integration strategy is to utilise APIs where possible. ServiceNow must be able to utilise the following methods of integration, this list is not exhaustive:
 - Rest API;
 - SOAP/XML; and
 - SFTP.
- ServiceNow must have a robust way of handling errors when calling external APIs. When required, administrators or business owners must know and be alerted when a process fails.
- When required, it must be possible to schedule integrations and/or run them on demand.
- Throttling of APIs must be supported (i.e. there must be control over how an API is used). Throttling allows for permissions to be set as to whether certain API calls are valid or not. Throttles indicate a temporary state and are used to control the data accessed through an API.
- All future integrations shall be managed through the change control procedure set out in Schedule 5 of this Agreement.

2.4 Service Category 4: ServiceNow System Migration / Service Transition

In the event of a transition or migration of the ServiceNow instance from the incumbent supplier to a successor supplier, the Supplier shall ensure that the migration is executed in a controlled manner with no loss of data, functionality, configuration, or security.

- The migration must maintain full business continuity for the Authority, with no material disruption to services, users, or operational processes.
- The migration must be completed within the NTA project guidelines and change approval processes.
- The Supplier shall ensure that the implementation and transition plan and process include an appropriate level of resources, including technical resources, and shall be completed within a reasonable time frame as agreed by the Authority after contract signing with reference to the Supplier's response.

2.4.1 Transition Plan

General

- a) The Operator shall develop and implement the Transition Plan to successfully meet the Transition Services requirements and achieve the milestones set out in this Schedule (the "**Milestones**").
- b) The Operator shall further ensure that the Transition Plan is consistent with any exit management plan agreed between the NTA and the Outgoing Service Providers and notified by the NTA to the Operator.
- c) The Operator shall provide the Transition Services in a timely manner and in accordance with the milestones and timeframes set out in this Schedule. Without prejudice to any other rights and remedies which may be available to the NTA in respect of failure to meet such timeframes, any delays to the Programme shall be actively managed by the Operator in order to mitigate the effects of any such delay.

2.4.2 Programme

- a) The Transition Plan shall contain a detailed programme (the "Programme") describing all tasks required to successfully meet the requirements of the Transition Services phase and to achieve the Milestones. The Programme shall clearly define the date and duration of each task, the interdependencies between tasks, the resources required and a logical work breakdown structure. The Programme shall further clearly define the scheduled dates for submission of documents or Certificates to the NTA in accordance with the Certification Procedure.

2.4.3 Transition Services Risk

- (a) The Operator shall describe the approach to managing risk during the Transition Services phase in the Transition Plan.

- (b) The Operator risks associated with Transition Services shall be tracked and managed in accordance with section 5 of the Governance Schedule.

2.4.4 Reporting and Engagement with the NTA and Outgoing Service Providers

Reporting

- a) The Operator shall provide at minimum fortnightly Transition Services reports to the NTA Representative from the Commencement Date until the Operational Services Start Date.
- b) The Transition Services reports shall include the following:
- executive summary;
 - update on the Programme;
 - updated risk register;
 - summary of status and progress of the Transition Services activities; and
 - identification of any decisions or actions required of the NTA.
- c) The Operator shall develop contingency plans where required as an appropriate risk mitigation measure or where instructed to do so by the NTA.

Engagement with the Outgoing Service Providers

- (a) The Operator shall co-operate with the Outgoing Service Providers in relation to the transition activities. The NTA shall use reasonable endeavours to assist the Operator in its engagement with the Outgoing Service Providers.

The Operator shall identify all data, assets and assistance it requires from the NTA and the Outgoing Service Providers as soon as is reasonably practical and shall identify the dates by which all such data, assets and assistance are required.

The Operator shall make every reasonable effort to obtain all such data and assistance it requires in a timely manner.

In the event of any delays or in the event that the identified data or assistance required by the Operator or provided by the Outgoing Service Providers do not meet the required standard to facilitate the Transition Services in accordance with the requirements of this Schedule, the Operator shall notify the NTA. The Operator shall take all such measures as are reasonably necessary to mitigate the effects of the events identified, including by developing and agreeing suitable contingency plans with the NTA and implementing such plans in order to achieve the Transition Services requirements.

2.4.5 Milestones

-
- a) The Operator shall comply with the requirements set out in respect of each Milestone by the relevant date.
 - b) Strictly without prejudice to any other rights or remedies which may be available to the NTA in the event of failure by the Operator to achieve a particular Milestone Completion Date, as soon as the Operator becomes aware of a risk in achieving a particular Milestone Completion Date, the Operator shall notify the NTA, provide a mitigation plan to the NTA for Approval and implement such plan once Approved.
 - c) The completion of Milestones shall be certified in accordance with the Certification Procedure set out in Appendix D of this Schedule.
 - While certain activities and documents are to be completed and certified by the relevant Milestone Completion Dates, nothing shall preclude the Operator from certifying such activities and documents in advance of the relevant Milestone Completion Date.
 - d) Milestone One (Delivery of Plans & Design Completion)
 - In order for Milestone One to be successfully achieved, the Operator shall have completed the following activities to the satisfaction of the NTA:
 - provision of updated Delivery Plans in accordance with the Governance Schedule;
 - provision of detailed discovery phase plan
 - Key Personnel relevant to the Transition Services are in place.
 - provision of updated Delivery Plans in accordance with the Governance Schedule;
 - confirmation that all licences have been ordered and a firm date for delivery and commissioning is available;
 - confirmation that all sub-suppliers have been identified and plans are in place to establish contracts with new Operator sub-suppliers and novate existing NTA Contracts (including any relevant Software License Contracts) to the Operator (where required);
 - confirmation that all ServiceNow integrations have been identified and firm dates are in place to implement these integrations;
 - an outline Service Catalogue is established and Operational Run Books (with defined Roles and Responsibilities) and additional supporting documentation for each ICT Operational Service are being drafted with firm dates for delivery and Service and Technical Readiness and Operational Testing is available.
 - All Key Personnel relevant to the Operational Services are in place and firm dates in place to on-board these resources;
 - e) Milestone Two (Service and Technical Readiness)
 - In order for Milestone Two to be successfully achieved, the Operator shall have completed the following activities to the satisfaction of the NTA when all

the Services are operational and service operational procedures have been developed and tested including:

- the Operators ICT Service Desk solution and phones;
- the Operator Support Systems are fully operational and have been validated by the Operator and the NTA as ready to commence operational readiness testing;
- all standard operating procedures have been developed by the Operator such that operational readiness testing can commence;
- subject to any consents or Approvals which may be required from the NTA, the Operator has executed all sub-contracts required for performance of the Services;
- the BC/DR Plan has been developed, reviewed, tested and implemented.
- examples of reports as set out in the Services Schedule

f) Milestone Three (Operational Readiness)

- The Operator shall demonstrate operational readiness (and achieve Milestone Three) by completing the following activities to the satisfaction of the NTA and providing evidence and the required compliance reporting against each Service area:
 - the Operator is capable of providing the full range of Services as set out in the Services Schedule;
 - operational readiness testing (in accordance to Appendix 1 to this Schedule) is complete;
 - updated versions of the System Design and the Operations Plan have been submitted to the NTA;
 - all Acceptance Tests have been completed and any defects (disregarding any minor and inconsequential failures) identified in accordance with this Schedule have been resolved to the satisfaction of the NTA;
 - all staff required for delivery of the Services are available and have completed all necessary training and the Operator has provided evidence of same (if requested by the NTA), including by facilitating visits to the premises of the Operator and its sub-contractors and staff interviews by the NTA;
 - all standard operating procedures have been documented and tested as part of the operational readiness testing;
 - information security has been tested and validated; and

Following successful achievement and certification of Milestone Three by the Operator, the Operator can request that the NTA issue an Operating Permit in accordance with Section 5 of Appendix D to this Schedule. Unless otherwise agreed with the NTA, the Operator may not commence provision of the

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICE NOW INSTANCES AGREEMENT

[•]

Operational Services in a live environment until the date specified in the Operating Permit.

g) Milestone Four (Operational Services Start)

- The date specified in the Operating Permit by the NTA, is the date on which the Service shall commence.

h) Milestone Five (Completion of Transition Services)

- In order for Milestone Six to be successfully achieved, the Operator shall have completed the following activities to the satisfaction of the NTA:
 - At least two (2) end-of-month compliance and operational; reports and reporting services required in relation to the Transition Services have been provided;

SCHEDULE 2 – Payments Schedule

1. General

All rates are provided in Euro (€) excluding VAT. The rates provided in the tables below shall be fixed for the full duration of the Contract term.

2. Services Payments

The figure inserted in the “Total Fixed Cost” column represents the total cost proposed to be charged to the Authority for the implementation of the ServiceNow initial system.

The “Total Fixed Cost” shall be an all-inclusive cost which must include all costs associated with the implementation of the dedicated ServiceNow instances such as but not limited to the following:

- ServiceNow system configuration changes;
- ServiceNow system low level code changes;
- Call management;
- Incident management;
- Change management;
- Knowledge base;
- CMBD;
- Configuration Item/Asset Management;
- Self Service Portal;
- Reporting & Business Intelligence;
- Office365 integration;
- Connectors;
- Identity Access Management;
- Implementation & Transition;
- System Architecture, Design & Approach;
- System Development;
- Testing;
- System Release Management;
- Project Management;
- Business Analysis; and
- Integration.

The “Total Fixed Cost” shall include the cost of all personnel allocated to deliver the Services as set out under Service Category 1: ServiceNow Maintenance and Support: General Support and Maintenance and Service Category 2: ServiceNow Maintenance and Support: Development and Customisations;

Table A: ServiceNow Licencing Costs

The figure inserted in the “Annual Cost” column represents, in the relevant row, the annual cost proposed to be charged to the Authority for a single licence within that particular category of ServiceNow licences.

In the circumstance, that the Authority would like to co-term existing ServiceNow licences, the cost charged by the Supplier shall be pro rata based on the relevant costs provided in the table below.

The NTA reserves the right to tender separately for licences if needed after the initial 2 year contract if ServiceNow change the licencing model.

CATEGORY OF LICENCE	ANNUAL COST PER LICENCE (EX. VAT) €
Fulfiller User License cost	n/a
Approver Users Licence Cost	n/a
Self-service Portal (Requestor)	n/a
ServiceNow Standalone Dedicated Instance Production	
ServiceNow Non-Prod Instance/s	
New Tier Pricing	
Additional assist pack pricing	
Other Licences – Modules HR, Finance, Case management Potential for expansion in these areas	
Optional Add-ins (per year cost): WDF (Workflow Data Fabric) Automation Hub SyncFish	

Table A: ServiceNow Licencing

Table B: Managed Service Delivery (Service Category 1: ServiceNow Maintenance and Support: General Support and Maintenance and Service

Category 2: ServiceNow Maintenance and Support: Development and Customisations)

The figure inserted in the “Annual Cost” column represents the cost proposed to be charged to the Authority for the delivery of Services and Service Maintenance & Support on a yearly basis.

The “Annual Cost” shall be an all-inclusive cost which must include all costs associated with the delivery of Services and the full maintenance and support of the ServiceNow system. The “Annual Cost” shall also include the cost associated with any and/or all ServiceNow system upgrades, ServiceNow version updates, ServiceNow service packs.

DESCRIPTION	MONTHLY COST (EX. VAT) €
Monthly Service Delivery and Maintenance & Support (Fixed Cost)	

Table B: Managed Service Delivery & Maintenance & Support

Table C: Professional Services Daily Rates - (Service Category 3: ServiceNow Future Scope System Design, Development and Approach)

The “Daily Rate” represents the maximum rate per day proposed to be charged for that particular role based on an eight (8) hour working day and shall include the items listed in Section 6. Please note the preferred locations of some resources due to a requirement of attending the NTA offices in a hybrid pattern (currently 2 days a week).

GRADE DESCRIPTION	Location Ireland (for on site)	Location NearShore (Europe)	Location FarShore (not Europe)
Business Analyst			
Project Manager			
ServiceNow AI & Automation Specialist.			
ServiceNow Developer & Release Manager			
ServiceNow Module Specialist			
ServiceNow Reporting Specialist			
ServiceNow Security and Data Segregation Specialist.			
ServiceNow System Administrator / Level 3 Engineer.			

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

ServiceNow Technical Architect (senior)			
ServiceNow Tester/Quality Assurance Lead			
UI / UX Specialist			

Table C: Professional Services Daily Rates

3. Rate Inclusions

For the avoidance of doubt the Daily Rates stated in Table C shall include, without limitation, such items as:

- salary payments;
- provision of all secretarial/administrative/clerical support;
- all equipment required in the performance of the services;
- office overheads;
- insurance;
- general office consumables;
- annual leave payments/sick leave payments;
- all travel and subsistence arrangements for attendance at Authority offices in Dublin;
- postage/telephone/fax/email costs;
- all analysis and reporting;
- all management, quality assurance and documentation services;
- internal photocopy and printing costs;
- general overheads; and
- profit.

Table D: Service Transition Costs

Milestone	Description of Contract Start Transition	Milestone Payment
One	Delivery of Plans & Design Completion	20%
Two	Service and Technical Readiness	20%
Three	Operational Readiness	20%
Four	Operational Services Start	20%
Five	Completion of Transition Services	20%
Milestone	Description of Contract Exit Transition	Milestone Payment
One	Delivery of Plans	30%
Two	Service and Technical Exit Readiness	30%
Three	Completion of Transition Services	30%

Table D: ServiceNow Contract Start and Exit Transition

4. Monthly Performance Review

4.1 Table 1 of Schedule 4 – Service Level Agreement sets out the required service level to be provided by the Supplier with regard to its obligations under this Agreement in a Contract Month.

4.2 The Supplier shall issue invoices to the Authority each month in respect of the Services Payment in accordance with clause 11 of the Agreement.

4.3 Where the Supplier fails to achieve the Target Service Levels for any KPI in any Contract Month, the Authority may, at its sole discretion, award Performance Points as follows:

- a) Category ‘Red’ shall incur twenty (20) Performance Points;
- b) Category ‘Amber’ shall incur ten (10) Performance Points; and
- c) Category ‘Yellow’ shall incur five (5) Performance Points.

4.4 Where the Service Provider fails to achieve the Target Service Levels for any KPIs for more than two (2) consecutive Contract Month, the Authority may, at its sole discretion, award additional Performance Points as follows:

- a) Category ‘Red’ shall incur an additional ten (10) Performance Points (Total Performance Points for this ‘Red’ category increases to thirty (30) Performance Points for that KPI);
- b) Category ‘Amber’ shall incur an additional five (5) Performance Points (Total Performance Points for this ‘Amber’ category increases to fifteen (15) Performance Points for that KPI); and,
- c) Category ‘Yellow’ shall incur an additional five (5) Performance Points (Total Performance Points for this ‘Yellow’ category increases to ten (10) Performance Points for that KPI);

4.5 Where the Supplier fails to achieve one or more Target Service Levels for the KPIs set out in Table 1 of the Schedule 4 – Service Level Agreement, the Authority may, at its sole discretion, deduct a percentage of the Monthly Service Delivery and Maintenance & Support Payment in that Contract Month until the Target Service Levels for those categories of KPIs are achieved. The percentage of the Managed Services - Services Payment deducted will be as follows:

Performance Points Accumulated	Accumulated Percentage of the Service Delivery and Maintenance &
--------------------------------	--

**NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICE NOW INSTANCES AGREEMENT**

[•]

	Support Payment deducted in that Contract Month
0-35 Points	0% of the Service Delivery and Maintenance & Support Payment
36-70 Points	5% of the Service Delivery and Maintenance & Support Payment
71-140 Points	10% of the Service Delivery and Maintenance & Support Payment
141-210 Points	15% of the Service Delivery and Maintenance & Support Payment
>210 Points	20% of the Service Delivery and Maintenance & Support Payment

4.6 If the Authority deducts any portions of the Service Delivery and Maintenance & Support Payment as set out above, the Supplier will be required to take remedial action that:

- (a) addresses the failure by the Supplier to achieve the relevant Target Service Levels in the short term; and
- (b) puts in place the necessary solution(s) and procedure(s) that, in the opinion of the Authority will mitigate against repeated failure of such Target Service Levels in subsequent Contract Months.

4.7 The Supplier will issue a report to the Authority detailing the measures taken in relation to paragraphs 7.6 (a) and (b) above for Approval (a "Remediation Report"). If the Authority (at its sole discretion):

- (a) is satisfied with the remedial action taken; and
 - (b) approves the Remediation Report,
- the Authority will agree the performance issue(s) has been addressed for an agreed amount of time.

SCHEDULE 3 – Key Personnel

1. Key Personnel and Representatives

The delivery of the Services under this Agreement will be managed at a day-to-day level through the Key Personnel set out in parts 1, 2, and 3 of this Schedule.

Contractual matters arising during the Term shall be dealt with by the NTA's Representative and the Service Provider's Representative.

Details of the NTA's Representative and the Service Provider's Representative are set out in part 4, 5, 6, and 7 of this Schedule.

Without prejudice to any other provisions of this Agreement regarding Key Personnel:

- a) the Supplier shall ensure that appropriate resources are made available on a regular basis such that the aims, objectives and specific provisions of this Agreement can be fully realised, including in relation to the Key Personnel;
- b) each Key Personnel and Representative will have relevant seniority and expertise; and
- c) the parties shall ensure that the Key Personnel and Representatives shall, as soon as reasonably practicable, resolve the issues and achieve the objectives placed before them. Each party shall endeavour to ensure that its Key Personnel and Representative is duly authorised to make relevant decisions or have access to duly authorised persons for such purposes.
- d) the Supplier shall ensure that appropriate segregation of duties is achieved when staffing Key Personnel as means to review and catch errors and as a fraud/theft prevention measure.

1.1 Key Personnel - Operational Services

The key personnel may comprise of the following roles as set out in Table 1 below, alongside the applicable role description with regard to duties, responsibilities and level of experience:

- Account Manager;
- Business Analyst;
- ServiceNow AI & Automation Specialist.
- ServiceNow Developer & Release Manager
- ServiceNow Module Specialist
- ServiceNow Reporting Specialist
- ServiceNow Security and Data Segregation Specialist.
- ServiceNow System Administrator / Level 3 Engineer.
- ServiceNow Technical Architect (senior)
- ServiceNow Tester/Quality Assurance Lead

- UI / UX Specialist

1.2 Key Personnel - Transition Period

The key personnel may comprise of the following roles as set out in Table 1 below, alongside the applicable role description with regard to duties, responsibilities and level of experience for the transition period:

- Business Analyst
- Project Manager (Transition)
- ServiceNow Developer & Release Manager
- ServiceNow Reporting Specialist
- ServiceNow Security and Data Segregation Specialist.
- ServiceNow System Administrator / Level 3 Engineer.
- ServiceNow Technical Architect (senior)
- ServiceNow Tester/Quality Assurance Lead

1.3 Key Personnel – Future Development / Professional Services

The key personnel may comprise of the following roles as set out in Table 1 below, alongside the applicable role description with regard to duties, responsibilities and level of experience for the transition period:

- Business Analyst
- Project Manager
- ServiceNow AI & Automation Specialist.
- ServiceNow Developer & Release Manager
- ServiceNow Module Specialist
- ServiceNow Reporting Specialist
- ServiceNow Security and Data Segregation Specialist.
- ServiceNow System Administrator / Level 3 Engineer.
- ServiceNow Technical Architect (senior)
- ServiceNow Tester/Quality Assurance Lead
- UI / UX Specialist

1.4 Key Personnel – Role Descriptions.

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Role	Role Description
Business Analyst	The service requirements, level of experience, skillset and capabilities associated with this role include but are not limited to the following: · Possesses the ability to lead, review and analysis the Authority's current and future ServiceNow business requirements, identify changes that lead to business improvements; · Holds a record of identifying technical solutions, defining strategies while validating and justifying business direction; · Possesses the ability to conduct feasibility studies, producing high-level and detailed business models; · A critical thinker with an well-developed set of problem solving skills and a strong business acumen to foresee and mitigate issues around the preparation of specifications, development and implementation of solutions, with due consideration to impact of change on the organisation and stakeholders; · Holds a strong communication and relationship management skillset, with the ability to deliver critical findings to management regarding any proposed organisational change; and · Possesses minimum of three (3) years relevant ServiceNow experience.
Project Manager	The service requirements, level of experience, skillset & capabilities associated with this role include but are not limited to the following: · Leads and manages the risk, quality & progress of ICT projects in accordance with organisational procedures; · Ensures projects are completed on time, on budget, to the Authority's standards, & within agreed scope; · Plans & manages the implementation of organisation-wide processes & procedures, tools & techniques for the identification, assessment, and management of risk inherent in the operation of business processes and of potential risks arising from planned ICT- enabled change; · Lead the documentation and maintenance of the NTA ServiceNow Platform · Possesses an appropriate level of communication (written, verbal and technical) and organisational skills which are required, through English, to fulfil this role; · Possesses a recognised Project Management qualification such as PRINCE2, PMP or equivalent; · In the case of a Technical Project Manager, possesses experience with computer development work with a project-based focus and experience working with IT teams; · Possesses experience of delivery of ServiceNow solutions;

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Role	Role Description
	and · Possesses minimum of five (5) years relevant experience.
ServiceNow AI & Automation Specialist.	The service requirements, level of experience, skillset and capabilities associated with this role include but are not limited to the following: · Strong ServiceNow administration experience (Min 5 years) · Excellent understanding of ServiceNow AI and Automation capabilities. · Experience configuring and administering: · Generative AI capabilities, Virtual Agent , Predictive Intelligence, Flow Designer, Integration Hub, Document Intelligence, AI Search, Knowledge Management and Service Operations automation · Strong understanding of ServiceNow platform architecture and security. · Experience with AI governance, risk management and compliance frameworks. · Knowledge of data protection and privacy requirements. · Experience implementing automation and workflow optimisation solutions. · Experience delivering enterprise-scale ServiceNow solutions. · Experience implementing AI or intelligent automation solutions. · Experience managing platform governance and compliance controls. · Experience creating technical standards, operating procedures and governance documentation.

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Role	Role Description
ServiceNow Developer & Release Manager	The service requirements, level of experience, skillset and capabilities associated with this role include but are not limited to the following: · Expert knowledge of ServiceNow administration and development (Min 5 years) · Advanced experience with: , Flow Designer, IntegrationHub, Business Rules, Script Includes, Client Scripts, UI Policies, Catalog Development, Scoped Applications, REST and SOAP integrations and Update Sets and Application Repository · Strong understanding of ServiceNow platform architecture. · Experience implementing and governing release management processes. · Strong understanding of Agile, Scrum and DevOps methodologies. · Experience with source control, deployment strategies and environment management. · Knowledge of ITIL Change and Release Management processes. · Significant experience leading ServiceNow development teams. · Proven experience managing Agile delivery within enterprise environments. · Experience establishing and enforcing release management controls. · Experience managing complex platform deployments and upgrades. · Experience producing technical standards, operating procedures and governance documentation.
ServiceNow Module Specialist	The service requirements, level of experience, skillset and capabilities associated with this role include but are not limited to the following: · Is a Subject Matter Expert (“SME”) in a particular module or function of ServiceNow; · A critical thinker with an well-developed set of problem solving skills; · Holds a third level degree or certification in a technology discipline; · Possesses experience implementing at least 10 substantial ServiceNow projects over the last five (5) years; · Possesses knowledge of relevant technologies to assist with selection of appropriate solution; · Possesses experience on large size [at least +1,000 users and three (3) ServiceNow modules] and medium size [at least +250 users and two (2) ServiceNow modules] implementations of ServiceNow; and · Possesses minimum of five (5) years relevant experience.

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Role	Role Description
ServiceNow Reporting Specialist	The service requirements, level of experience, skillset and capabilities associated with this role include but are not limited to the following: · Possesses the ability to identify business intelligence, reporting, and data analysis needs within ServiceNow; · Holds a strong understanding of ServiceNow data models; · Works closely with clients and ICT teams to turn data into critical information and knowledge that can be used to make sound business decisions; · Holds experience in building an understanding of the business at a level of detail that enables them to identify and address critical issues; · Provides data that is accurate, congruent and reliable, and ensures the information is easily available to users for direct consumption or integration with other systems; · Assists in educating and training clients to use the data as an analytical tool, displaying the information in new forms and content for the purpose of analysis and option exploration; · Possesses the ability to conduct feasibility studies, producing high-level and detailed business models; · A critical thinker with a well-developed set of problem-solving skills; and · Possesses minimum of four (4) years relevant experience.

[•]

Role	Role Description
ServiceNow Security and Data Segregation Specialist.	The service requirements, level of experience, skillset and capabilities associated with this role include but are not limited to the following: · Expert knowledge of ServiceNow ACL architecture and evaluation logic. · Strong understanding of role-based access control (RBAC) principles. · Experience designing complex data segregation models within ServiceNow. · Advanced knowledge of: ACL scripting, Dynamic filters, User Criteria, Business Rules, GlideRecord, Script Includes, Client Scripts, Catalog and Portal security Group and role management · Experience securing ITSM processes including Incident, Request, RITM, Catalog · Tasks and custom applications. · Understanding of ServiceNow platform security, auditability and governance controls. · Experience troubleshooting visibility and access issues across large-scale ServiceNow environments. · Knowledge of GDPR, least privilege principles and enterprise security frameworks. · 5+ years ServiceNow administration and development experience. · Demonstrated experience designing and implementing ACL frameworks in enterprise environments. · Experience managing large role and group structures with complex segregation requirements. · Experience supporting multi-party environments involving internal users, external users, vendors and managed service providers. · Experience producing solution designs, technical standards and governance documentation.

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Role	Role Description
ServiceNow System Administrator / Level 3 Engineer.	The service requirements, level of experience, skillset and capabilities associated with this role include but are not limited to the following: · Configures ServiceNow Modules based on agreed business requirements; · Adheres to a given set of constraints specified at the outset of the design process; · Possesses experience with Agile Methodologies; · Methodical in approach to configuration; · Possesses very good understanding of workflows and business processes; · Maintain secure and robust RBAC model to meet NTA data segregation requirements. · Ensure that the RBAC model is scalable, testable, performant and maintainable for the lifetime of NTA contract. · Holds a third level degree or certification in a technology discipline; · Certificated in the Administration and Configuration of ServiceNow; and · Possesses minimum of three (3) years relevant experience.

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Role	Role Description
ServiceNow Technical Architect (senior)	The service requirements, level of experience, skillset and capabilities associated with this role include but are not limited to the following: · Possesses strong solution design and architecture pedigree and technical experience relating to management of ServiceNow type projects; · Possesses experience implementing at least two (2) ServiceNow projects over three (3) years; · Possesses experience across all phases of the delivery from design to transition to operational support; · Oversees the implementation of the solution and ensure it is delivered aligned with standards defined and supplier contractual obligations; · Works with technology partners to ensure successful delivery of solutions and interfaced systems; · Manages business and technology stakeholders; · Manages and oversees the successful and timely delivery of obligations to ensure successful delivery of the solution; · Works with supplier team review and sign off solution designs; · Holds a third level degree or certification in a technology discipline; · Possesses the ability to create solution prototypes; · Holds knowledge of relevant technologies to assist with selection of appropriate solution; · Holds direct solution development by acting as an advisor to the development team; · Supports project management and implementation to ensure that resources, risk management and planning stay aligned with the solution goals; and · Possess minimum of five (5) years relevant experience.
ServiceNow Tester/Quality Assurance Lead	The service requirements, level of experience, skillset and capabilities associated with this role include but are not limited to the following: · Possesses practical test knowledge of documentation (Test Strategy & Plans), scripting, defect management and test reporting; · Possesses experience with the setup, configuration, usage and maintenance of automated testing in ServiceNow; · Possesses understanding of multiple Software development methodologies including Waterfall and Agile; · Holds experience of leading small teams of Test Analysts and/or Business Users; · Holds experience of working with third party suppliers; · Holds experience in using test and defect management tools; and · Possesses minimum of three (3) years relevant experience.

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Role	Role Description
UI / UX Specialist	A specialist in all UX / UI aspects in relation to Service Portal, Employee Center, UI Builder, Workspaces and Email Notifications.

Table 1 - Role Descriptions

SCHEDULE 4 – Service Level Agreement

1. Provision of Services

This Schedule describes the performance management model for the Services and the Service Levels the Supplier is required to achieve.

1.1 The Performance Management Model

The performance management model seeks to:

- (a) facilitate linkage between the Authority's desired business objectives and the activities to be performed by the Supplier;
- (b) support the achievement of best value by ensuring that performance is continually measured and lessons learned to achieve continuous improvement in the provision of the Services; and
- (c) incentivise the Supplier to meet the Target Service Levels and to remedy any failure to meet the Target Service Levels expeditiously.

1.2 Objectives in the Performance of the Management Model

The Authority's objectives in the performance of the management model are

- (a) to ensure that the Services are of a consistently high quality and meet the requirements of the Authority;
- (b) to ensure the Authority experiences good customer service;
- (c) without prejudice to paragraphs 1.2 (a) and (b) above, maximise revenue collection on behalf of the Supplier;
- (d) prevent any damage to the reputation of the Authority; and
- (e) provide a mechanism whereby the Authority can attain meaningful recognition of inconvenience or losses resulting from any failure by the Supplier to deliver the Target Service Levels.

2. The Performance Management Regime

2.1 Target Service Levels and Key Performance Indicators

Table 1 sets out the Key Performance Indicators ("KPIs").

Appendix 1 details the Service Levels assigned to the KPI.

- (a) The Supplier shall monitor and measure its performance against each of the KPIs set out in Table 1 below, and shall send the Authority a report detailing:
 - i. the actual service level as measured;
 - ii. separate detail and adjustments for exceptions;
 - iii. the service level which was achieved after adjustments; and

- iv. its calculation of Performance Points accrued (if any) in accordance with the Payments Schedule and the Services Schedule.
- (b) The Supplier shall develop, agree with the NTA and implement a guidebook which shall detail how it intends to gather the data for each KPI, process such data to calculate the performance and report on the results (the “Performance Guidebook”).
- (c) The Performance Guidebook shall also list the safeguards and checks put in place to avoid errors and to ensure accurate reporting and provide for an audit trail so that the origins of the reported performance can be easily traced and checked by the Authority.
- (d) The Supplier shall develop, agree and implement operating level agreements with its sub- contractors and include the details of the agreed working relationships and response times in the Performance Guidebook. The Supplier shall be responsible for coordinating the activities between each of its sub-contractors and Suppliers of fulfilment systems in respect of the Services.
- (e) The Performance Guidebook shall be approved by the NTA prior to the Operational Services Start Date and shall be subject to annual review and approval by the Authority.
- (f) The Supplier shall at all times provide the Services in such a manner that the Target Service Level for each KPI (as set out in Table 1) is achieved.
- (g) For each KPI, performance below the Target Service Level shall lead to the accrual of Performance Points, as set out in the Payments Schedule.

2.2 Calculation of Performance Points

- (a) Each Target Service Level set out in Table 1 of this Schedule has been assigned a ‘category’ on the basis of how critical it is to the successful operation of the Dedicated ServiceNow Instance contract.
- (b) Red categorises the most critical category of Target Service Level, amber is the next most critical category of Target Service Level and Yellow is the least critical category of Target Service Level. A number of points have been attached to each ‘category’.
- (c) Where a failure to achieve a Target Service Level is caused by a Relief Event or Force Majeure and the Supplier complies with the relevant requirements, then from the time at which the Relief Event or Force Majeure begins until such time as the Relief Event or Force Majeure ends, the NTA may not allocate Performance Points in relation to such failure to achieve that Target Service Level.

2.3 Performance Points Allocation.

Performance points shall be allocated as follows:

-
- (a) For Target Service Levels that are measured monthly, Performance Points shall be incurred for each month in which the failure to meet the relevant Target Service Level subsists.
 - (b) Performance Points are applied once per KPI to the maximum extent where the maximum Performance Points are applied where there are multiple failures. For the avoidance of doubt, Performance Points in a KPI category are not aggregated where two Target Service Level failures occur.
 - (c) For Target Service Levels that are measured once, per event, in a calendar quarter or annually, Performance Points shall be incurred in the month that the Target Service Level is measured and for each remedy period thereafter that the failure to meet the relevant Target Service Level subsists.
 - (d) Failure by the Supplier to meet a Target Service Level that is:
 - i. Category 'Red' shall incur twenty (20) Performance Points;
 - ii. Category 'Amber' shall incur ten (10) Performance Points; and
 - iii. Category 'Yellow' shall incur five (5) Performance Points.
 - (e) Where the Supplier fails to achieve the Target Service Levels for any KPIs for more than two (2) consecutive Contract Month, the Authority may, at its sole discretion, award additional Performance Points as follows:
 - i. Category 'Red' shall incur an additional ten (10) Performance Points (Total Performance Points for this 'Red' category increases to thirty (30) Performance Points for that KPI);
 - ii. Category 'Amber' shall incur an additional five (5) Performance Points (Total Performance Points for this 'Amber' category increases to fifteen (15) Performance Points for that KPI); and,
 - iii. Category 'Yellow' shall incur an additional five (5) Performance Points (Total Performance Points for this 'Yellow' category increases to ten (10) Performance Points for that KPI);
 - (f) Where the Supplier fails to achieve the Target Service Levels for any KPIs for more than three (3) consecutive Contract Months, the Authority may, at its sole discretion, award additional Performance Points as follows:
 - i. Category 'Red' shall incur an additional fifteen (15) Performance Points (Total Performance Points for this 'Red' category increases to thirty five (35) Performance Points for that KPI);
 - ii. Category 'Amber' shall incur an additional ten (10) Performance Points (Total Performance Points for this 'Amber' category increases to twenty (20) Performance Points for that KPI); and,

- iii. Category 'Yellow' shall incur an additional ten (10) Performance Points (Total Performance Points for this 'Yellow' category increases to fifteen (15) Performance Points for that KPI);
- (g) Any complete failure to perform the Services to which a Target Service Level relates (rather than non-conformance with a Target Service Level) shall be deemed to be Red.

2.4 Monthly Performance Factor

- (a) The total number of Performance Points accrued by the Supplier in the Contract Month shall determine the Monthly Performance Factor to be applied to the Monthly Service Delivery and Maintenance & Support Fixed Cost for that Contract Month as set out in Section 7 of Schedule 2 – Payments Schedule.
- (b) If after six (6) months following the Operational Services Start Date in any successive 12 Contract Months the Supplier incurs more than one thousand (1000) Performance Points in total, the NTA shall be entitled to terminate this Agreement on six (6) months' written notice.

3. Service Level KPIs

The Supplier shall monitor and measure its performance against each of the Key Performance Indicators (“KPIs”) set out in Table 1 below on a continuous basis during the Contract term.

Table 1 – Key Performance Indicators (KPIs)

Ref.	Title	Description	Target Service Level	Performance Points	Type
Service Desk Services					
KPI01	Service Desk Incident Management	Adherence to Incident Response and Resolution Time.	Target Service Level	Target Service Level	Per Table A.1- Service Desk Incident Resolution Time set out in Appendix A – Target Service Levels
KPI02	Service Desk Request Fulfilment	Adherence to Service Desk Request Fulfilment Time.	Target Service Level	Target Service Level	Per Table A.2- Service Desk Request Fulfilment Time set out in Appendix A – Target Service Levels

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Ref.	Title	Description	Target Service Level	Performance Points	Type
KPI03	Customer Satisfaction (CSAT)	Customer satisfaction score of service (based on resolution of tickets) Customer satisfaction score from the VIP stakeholders	80% positive (Monthly) 90% positive (Bi-annually)	Target Service Level	Per Table A4 – Customer Satisfaction in Appendix A – Target Service Levels
ICT Service Governance Services					
KPI04	Availability Management	Adherence to System Availability.	Target Service Level	Target Service Level	Per Table A.6. and A.7- System Availability set out in Appendix A – Target Service Levels
KPI05	Change Management	Adherence to Change Management.	Target Service Level	Target Service Level	Per Table A.8- Change Management set out in Appendix A – Target Service Levels
KPI06	Access Management	Adherence to Access Management Schedule.	Target Service Level	Target Service Level	Per Table A.9- Access Management set out in Appendix A – Target Service Levels

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Ref.	Title	Description	Target Service Level	Performance Points	Type
KPI07	Knowledge Management	Delivery and Maintenance of complete technical and operational documentation for all instances of ServiceNow. As per the Authority's requirements.	99% accuracy	Red	Bi-annually (every 6 months)
KPI08	Standard Reports	Delivery of key Standard Reports as set out in Appendix C – Standard Reports If a delivery time for a Standard Report is not stated in this Agreement, the Supplier and the NTA shall Approve the date of relevant delivery and frequency of the Standard Report during the Initial Services period. To the extent that the Supplier provides a Standard Report late, incomplete or incorrect as a direct result of the failure of the NTA to provide information necessary to complete the Standard Report and the Supplier has notified the NTA of this, such Standard Report shall not be included in the calculation for this KPI only be for a period equivalent to only the period of delay in receiving such information from the NTA. Any further or unrelated delay by the Supplier in providing the Standard Report will be included in the calculation for this KPI.	100%	Amber	As set out in Appendix C – Standard Reports (Frequency)

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

KPI09	Delivery of ICT Managed Services Plans	Delivery and Maintenance of Managed Services Plans, including: • Service Management and Operations Plan (annually) • Service Continuity Plans and Recovery Plans (every six (6) months) • Service Benchmark and Service Improvement and Innovation Plan (annually) • Exit Management Plan (annually) If a delivery time for an ICT Managed Services Plan is not stated in this Agreement, the Supplier and the NTA shall Approve the date of relevant delivery and frequency of the ICT Managed Services Plan during the Initial Services period. To the extent that the Supplier provides an ICT Managed Services Plan late, incomplete or incorrect as a direct result of the failure of the NTA to provide information necessary to complete the Plan and the Supplier has notified the NTA of this, such Plan shall not be included in the calculation for this KPI only be for a period equivalent to only the period of delay in receiving such information from the NTA. Any further or unrelated delay by the Supplier in providing the Plan will be included in the calculation for this KPI.	100%	Amber	As defined in the Description
-------	--	--	------	-------	-------------------------------

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Ref.	Title	Description	Target Service Level	Performance Points	Type
ICT Service Operations Services					
KPI10	Utilisation and integration with Key NTA ICT Systems	- SFTP Servers in the NTA. - CI synch for CMDB integration. - Any other integrations owned or managed by the NTA connected to ServiceNow, as per the Authority's requirements	Target Service Level	Target Service Level	As Per Table A10 - Utilisation and integration with Key NTA ICT Systems
KPI11	Vulnerability Management	Adherence with Vulnerability Management Resolution Time. In relation to custom code, scripting and integrations to / from the platform	Target Service Level	Target Service Level	Per Table A.12- Vulnerability Resolution Time set out in Appendix A – Target Service Levels
KPI12	Patch Management	Adherence with Patch Management Time. Percentage of patches applied to the relevant assets. For firmware and software updates as agreed with the NTA and in line with the minimum of n-1 level.	Target Service Level	Target Service Level	Per Table A.14- Patch Resolution Time set out in Appendix A – Target Service Levels

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Ref.	Title	Description	Target Service Level	Performance Points	Type
KPI13	Malware Defences	Adherence to Malware Defence Time. With information from the service now ISC on antimalware updates and testing.	Target Service Level	Target Service Level	Per Table A.15- Malware Defence Management Time set out in Appendix A – Target Service Levels
KPI14	Data backup	The number of successful backups performed according to backup schedule shall not be less than 95%.	Not less than 95%	Red	Daily Monthly
KPI15	Security Events	Security Event mean time to detect (MTTD), mean time to respond (MTR) and mean time to resolve (MTTR)	Target Service Level	Target Service Level	Per Tables A.16 & A17 Security Event MTTD, MTR & MTTR set out in Appendix A – Target Service Levels

Table 2 – Performance Indicators (PIs)

Ref.	Title	Description	Target Service Level	Performance Points	Type
Systems Management					
PI01	Licence Management	The number of notifications of expiry of a system licence (those where the Supplier is directly responsible for and those that the Supplier is monitoring. Also includes warranty or support renewals.) received less than three (3) months before the expiry of a system licence shall be zero (0). Ensure that the NTA (and its users) are only using software it is authorized to use. Noncompliance items shall not exceed zero (0). Ensure that the number of users of an application does not exceed the number of licences available. Noncompliance items shall not exceed zero (0).	100% 100% 100%	Amber	Monthly

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Ref.	Title	Description	Target Service Level	Performance Points	Type
PI02	CMDB Health & CSDM Governance	The Supplier shall ensure that the ServiceNow CMDB framework, health monitoring, identification and reconciliation processes, CI relationship management, and CSDM-aligned data model operate effectively. The Supplier is not responsible for the ensuring the completeness or accuracy of business-owned Configuration Item data but is responsible for maintaining the mechanisms, controls, and governance required to support CMDB health and CSDM compliance.	95% - Percentage of CMDB governance controls, health monitoring and CSDM compliance.	Amber	Monthly
PI03	Supplier Processes and Procedures	The Supplier shall review and update all documented processes, procedures and systems architecture documentation for the Managed Services annually. The Supplier shall ensure that all changes to the Managed Services are updated in the relevant process, procedures, and systems architecture	Failure to review and update the process, procedures and systems architecture documentation for the Services on an annual basis.	Amber	Annual

[•]

Ref.	Title	Description	Target Service Level	Performance Points	Type
		documentation within ten (10) Working Days of the relevant change's completion. These processes these PIs relate to are those done by the Supplier internal to the Supplier, but which relate to and involve the NTA departments and users AND processes created by the NTA which are followed by the Supplier but may be amended in collaboration with the NTA to provide services e.g. starters / leavers, User access etc	Failure to update the process, procedures and systems architecture documentation for all changes to the ServiceNow Managed Services within ten (10) Working Days of the relevant change being made.	Amber	Monthly
Service Continuity and Disaster Recovery					

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

PI04	Disaster Recovery	The Supplier shall be responsible for undertaking that - the NTA ServiceNow instances are included in at least 1 annual full failover test per environment and retest if required - The backup of the production NTA data has a full restore test at least every 6 months and this is fully tested. - the testing and execution of system and service recovery plans, at least annually (every twelve (12) months), or as determined in the ICT Service Continuity Plans; and, In the event of an unsuccessful test of the areas above, the Supplier shall: - update all documentation, processes and procedures within one (1) week of an unsuccessful test; and - perform a new test within one (1) month of the unsuccessful test.	100% undertake at least 1 annual full failover test per environment and retest if required. 100% testing and restoring the NTA production backup bi-annually (every 6 months) 100% testing and executing of system and service recovery plans bi-annually (every 6 months) 100% update documentation, processes and procedures within one (1) week of an unsuccessful test 100% performance of new test within one (1) month of	Red	Per event, reported monthly
------	-------------------	--	--	-----	-----------------------------

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Ref.	Title	Description	Target Service Level	Performance Points	Type
			the unsuccessful test		
Audit and Compliance					
PI05	Remedial plan	Where exceptions or control deficiencies are identified as part of any audit of controls for which the Supplier has responsibility, the Supplier shall present a plan to the NTA to rectify such exceptions or control deficiencies, within ten (10) Working Days.	Plan to rectify any exceptions or control deficiencies presented no later than ten (10) Working Days from date of identification of such exception or control deficiency	Amber	Per event, reported monthly

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Ref.	Title	Description	Target Service Level	Performance Points	Type
PI06	Remedial action	Where exceptions or control deficiencies are identified as part of any audit of controls for which the Supplier has responsibility, the Supplier shall rectify such exceptions or control deficiencies, within twenty (20) Working Days.	100% of any exceptions or control deficiencies identified as part of any audit of controls rectified within twenty (20) Working Days or as (or as otherwise Approved by the NTA)	Red	Monthly
PI07	Provision of information	Provision of information on foot of audit request received from the NTA. This is to include evidence to support audit requests from third parties auditing the NTA as well as requests from the NTA to audit the MSP processes.	Provision of 100% of requested information to the NTA within five (5) Working Days	Red	Monthly

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Ref.	Title	Description	Target Service Level	Performance Points	Type
PI8	Retention of Evidence of Approval	The number of failures by the Supplier to record and retain appropriate evidence of: • completion of required tasks /activities to perform the Services; and • review/approval of the required tasks /activities by the appropriate Supplier/NTA personnel; (together with any required supporting evidence to support any audit or review of the ICT Managed Services) shall be zero (0).	Zero (0)	Amber	Monthly
Catalog Management					
PI9	Service Catalogue Management	Delivery and Maintenance of Service Catalogue.	99% accuracy	Red	Bi-annually (every 6 months)
Data Protection					

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

Ref.	Title	Description	Target Service Level	Performance Points	Type
PI10	Data Protection	The number of instances where the Supplier failed to notify the NTA immediately after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data, including personal data, transmitted, stored or otherwise processed by the Supplier or its sub-processors shall be zero (0). This relates to data held on the NTA environment and data about or relating to the NTA held on the Supplier's environment.	100%	Red	Daily, Reported Monthly
PI11	Data Protection	The number of failures by the Supplier to accurately compile and provide the Supplier's response to a subject access request to the NTA within ten (10) days of receipt of the request shall be zero (0). The number of failures by the Supplier to complete any requests to update or delete (if applicable) a Customer's personal data in accordance with the NTA's Data Protection Policy within one (1) day of receipt of the request by the Supplier shall be zero (0). This relates to data held on the NTA environment and data about or relating to the NTA held on the Supplier's environment.	100%	Red	Daily, Reported Monthly

[•]

Ref.	Title	Description	Target Service Level	Performance Points	Type
Event Management					
PI12	Event Management within the ServiceNow instance. For example: Errors, Warnings in the Logs of the instance.	Adherence to Event Resolution Time.	100%	Red	Per Table B.1- Event Resolution Time set out in Appendix B – Target Service Levels for PIs
Problem Management					
PI13	Problem Management	Adherence with Problem Management Resolution Time.	100%	Amber	Per Table B.2- Problem Resolution Time set out in Appendix B – Target Service Levels for PIs

4. Service Levels – Response Times

See Appendix A

5. Contract Management

5.1 The Supplier will be required to attend monthly performance review meetings with the Authority and any other relevant agencies to review ongoing tasks as well as new projects. The frequency of these monthly meetings shall be kept under review and may increase/decrease as required by the Authority.

5.2 The Supplier shall provide a monthly report in advance of each meeting that shall provide a view of the previous quarter's performance and the up to date progress report on current activities and cover topics such as:

- a) High priority topics;
- b) Status of work in progress projects/ action items including next steps;
- c) Monthly performance data;
- d) Support queries;
- e) Discussion items/issues; and
- f) Projects Update

5.3 The Supplier will be required to attend monthly steering / contract review meetings with the Authority and any other relevant agencies to review ongoing tasks as well as new strategic initiatives. The frequency of these monthly meetings shall be kept under review and may increase/decrease as required by the Authority.

5.4 The Supplier shall also provide access to a dedicated Account Manager who will be required to manage the day-to-day operation of the account. The Account Manager may be required to facilitate a weekly call with the Authority's personnel in relation to the account.

5.5 The Supplier shall ensure that the dedicated Account Manager is available at any time during normal business hours to discuss with representatives of the Authority any matter that may be of concern/of urgency to the Authority. During absences of the Supplier's Account Manager due to illness or annual leave the Supplier will nominate for this purpose a substitute executive of appropriate seniority and qualifications.

SCHEDULE 5 – Contract Change Control

1. Change Control Procedure

1.1 Where either party (the "Requesting Party") wishes to make a material change to the terms of this Agreement including, without limitation, any change to:

- any Deliverable or Services;
- any Supplier Support Systems;
- the timeframes for the provision of any Deliverable or Services;
- this Agreement; or
- any Delivery Plan

the procedure in this Schedule (the "**Change Control Procedure**") shall apply. The Change Control Procedure shall also apply in respect of any matters which are specifically identified in the Agreement as being subject to the Change Control Procedure.

1.2 A "**Change**" in the context of the Change Control Procedure shall mean any change which is not a Service Request as defined below.

1.3 A "**Change Request**" is a request for any Change

1.4 The Change Control Procedure shall also apply in respect of any matters which are specifically identified in this Agreement as being subject to the Change Control Procedure.

1.5 A "**Service Request**" is a request for any service included in this Agreement.

1.6 Service Requests shall be performed in accordance with this Agreement, and where payments are applicable, such payments shall be calculated and paid in accordance with the Payments Schedule

2. Change Request Form

2.1 All change requests must be documented in a request form (a "**Change Request Form**") which shall include, as a minimum, the following details:

- a) a description of the proposed Change and the timeframe within which the Change should be effected;
- b) the reasons for the Change (including specifying whether the Change is required as a result of any change in Applicable Law) and a high-level description of the proposed business impact;
- c) where the Change is being requested to reflect new Services or Supplier Support System requirements, a comparison of the new requirements with the existing requirements; and

-
- d) any other details relevant to the request for the Change.
- 2.2 The Change Request Form shall be signed by the Project Manager of the Requesting Party and submitted to the Project Manager of the other party.
- 2.3 The Supplier shall create an entry in the Change Control Register, as set out in section 5, for the Change Request and mark it with a status of “pending approval”.
- 2.4 The Change Request shall be automatically allocated a unique reference number. This number shall be used in all future references to the Change Request.
- 2.5 The NTA’s Representative may elect to meet and discuss the matters referred in the Change Request with the Supplier, the location of the meeting being at the discretion of the NTA. The meeting shall be attended by the Key Personnel specified in Table 1 of the Governance Schedule and such other Supplier Staff and sub-contractors who have responsibilities relevant to the subject matter of the meeting. Each party shall be responsible for their own costs associated with preparing for and attending such meetings.
- 2.6 Each party shall be responsible for their own costs associated with preparing, considering and submitting Change Request Forms including but not limited to any related record keeping.
- 2.7 The Supplier shall not implement any Change until it is approved by the NTA’s Representative in accordance with the approval procedure set out in clause 5 of this Agreement.
- 3. Impact Statement**
- 3.1 The Supplier shall provide the NTA’s Representative with a cost for preparing an **“Impact Statement”** within five (5) Working Days of receipt or submission of a Change Request Form (or such other period as the parties may agree).
- 3.2 The NTA’s Representative, as soon as practicable after receipt and consideration of such cost, may elect by giving written notice to the Supplier either to:
- a) accept the cost in which case the Supplier shall provide the NTA’s Representative with an Impact Statement within ten (10) Working Days of receipt of an acceptance notification (or such other period as the parties may agree);
 - b) reject the cost in which case the Change Request shall be marked as rejected;
 - c) direct the Supplier to proceed with the preparation of an Impact Statement without reaching agreement in respect of the cost, in which case the Supplier shall provide the NTA’s Representative with an Impact Statement within ten (10) Working Days of receipt of an

acceptance notification (or such other period as the parties may agree); or

- d) require the Supplier to produce a revised cost for preparing an Impact Statement.

3.3 The Impact Statement shall include, as a minimum, the following details:

- a) the estimated number of labour days (or labour hours) and personnel (including levels of qualification) and details of the work categories required to deliver the Change within the timeframe specified in the Change Request Form;
- b) details of verification checks to be performed by the Supplier to ensure that the Change complies with the information set out in the Change Request Form;
- c) description of risk assessment and back-out plan where Supplier Support System changes are required;
- d) full disclosure of any assumptions underlying any estimates;
- e) the overall impact on the Payments under this Agreement (i.e. reduction or increase) which shall include a breakdown of how such charges relate to the details in paragraph 3.3(a) above so as to facilitate, where relevant, any variation in the Payments under this Agreement and sharing of any consequent savings, as described in paragraph 3.7 below;
- f) any regulatory approvals required to implement the proposed Change;
- g) details of any sub-contractors the Supplier is required/wishes to employ to implement the proposed Change;
- h) the timetable for the Change including any impact on the timeframes for the delivery of the Services;
- i) any impact on the scope of the Services (including, where relevant, any benefit to the Services, e.g. in terms of KPIs etc.) to be provided under this Agreement;
- j) any impact on any Delivery Plan;
- k) the estimated costs on a time and material basis; and
- l) the proposed costs on a fixed cost basis.

3.4 The NTA's Representative as soon as practicable after receipt and consideration of the Impact Statement may elect to meet and discuss the matters referred in the Impact Statement with the Supplier, the location of the meeting being at the discretion of the NTA. The meeting shall be attended by the Key Personnel specified in Table 1 of the Key Personnel Schedule and such other Supplier Staff who have responsibilities relevant to the subject matter of the meeting. Each party shall be responsible for their own costs associated with preparing for and attending such meetings.

3.5 Following consideration of the Impact Statement the NTA's Representative may elect by giving written notice to the Supplier either to:

- a) accept the Impact Statement in which case this Agreement and the scope of the Services shall be amended accordingly, and the Change shall be implemented in accordance with this Schedule;
 - b) reject the Impact Statement in which case this Agreement and the scope of the Services shall remain unchanged; or
 - c) direct the Supplier to proceed without reaching agreement in respect of the cost of implementing such Change (as set out in the Impact Statement), in which case this Agreement and the scope of the Services shall be amended accordingly, and the Change shall be implemented in accordance with this Schedule; or
 - d) require the Supplier to produce a revised Impact Statement by repeating (up to a maximum of two (2) times) the procedure set out in paragraphs 3.1 and 3.2 above.
- 3.6 If the NTA accepts the Impact Statement (with or without revision in accordance with paragraph 3.5(c) above), implementation of the relevant Change shall be commenced and completed by the Supplier in accordance with the programme for implementing and verifying the proposed Change included in the Change Request Form (as modified). Within this period (or such longer period as may be agreed by the parties), the parties shall agree the remaining details as soon as practicable and shall enter into any documents which are reasonably required to implement the Change.
- 3.7 If the proposed Change causes or will cause the Supplier's costs or those of a sub-contractor to decrease, there shall be a decrease in the Payments under this Agreement. The amount of such decrease shall be agreed between the parties as part of the Impact Statement review and acceptance procedure set out at paragraphs 3.4, 3.5 and 3.6 of this schedule.
- 3.8 Where the Supplier proposes to employ sub-contractors to implement some or part of the Change, the NTA may require the Supplier to seek alternative quotes/estimates in respect of such proposed work or provide evidence that it has used all reasonable endeavours to oblige the proposed sub-contractors to minimise any increase in costs and maximise any potential cost savings.
- 3.9 Where the estimated costs associated with any Change include the purchase of equipment (e.g. hardware), software products or software subscription products, and such products are procured by the Supplier through third party providers, the Supplier shall at the request of the NTA, provide evidence of obtaining value for money on behalf of the NTA through benchmark pricing information.
4. Costs
 - 4.1 Where a Change is required as a result of a change in Applicable Law, the costs of implementing such Change, including the cost of preparing the Impact Statement (provided that the costs of preparing the Impact Statement are reasonable and agreed in advance with the NTA) shall be borne by the

NTA, save where the change in Applicable Law applies generally to the business of the Supplier or will affect the provision of services by the Supplier to some or all of its other customers, in which circumstances the Supplier shall be responsible for all costs associated with the Change.

4.2 Subject to paragraph 4.1 above, and save as may be agreed otherwise between the parties, in respect of Changes, where

- a) the Supplier is the Requesting Party, the Supplier shall bear the cost of preparing the Impact Statement and (where relevant, the cost of carrying out the activities set out at section 6 below); and
- b) where the NTA is the Requesting Party, the NTA shall bear the Supplier's additional costs in preparing the Impact Statement and (where relevant, the cost of carrying out the activities set out at section 6 below), provided that such costs are reasonable and agreed in advance with the NTA.

4.3 Any costs payable by the NTA in connection with the implementation of a Change (including in connection with the preparation of an Impact Statement and, where relevant, the cost of carrying out the activities set out at section 6 below) shall be:

- a) at the choice of the NTA, based on a fixed cost as proposed by the Supplier in paragraph 3.3(l) or the estimated costs incurred by the Supplier as required under paragraph 3.3(k), plus a reasonable margin, in implementing the relevant Change and preparing the relevant Impact Statement subject to review at intervals agreed in advance with the NTA; and
- b) allocated to a particular budget or payment category (e.g. Operating Payments, Additional Payments) as agreed between the parties or as set out in the Payments Schedule.

4.4 In circumstances where the Supplier does not have the specialist skills required to implement a particular Change, or to produce an Impact Statement in respect of a particular Change, the parties may, on an exceptional basis, agree to engage a specialist consultancy service provider (the "Consultancy Service Provider") to advise or consult in relation to the Change. The terms of engagement of any Consultancy Service Provider shall be agreed between the parties and any costs payable in respect of the Consultancy Service Provider shall be agreed in accordance with paragraph 4.3 above.

4.5 In the event that the NTA directs the Supplier to continue with:

- a) the preparation of an Impact Statement in accordance with paragraph 3.2(c) above; or
- b) the implementation of a Change in accordance with paragraph 3.5(c) above;

then the parties shall meet in good faith as soon as reasonably practicable to try and reach agreement in respect of the relevant costs. If the parties cannot reach

agreement in respect of such costs, the dispute shall be dealt with in accordance with the dispute resolution procedure set out in clause 48 of this Agreement.

5. Record Keeping

5.1 The Supplier shall keep records, in an online system (the “Change Control Register”) provided by the Supplier, in such form and for such period as may be agreed between the Supplier and the NTA, of all Changes carried out pursuant to the Change Control Procedure. Such records shall include, as a minimum, the following details:

- a) unique identification number corresponding to the relevant Change Request Form;
- b) the Change Request Form;
- c) description and status of the Change (e.g. pending approval, agreed, implemented, completed, rejected);
- d) description and status of the verification checks conducted;
- e) actual cost of implementing the Change (including costs to date and expected final costs);
- f) details of the business impact of the Change;
- g) a log of all written notifications to accept, reject and revise the Change, including scanned copies of signed acceptance documents;
- h) a log of all purchase orders issued by the NTA in respect of the Change; and
- i) a log of all invoices paid by the NTA in respect of the Change.

5.2 The Change Control Register shall be accessible in a secure manner via the Internet and shall incorporate access control based on approved roles.

5.3 The Supplier shall provide access to the Change Control Register for the NTA’s personnel.

5.4 The Change Control Register shall include a user interface for keyword and content searching.

5.5 The Change Control Register shall include a user interface for navigation of records via categories, filtering based on date range (for created date, approved date, implemented date, invoiced date, paid date), status, and sort order for selected filters or combination of filters.

6. Disputes

6.1 The dispute resolution procedure set out in clause 48 of this Agreement may be invoked where following completion of the procedure in section 3, the parties fail to reach agreement on a request for Change, including in relation to costs.

7. Updates to documentation subject to Change

- 7.1 The Supplier shall review and update all relevant documents forming part of or agreed in connection with this Agreement to the extent necessary to take account of any Change agreed pursuant to the Change Control Procedure.
8. Emergency Changes
- 8.1 In the event of an emergency, where there is not sufficient time available for the parties to carry out their respective obligations as set out in the Change Control Procedure, the Supplier shall use reasonable endeavours to satisfy the Change Request on an emergency basis (an “Emergency Change”). As soon as is reasonably practicable, the parties shall complete the Change Control Procedure (insofar as possible) in respect of the Emergency Change. In an event of a dispute relating to an Emergency Change, the parties shall meet in good faith as soon as reasonably practicable to try and reach agreement. If the parties cannot reach agreement, the dispute shall be dealt with in accordance with the Dispute Resolution Procedure set out in clause 48 of this Agreement.
- 8.2 Each party agrees to carry out its respective obligations in relation to this process in good faith and acting reasonably.

SCHEDULE 6 – Exit Management Plan

1. General

- 1.1 This Schedule describes the Exit Management Services to be provided by the Supplier under this Agreement, and the elements to be included in the Exit Management Plan. The Exit Management Services include:
- (a) Providing information to support the re-tendering of the Services (or any part thereof);
 - (b) Developing and updating of the Exit Management Plan
 - (c) Organising, planning, and implementing tasks and activities during the period from notification of the termination of this Agreement to the end of the Term, or twelve (12) months prior to the expiry of this Agreement (as applicable) (the “Exit Transition Period”) pursuant to the Exit Management Plan;
 - (d) Transferring of the overall operation of the Services (or any part thereof) from the Supplier to the New Service Provider under this Agreement during the Exit Transition Period;
 - (e) Transferring knowledge;
 - (f) Transferring administrative user accounts, passwords, assets, sub-contracts and software licenses; and
 - (g) Data held in Supplier systems as required by the NTA.
- 1.2 The Exit Management Services shall be carried out without interruption to the Services.
- 1.3 The Supplier shall be responsible for the overall management of the exit and service transfer arrangements and shall provide a project manager (the “**Exit Manager**”) who shall be appointed for the duration of the Exit Transition Period. The Supplier shall ensure that the Exit Manager has the requisite authority to arrange and procure all necessary resources to enable the Supplier to comply with the requirements set out in this Schedule.
- 1.4 The Supplier shall ensure that appropriate resources are made available on a regular basis and as necessary throughout the Exit Transition Period such that the aims, objectives and specific provisions of this Schedule can be fully realised.
2. **Obligations on providing information to support the re-tendering of Services**

2.1 The Supplier shall provide, at the request of the NTA, the following material in relation to any re-tendering activity or any potential New Service Provider undertaking due diligence activities:

- (a) details of the Services;
- (b) details of the ICT Managed Services support systems, including system architecture, host systems, software libraries and components, manuals and support documentation;
- (c) details of all Third Party Software;
- (d) details of any NTA assets or equipment used and managed by the Supplier to provide the Services (the “**Assets**”) including make, model and asset number and details of their condition and physical location;
- (e) a copy of any training plan and training materials, in editable format;
- (f) a copy of the latest NTA Business Continuity and Disaster Recovery Plan, in editable format;
- (g) an inventory of NTA Materials in the Supplier's possession or control (if applicable);
- (h) the numbers and grades of all staff employed by the Supplier or its sub-contractors in the provision of the Services and details of their remuneration (including salary and all benefits, perquisites, bonuses, commission, overtime or other such payments);
- (i) historical usage and performance data not previously provided in monthly operational reports; and
- (j) supporting additional information requests as required by the NTA.

3. Development and Updating of Exit Management Plan

- 3.1 The parties shall discuss and agree an exit management plan within not more than 12 months from the date of signature of this Agreement (the “Exit Management Plan”) covering action to be taken in respect of the termination or expiry of the Agreement.
- 3.2 The parties shall review and, if necessary, agree updates to the Exit Management Plan at 6 monthly intervals from the date on which the Exit Management Plan is first agreed in order to ensure that it reflects the contemporaneous state of the Services.

4. Content of Plan

- 4.1 The Exit Management Plan shall, as a minimum:

- a) provide for the assignment and/or novation to the Authority of any licences or other contracts with third parties on which the supply of the Services, or any replacement services, are dependent or for the procurement of similar licences or contracts directly between the Authority and the relevant third party on terms no less favourable than those provided to the Supplier;
- b) seek to ensure that there is an orderly and smooth transition from the performance of the Services by the Supplier to the performance of the Services, or any replacement services, by the Authority or any New Service Provider;
- c) define the responsibilities of both parties clearly in the event of exit and transfer;
- d) provide for the handover of the following data to the Authority in such manner as the Authority may reasonably require:
- e) all such data as may be necessary to facilitate the continued provision of the Services, or any replacement services, by the Authority or a New Service Provider seamlessly and without interruption; and
- f) all such data as the Authority may deem necessary to enable a New Service Provider to tender for the provision of the Services or any replacement services; and
- g) provide for any training reasonably required by the Authority for the personnel (of either the Authority or any New Service Provider) who will be assuming responsibility for the Services or any replacement services.

4.2 The Exit Management Plan shall include the following:

- a) a list and timetable of activities for the Authority and the Supplier to undertake during the exit management period;
- b) full details of any dependencies on the Authority for the successful implementation of the Exit Management Plan; and
- c) such other details as the Authority and the Supplier consider appropriate when agreeing the terms of the Exit Management Plan.

5. Exit and Service Transfer

5.1 Subject to any other management or governance structures agreed between the parties in accordance with the paragraphs above, the Supplier shall cooperate with the New Service Provider in relation to exit and service transfer arrangements and shall attend co-ordination meetings at minimum every two (2) weeks with the New Service Provider.

5.2 The Supplier shall be responsible for the overall management of the exit and service transfer arrangements in accordance with the Exit Management Plan.

5.3 During the Exit Transition Period (or such shorter period as the NTA may reasonably require), the Supplier will:

- a) continue to provide the Services (for the duration of the Term); and

- b) at the request of the NTA, provide the Exit Management Services in accordance with the provisions of the Exit Management Plan and the Payments Schedule;
 - c) in each case at no detriment to the Target Service Levels, save to the extent that the parties agree otherwise.
- 5.4 The Supplier shall abide by any reasonable notice of requests from the New Service Provider for access to the Assets and any ICT Managed Services support systems.
- 5.5 At the NTA's request and on reasonable notice, the Supplier shall deliver up-to-date Registers to the NTA.
- 5.6 Subject to paragraph 5.3, the NTA shall be entitled to require the provision of Exit Management Services by providing the Supplier written notice up to twelve (12) months prior to the date of termination or expiry of this Agreement or as soon as reasonably practicable (but in any event, not later than one (1) month) following the service by either party of any notice to terminate. Such notice shall specify:
 - (a) the date from which the Exit Management Services are required, which shall be no earlier than twelve (12) months prior to the expiry of this Agreement or from the service by either party of any notice to terminate (as applicable); and
 - (b) the period during which it is anticipated that Exit Management Services will be required, which shall continue no longer than six (6) months after the date on which the Supplier ceases to provide the Services.
- 5.7 The NTA shall be entitled to require the provision of information to support re-tendering of the Services by providing the Supplier written notice at any time prior to the date of termination or expiry of this Agreement. Such notice shall specify the date from which the support is required and the information to be provided.
- 5.8 The NTA shall have the right to suspend its requirement for the Exit Management Services by serving not less than twenty (20) Working Days written notice upon the Supplier to such effect. The NTA shall be entitled to require the resumption of provision of Exit Management Services by serving not less than twenty (20) Working Days written notice upon the Supplier to such effect.
- 5.9 The NTA shall have the right to terminate its requirement for the Exit Management Services by serving not less than twenty (20) Working Days written notice upon the Supplier to such effect.
- 5.10 The Supplier, the NTA and the New Service Provider shall comply with all of their respective obligations in accordance with the provisions of the Exit Management Plan.

- 5.11 Subject to paragraph 5.3, the Exit Management Services to be provided by the Supplier may include such of the following services as the NTA may specify, solely to the extent that such services are reasonably required to facilitate the orderly transfer to the NTA or the New Service Provider:
- (a) ceasing implementation of all non-critical NTA Software changes (unless otherwise agreed by the parties);
 - (b) notifying the Supplier's sub-contractors of the procedures to be followed during the Exit Transition Period and providing management to ensure these procedures are followed;
 - (c) delivering the existing systems support profiles, monitoring or system logs, problem tracking/resolution documentation and status reports for the twelve (12) month period immediately prior to the commencement of the Exit Transition Period to the NTA;
 - (d) providing details of work volumes and staffing requirements over the twelve (12) month period immediately prior to the commencement of the Exit Transition Period;
 - (e) with respect to work in progress as at the end of the Exit Transition Period, documenting the current status and stabilising for continuity during transition;
 - (f) providing the NTA with any fault logs required under this Agreement which have not previously been provided to the NTA;
 - (g) reviewing all software libraries used in connection with the Services and providing details of these to the NTA or the New Service Provider;
 - (h) analysing and providing information about capacity and performance requirements, processor requirements and bandwidth requirements, and known planned requirements for capacity growth across these areas, for the twelve (12) month period immediately prior to the commencement of the Exit Transition Period;
 - (i) providing a list of the Software and components required for the provision of the Services in a form and on media reasonably requested by the NTA;
 - (j) agreeing a handover plan for all of the Supplier's responsibilities as set out in the Services Schedule with the NTA. The Supplier will co-operate fully in the execution of the agreed plan, providing skills and expertise of a suitable standard;
 - (k) all ICT Managed Services Materials, including those relating to the ICT Managed Services support systems;

-
- (l) delivering the administrative and service accounts' usernames and passwords operated by the Supplier (on behalf of the NTA) to the NTA;
 - (m) delivering copies of the databases (with content listings) to the NTA or the New Service Provider (on appropriate media) as reasonably requested by the NTA;
 - (n) providing reasonable assistance with the loading, testing and implementation of the databases;
 - (o) providing an information pack listing and describing the Services for use by the NTA in the procurement of the replacement Services; and,
 - (p) agreeing a suitable plan for the migration of any databases used for the performance of the Services (to the NTA or the New Service Provider) with the NTA or the New Service Provider. The Supplier will fully co-operate in the execution of the agreed plan, providing skills and expertise of a reasonably acceptable standard.
- 5.12 The NTA shall agree with the Supplier appropriate timeframes for delivery of the Exit and Service Transfer.
- 5.13 Except where legally required, the Supplier when processing the NTAs personal data will comply with data protection legislation and the NTA's data protection policies, in particular data retention, destruction and transfer.
- 6. Knowledge Transfer**
- 6.1 During the Exit Transition Period, the Supplier shall:
- (a) transfer all relevant training materials and provide reasonably appropriate training to the NTA or New Service Provider staff responsible for internal training, in connection with the provision of any replacement services; and
 - (b) provide for transfer to the NTA or the New Service Provider of all recorded knowledge reasonably required for the provision of any replacement services which may, as appropriate, include information, records and documents.
- 6.2 To facilitate the transfer of recorded knowledge from the Supplier to the NTA or the New Service Provider, the Supplier shall provide a detailed explanation of the procedures and operations used to provide the Services, the configuration management process and other standards and procedures to the operations personnel of the NTA or the New Service Provider.
- 6.3 The information which the Supplier shall provide to the NTA or the New Service Provider pursuant to paragraph 6.1 above will include:

- (a) copies of the NTA relevant Materials including up-to-date procedures and operations manuals;
- (b) product information;
- (c) information regarding any unresolved faults in progress at the commencement of the Exit Transition Period and those expected to be in progress at the end of the Exit Transition Period;
- (d) details of physical and logical security processes, tools and administrative accounts; and
- (e) any relevant design, architectural and system interface information.

7. **Assets, Sub-Contracts and Software**

7.1 Following notice of termination of this Agreement and during the Exit Transition Period, the Supplier shall not, without the NTA's prior written consent (not to be unreasonably withheld):

- (a) terminate, enter into or vary any sub-contract with any sub-contractor;
- (b) (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Assets or acquire any new Assets; or
- (c) terminate, enter into or vary any licence for NTA Software in connection with the Services, save as required under this Exit Management Schedule.

7.2 Within thirty (30) days of receipt of the up-to-date Registers from the Supplier, the NTA shall provide written notice to the Supplier setting out:

- (a) which Assets (if any) the NTA wishes to be transferred to the NTA or the New Service Provider; and
- (b) which sub-contracts the NTA wishes to be assigned or novated to the NTA or the New Service Provider (the "Transferring Contracts"),

in order for the NTA or the New Service Provider to provide any replacement services at the expiry of the Exit Transition Period.

7.3 Where requested by the NTA or the New Service Provider, the Supplier shall provide reasonable assistance to the NTA or the New Service Provider to enable them to determine which Assets and Transferring Contracts are required in order to provide any replacement services.

7.4 The Supplier shall assign, or procure the novation to the NTA, of the Transferring Contracts. The Supplier shall execute such documents and provide such other assistance as the NTA reasonably requires to effect this novation or assignment.

-
- 7.5 The Supplier shall assist with the transfer of the Managed Services support systems to a third party hosting service, including the following where relevant:
- (a) providing or consenting (as appropriate) to the transfer of the domain name and updating of the DNS and MX records to the new host;
 - (b) providing the source code for any customisations and all files and scripts used by any of the ICT Managed Services support systems;
 - (c) providing updated versions of all support system design, implementation and maintenance documentation;
 - (d) providing a full listing of the directory and file structures, folder and user permissions and naming conventions used by any support system;
 - (e) providing a copy of the server configuration for any support systems;
 - (f) providing an useable description of any database schemes; and
 - (g) exporting any database data in a format that facilitates the import of the data into a database on the third party hosting service provider.
- 7.6 The Supplier shall use reasonable endeavours to assist with the assignment or novation of all licenses in respect of Third Party Software licences (where possible) to the NTA or the New Service Provider.
- 7.7 The NTA shall:
- (a) accept assignments from the Supplier, or join with the Supplier in procuring a novation, of each Transferring Contract or procure that a New Service Provider does the same (as applicable); and
 - (b) carry out, perform and discharge all the obligations and liabilities created by or arising under that Transferring Contract, once it is novated or assigned to the NTA or the New Service Provider, and exercise its rights arising under that Transferring Contract or procure that a New Service Provider does the same (as applicable).
- 7.8 At the end of the Exit Transition Period (or earlier if this does not adversely affect the Supplier's performance of the Services, including the Exit Management Services, and its compliance with the other provisions of this Schedule):
- (a) the Supplier will return to the NTA such of the following as are in the Supplier's possession or control:
 - (i) all copies of the NTA Software and any other software licensed by the NTA to the Supplier under this Agreement;

-
- (ii) the Managed Services Materials including the training plan and any training materials, the operational manuals and procedures, system design and architecture documents, the latest Business Continuity and Disaster Recovery Plan and the security procedures;
 - (iii) any parts of the support systems and any other equipment which belongs to the NTA; and
 - (iv) any items that have been on-charged to the NTA, such as consumables;
 - (b) the Supplier will transfer all NTA Data upon request (in complete, uncorrupted form) in its possession or control to the NTA save to the extent (and for the limited period) that such NTA Data is required for the purposes of providing any services to the NTA under this Schedule or the Exit Management Plan; and
 - (c) each party will return to the other party all Confidential Information of the other party and will certify that it does not retain the other party's Confidential Information save to the extent (and for the limited period) that such Confidential Information needs to be retained by the party in question for the purposes of providing or receiving any Services or Exit Management Services.
- 7.9 Except where this Agreement provides otherwise, all licences, leases and authorisations granted by the NTA to the Supplier in relation to the Services shall be terminated with effect from the end of the Exit Transition Period.

8. Charges and Apportionments

- 8.1 All outgoings and expenses (including any remuneration due) and all rents, royalties and other periodical payments receivable in respect of the Assets and Transferring Contracts transferred to the NTA or the New Service Provider pursuant to paragraph 7 above shall be apportioned between the NTA and the Supplier or the New Service Provider and the Supplier (as applicable).
- 8.2 This apportionment shall be carried out as follows:
- (a) the payments shall be annualised and divided by three hundred and sixty five (365) to reach a daily rate;
 - (b) the NTA shall be responsible for, or shall procure that the New Service Provider shall be responsible for, or entitled to (as the case may be), the number of complete days remaining in respect of the relevant Asset and Transferring Contract following the transfer, multiplied by the daily rate; and
 - (c) the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

- 8.3 Each party shall pay, or the NTA shall procure that the New Service Provider shall pay, any monies due under paragraphs 8.1 or 8.2 as soon as reasonably practicable.

9. Payments

- 9.1 Any Exit Management Payments separate to the charges and apportionments described in paragraph 8 shall be payable to the Supplier in accordance with the relevant provisions of the Payments Schedule.

The NTA may provide an additional Exit Management Payment in the final year of the Term if the Exit Transition Period is extended beyond that contemplated by this Agreement.

SCHEDULE 7 – Data Processing Obligations

The following data processing obligations should be adhered to at all times:

The following data processing instructions should be adhered to at all times in respect of any personal data that the Supplier processes on behalf of the Authority:

1. The Supplier shall ensure that data is hosted either within EEA, or in a country deemed by the European Commission to provide an adequate level of protection for personal data.
2. The Supplier shall not copy production data to a test or development server without the approval of the Authority's Data Protection Officer and the Authority's security officer.
3. The Supplier shall not export data from the Authority's site or any of its data centres without the permission of the Authority's Data Protection Officer and Authority's Security Officer.
4. The Suppliers shall implement Authority's data retention policies or alternatively agree an appropriate policy with the Authority for the data being processed.
5. The Supplier shall adopt appropriate and agreed data protection procedures if copying data to a test server for maintenance / fault-finding purposes. Such procedures should be signed off by the Authority's Data Protection Officer and Authority's security officer each time data is copied.
6. The Supplier shall implement appropriate and agreed quality assurance processes to ensure accuracy of personal data processed on behalf of the Authority.
7. Where the Authority advises that consent is the basis for processing personal data, the Supplier shall implement consent capture / recording processes.
8. The Supplier shall have a physical document management process in place, and this process must be approved by the Authority.
 - The document management process shall ensure the synchronisation of physical and automatic data.
 - The document management process shall specify storage procedures for physical documents and scanned physical documents.
 - On request from the Authority, the Supplier shall provide 'proof of record' when shredding physical personal data.

-
9. The supplier shall ensure Data Protection scripts and recording processes used are compliant with Data Protection Law.
 10. The Supplier shall respond to subject access requests as requested by the Authority in line with the Data Protection Law timelines for response.
 11. On request of the Authority, the supplier shall partake in simulated data access requests exercises in order to test the subject access request process.
 12. The Supplier shall have user training processes in place to provide clear instructions on personal data processing. The Supplier shall carry out regular training on an on-going basis (at least annually).
 13. The Supplier shall ensure that appropriate security measures are in place to protect data at all times, and that the level of security is appropriate according to the sensitivity of the data.
 14. The Supplier shall regularly (minimum annually) demonstrate adherence to data protection instructions / policies / legislation. Evidence of adherence shall be provided to the Authority. This includes completion and return of the Authority's Data Processor Questionnaire.
 15. The Supplier shall ensure that appropriate internal confidentiality controls are in place to protect data.
 16. The Supplier shall maintain a written record of all personal data categories which it processes.
 17. The Supplier shall notify the data controller (the Authority) of a personal data breach as soon as they are aware of the incident.
 18. The Supplier shall inform the data controller (the Authority) should any of its requests breach Data Protection Law obligations or EU law.
 19. The Supplier shall seek written consent from the data controller (the Authority) prior to sub-contracting any work.
 20. In the event of sub-contracting any work, the Supplier shall ensure that their sub-contract adheres to each and every one of the instructions in this schedule.
 21. The Supplier shall maintain records of all processing activities and provide all necessary data to the data controller to demonstrate Data Protection Law compliance.

NATIONAL TRANSPORT AUTHORITY AGREEMENT FOR THE SUPPORT, MAINTENANCE, AND DEVELOPMENT OF
NTA DEDICATED SERVICENOW INSTANCES AGREEMENT

[•]

22. The Supplier shall implement appropriate privacy notices for any websites deployed on behalf of the Authority, that are both consistent with Articles 12 to 14 of the Data Protection Law, and agreed with the Authority.

[SUBJECT TO CONTRACT/CONTRACT DENIED]

Appendix A – Target Service Levels for KPIs

The following tables in this Section shall be used for determining the Target Service Level and KPIs against key Managed Services in the context of ServiceNow.

- The following table shall be used for determining the Incident resolution time in relation to Incident management (the “**Incident Resolution Time**”). Incident resolution means that the Incident has been fully resolved and there are no other tasks to be undertaken by the Supplier in relation to that Incident.

Table A.1 – Service Desk Incident Resolution Time (KPI)

Incident Priority Type	Target Response Time SLA	Target Resolution Time SLA	Target Service Level	Performance Points
P1 – Critical - Severity Level P1 - A core system is unavailable. - Customers/consumers unable to complete their transactions. - Mission critical functions affected. - P1 Security Incidents	1 hour	3 actual hours (not business hours)	>1 Incidents 1 Incidents	Red Amber
P2 – Medium - Severity Level P2 - A core system is partially unavailable / work around in place. - Business critical functions affected. - No major impact to customers/consumers - P2 Security Incident	4 hours	24 actual hours (not business hours)	>2 Incidents 2 Incidents	Red Amber
P3 – Low - Severity Level P3 - Certain non-core processes / required functions affected.	One (1) business day	Four (4) business days Call will be resolved within 4	<90% 91%-95%	Amber Yellow

[SUBJECT TO CONTRACT/CONTRACT DENIED]

- No impact to customers/consumers - Single user access issues.		business days. e.g., call raised at 16:00 day 1 will be resolved by same time 4 business days later)		
P4 – Information - Minor or cosmetic issues - Low impact system issues that are not mission critical. - No impact to customers/consumers	One (1) business day	Five (5) business days	<90% 91%-95%	Amber Yellow

2. The following table shall be used for determining the resolution time in relation to Service Desk Request Fulfilment (the “Service Desk Request Fulfilment Time”).

The ‘Response time’ – commences from time request is logged.

The ‘Resolution time’- commences from time request is logged through to completion.

The ‘time to respond to a call’ is the elapsed time from the time a call is logged for the service provider to contact the NTA and to begin work on fault resolution.

The Supplier will be expected to make all reasonable endeavours to resolve calls within the times set out in below. Failure to resolve calls within these times may be considered a breach of the Supplier’s obligations under the SLA.

It is expected that call response and resolution times will be agreed and identified within the Service Level Agreement. However, the following tables outline the NTA’s expectations in this regard.

The service provider must ensure that at all times there is appropriate resource cover to ensure delivery of agreed KPI’s and SLA’s of these requests.

Table A.2 – Service Desk Request Fulfilment Time (KPI)

Service Request Priority	Target Response Time SLA	Provision of Plan SLA	Target Resolution Time SLA	Target Service Level	Performance Points
P1 E.g. Access Request	4 hours	6 hours	One (1) business day	>2 Service Requests	Red

[SUBJECT TO CONTRACT/CONTRACT DENIED]

Add/ Remove user to groups Role addition / removal to groups - Add/Remove Service Accounts				2 Service Requests	Amber
				1 Service Request	Yellow
P2 - Report Creation / Report Modification - OOTB report requests. - Requests related CMDB Data Upload, Creating New / Modify Existing Cis	8 hours	12 hours	Two (2) business days	> 2 Service Requests	Red
				2 Service Requests	Amber
P3 Enhancement Requests including but not limited to - Minor Changes and modifications to Existing Catalogue Items - New Catalogue Item Creation - Minor Portal Changes and Enhancements OOTB - Form Level Changes	8 business hours	16 business hours	Seven (7) business days	<80% 81%-90% 91%-98%	Red Amber Yellow

[SUBJECT TO CONTRACT/CONTRACT DENIED]

(Minor Changes) • Addition of New Fields • Security Level Configurations (ACL) Minor Changes Only • Global Properties Modification • New SLA Creation • Existing SLA Modifications • New Email action Creation • Existing Email Modifications • New Business rules or scripting or Flows to meet Minor NTA Business requirements. • Notification Configuration and Maintenance • Scheduled Job Creation and Modification • Other Minor customisations and					
---	--	--	--	--	--

[SUBJECT TO CONTRACT/CONTRACT DENIED]

configuration Changes					
--------------------------	--	--	--	--	--

3. The following table shall be used for determining the severity scores in relation to Incident management (the “**Severity Score**”):

Table A.3 – Service Desk Incident Severity Scores

Factor number	Factor	Value	Score of Severity Calculation
1	Number of users affected	<1%	2
		1-10%	4
		>10%	6
2	Impact	Reduced performance/response time	1
		Intermittent	2
		System Fault	3
		System unavailable	6

3. The following table shall be used to determine the service level in relation to Customer Satisfaction (the “**Customer Satisfaction**”):

Table A.4 – Customer Satisfaction

Description	Target Service Level	Performance Points
Customer satisfaction score of service (based on resolution of tickets) higher than 80% (Monthly)	<70%	Amber
	71%-79%	Yellow
Customer satisfaction score from the VIP stakeholders higher than 90% (Bi-Annually)	<80%	Amber
	81%-89%	Yellow

[SUBJECT TO CONTRACT/CONTRACT DENIED]

4. The following table shall be used for determining the severity level in relation to Incident management (the “**Incident Severity Level**”):

Table A.5 – Service Desk Incident Severity levels

Sum of Severity Scores	Severity Level
>= 6	P1 - Critical
4 to 5	P2- Medium
3	P3 - Low
< 3	P4 - Informational

5. The following table shall be used for determining the service level in relation to System Availability (the “**Availability Management**”).

Table A.6 – System Availability - Core Service Hours

Environment	Core Service Hours
Production (24x7)	00:00 – 23:59 (24 hours)
User Acceptance Test	08:00 – 20:00 (12 hours)
Development	08:00 – 20:00 (12 hours)

Table A.7 – System Availability (KPI)

Description	Target Service Level	Performance Points
Availability target meet within core service hours	99.5% – 100.0%	N/A
Serious failure to meet system availability service level within core service hours	99.0% – 99.4%	Amber
Severe failure to meet system availability service level within core service hours	< 99.0%	Red

[SUBJECT TO CONTRACT/CONTRACT DENIED]

6. The following table shall be used to determine the service level in relation to Change Management (the “**Change Management**”).

Table A.8 – Change Management (KPI)

Description	Target Service Level	Performance Points
The number of non–authorised changes number shall not exceed zero (0).	Zero (0)	Red
The number of changes that failed compliance audit (e.g. approvals complete and changes completed as described and within the approved change window) shall not exceed zero (0).	Zero (0)	Amber
The number of failed production changes shall not exceed two (2).	Shall Not Exceed Two (2)	Amber
The number of Incidents traced to the production change and the reasons shall not exceed one (1).	Shall Not Exceed One (1)	Amber

The following table shall be used for determining the service level in relation to Access Management (the “**Access Management**”).

Table A.9 – Access Management (KPI)

Description	Target Service Level	Performance Points
The number of non–authorised access requests granted number shall not exceed one (1).	Shall Not Exceed One (1)	Red
The number of access permissions that failed compliance audit shall not exceed one (1).	Shall Not Exceed One (1)	Amber
The number of failed access requests removals shall not exceed one (1).	Shall Not Exceed One (1)	Red

[SUBJECT TO CONTRACT/CONTRACT DENIED]

4. The following table shall be used for determining the service level in relation to Utilisation and integration with Key NTA ICT Systems: (the “**Utilisation and integration with Key NTA ICT Systems**”).

Table A.10 – Utilisation and integration with Key NTA ICT Systems.

Description	Target Service Level	Performance Points
Integrity of integration – Amount of time that the integration connections and data synchronisation is happening as scheduled.	99%	Red
Integrity - Data in the system is accurate and trustworthy	95%	Amber
Utilisation – Percentage of incidents, requests, problems, knowledge base (KB) article, CMDB & Configuration Items (CI's) logged correctly in the NTA systems	95%	Red

7. The following table shall be used in relation to Vulnerability Management (the “**Vulnerability Severity Level**”).

Table A.11 – Vulnerability Severity Level (using Qualys definitions)

Vulnerability Level	Equivalent Qualys Rating	Definition
5	Urgent	Intruders can easily gain control of the host, or data which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors. -
4	Critical	Intruders can possibly gain control of the host or data, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host. -

[SUBJECT TO CONTRACT/CONTRACT DENIED]

3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities. Vulnerability allowing easy collection of information about the host

5. The following table shall be used for determining the resolution time in relation to Vulnerability Management (the “**Vulnerability Resolution Time**”). Vulnerability resolution time means the vulnerability has been fully resolved and there are no other tasks to be undertaken by the Supplier in relation to that vulnerability.

Table A.12 – Vulnerability Resolution Time (KPI) (after detection and fix / compensating control becomes available)

Trigger	Severity Level	ServiceNow Platform	Target Service Level	Performance Points
Internet Facing				
Emergency / Zero day vulnerability	1	Seven (7) Working Days	<95% 96%- 97% 98%- 99%	Red Amber Yellow
Vulnerability Level: 5		Seven (7) Working Days		
Vulnerability Level: 4		Seven (7) Working Days		

[SUBJECT TO CONTRACT/CONTRACT DENIED]

Vulnerability Level: 3	2	Fifteen (15) Working Days		
Vulnerability Level: 2	3	Ninety (90) Days	N/A	N/A
Vulnerability Level: 1	4	Ninety (90) Days	N/A	N/A

8. The following table shall be used in relation to Patch Management (the “**Patch Severity Level**”).

Table A.13 – Patch Severity Level

Patch Level	Equivalent Rating	Definition
4	Critical	Patches that resolve critical issues e.g. systems not functioning. Patches that address vulnerabilities which could be exploited to gain complete control over a system or cause significant damage. These should be applied immediately..
3	High	Patches that bring security enhancements and added functionality which is deemed high importance by the vendor and / or the NTA. Patches for vulnerabilities that could lead to significant security breaches but may require certain conditions to be exploited. These should be applied as soon as possible. eg a vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. These scenarios include common use scenarios where client is compromised with warnings or prompts regardless of the prompt's provenance, quality, or usability. Sequences of user actions that do not generate prompts or warnings are also covered.
2	Medium	Patches that bring security enhancements and added functionality which is deemed of medium importance by the vendor and / or the NTA. Patches for vulnerabilities that could potentially be exploited but are less likely to cause severe damage. These can be scheduled for regular

[SUBJECT TO CONTRACT/CONTRACT DENIED]

		patch cycles e.g.Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations.
1	Low	Patches that bring security enhancements and added functionality which is deemed of low importance by the vendor and / or the NTA. Patches for vulnerabilities that are unlikely to be exploited or cause minimal impact. These can be applied during routine maintenance e.g. Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.

[SUBJECT TO CONTRACT/CONTRACT DENIED]

6. The following table shall be used for determining the resolution time in relation to Patch Management (the “**Patching Resolution Time**”). Patching resolution time means the patching has been fully resolved and there are no other tasks to be undertaken by the Supplier in relation to that patching. This relates to patching bug fixes etc. Patching for vulnerabilities should use the table above (A11&12)

Table A.14 - Patching Resolution Times (KPI)

Trigger	Severity Level	ServiceNow Platform	Target Service Level	Performance Points
Internet Facing				
Emergency / Zero day Patches	1	Seven (7) Working Days	<95% 96%-97% 98%-99%	Red Amber Yellow
Scheduled release patches eg. Microsoft patches	2	Thirty (30) Days		
Deferred patches	3	Ninety (90) Days		

9. The following table shall be used for determining the service level resolution time in relation to Malware Defences Management (the “**Malware Defences Management**”).

Table A.15 – Malware Defences Management Time (KPI)

Item	Description	All Platforms	Target Service Level	Performance Points
Malware Defence Software/Platform Version N/N-1 (1 software version behind latest release)	Elapsed time to identify latest Malware Defence Software/Platform version, identify target population impacted and business risk associated with not applying the latest Malware Defence Software/Platform	≤ 10 business days	<90% 91%-95%	Red Amber

[SUBJECT TO CONTRACT/CONTRACT DENIED]

Malware Defence Signature Definitions 1 business day behind latest Signature Definitions	Elapsed time to deploy Malware Defence Signature Definitions to target population	≤ 1 business days	<97% 98%- 99%	Red Amber
--	---	------------------------	---------------------	--------------

7. The following definition shall be used for determining the Utilisation and Integration with Key NTA ICT Systems.
- Integrity of integration is that 99% of the time the integration connections will be happening, and that the data Sync is happening.
 - Integrity of Data is that 95% of the data in the system is accurate and trustworthy.
 - Utilisation is that all incidents, requests, problems, KB articles, CMDB / Cis are logged correctly in the NTA systems.
8. The following tables shall be used for determining the Mean Time to Detect, Mean Time to Respond and Mean Time to Resolve in relation to Security Event Management (the “**Security Event Management**”).
- Mean Time to Detect** a security event means the time taken between the event happening and the reporting notification being sent and/or ticket creation in the system whichever process is appropriate to the system.
- Mean Time to Respond** to a security event means the time taken to notify the relevant NTA Teams about the security event.
- Mean Time to Resolve** a security event means time taken to resolve the event on the impacted service and there are no other tasks to be undertaken by the Supplier in relation to that problem. Patching in this instance relates to patching bug fixes etc. Patching for vulnerabilities should use the table above (A11&12)

Table A.16 – Security Event Management Level (KPI)

Sev Code	Level	Criteria	Example (non-exhaustive)
S1	Critical:	Severe impact on business operations, such as complete system outages, major security breaches, or critical infrastructure failures.	Data breaches, ransomware attacks, denial of service (DoS) attacks. Elevated privileges gained by attackers, significant data loss, service degradation.

[SUBJECT TO CONTRACT/CONTRACT DENIED]

S2	High:	Significant impact on business operations, such as partial system disruptions or critical functionalities being affected.	Unusual data access, attempts to exploit Zero-day / unpatched vulnerabilities, detection of brute force attempts, Insider threat.
S3	Medium:	Moderate impact on business operations, such as non-critical feature malfunctions or minor security incidents.	Unauthorized access attempts, minor malware detections, policy violations.
S4	Low (informational):	Minimal impact on business operations, such as small inconveniences or minor issues that do not affect core functions.	System Alerts, Email messages removed after delivery, Engineering maintenance and Troubleshooting

Table B.17 - Security Event Detection, Response and Resolution Times (KPI)

Service Request Priority	Target Detection Time SLA (MTTD)	Target Response Time SLA (MTR)	Target Resolution Time SLA (MTTR)	Target Service Level	Performance Points
S1: Critical	Real-time < Thirty (30) seconds	15 mins (Phone)	60 mins (Phone)	<90% 91-95%	Red Amber
S2: High		30 mins (written report)	120 mins (summary report)		
S3: Medium		60 mins	480 mins		
S4: Low (Informational)		180 mins	1 Business Day		
		7 working days	7 working days		

[SUBJECT TO CONTRACT/CONTRACT DENIED]

Appendix B – Target Service Levels for PIs

The following tables in this Section shall be used for determining the Target Service Level and PIs against key Managed Services.

9. The following table shall be used for determining the resolution time in relation to Event Management (the “**Event Resolution Time**”). Event Resolution Time means the impacted service has been fully resolved and there are no other tasks to be undertaken by the Supplier in relation to that event.

Table B.1 – Event Resolution Time (KPI)

Event Severity Level	Target Resolution (Time)
P1 – Exceptional An exception means that a service is currently operating abnormally (however that has been defined). Typically, this means that a SLA has been breached and the business is being impacted. Exceptions could represent a total failure, impaired functionality or degraded performance. Examples of exceptions include: • system/application errors (including when a service or application is experiencing unplanned downtime) • Integration failure • System log errors related to code / script errors. • Platform health errors in system log table. • Any System logs that would indicate down time or malfunction of any critical business services within ServiceNow instances.	Four (4) hours
P2 - Warning A warning is an event that is generated when a service is approaching a threshold. Warnings are intended to notify the appropriate person, process or tool so that the situation can be checked and the appropriate action taken to prevent an exception. •	Twenty-Four (24) hours

10. The following table shall be used for determining the resolution time in relation to Problem Management (the “**Problem Resolution Time**”). Problem Resolution Time means the impacted service has been fully resolved and there are no other tasks to be undertaken by the Supplier in relation to that problem.

Table B.2 – Problem Resolution Times (KPI)

[SUBJECT TO CONTRACT/CONTRACT DENIED]

Problem Severity Level	Target Resolution (Time)
P1 Examples of P1 problems are: • Suspicion or detection of an unknown cause of one or more incidents by the Service Desk, resulting in a Problem Record being raised – the Service Desk may have resolved the incident through a workaround but has not determined a definitive cause and suspects that it is likely to reoccur, so the Service Desk will raise a Problem Record to allow the underlying cause to be resolved. • Alternatively, it may be immediately obvious from the outset that an incident, or incidents, has been caused by a major problem, so a Problem Record will be raised without delay. • Analysis of an incident by a technical support group which reveals that an underlying problem exists, or is likely to exist. • Automated detection of an infrastructure or application fault, using event/alert tools automatically to raise an incident which may reveal the need for a Problem Record.	Five (5) Working Day
P2 Examples of P2 problems are: • A notification from a supplier or contractor that a problem exists which needs to be resolved. • Analysis of incidents as part of proactive Problem Management – resulting in the need to raise a Problem Record to investigate the underlying fault further.	Thirty (30) Working Day
P3 Examples of P3 problems are: • A process is overly manual and would benefit from automation/process improvement or innovation to transform it.	Quarterly (and annually as part of Continuous Improvement and Innovation Plan)

[SUBJECT TO CONTRACT/CONTRACT DENIED]

Appendix C – Standard Reports

Ref.	Title	Description	Frequency
Service Desk Services			
SR01	Service Desk - Incident Management	Service Desk – Incident Management Report that includes: • Summary of number of incidents opened by severity • Incident response and resolution performance against SLA • Detail of P1 and P2 incidents • Details of incident type (user notified / automated alert) • Total number of open tickets by age. • • Trends of: ○ Incident tickets opened by severity for last 12 months ○ Incident response and resolution by severity for last 12 months	Monthly
SR02	Service Desk - Service Request Fulfilment	Service Desk – Service Request Fulfilment Report that includes: • Summary of number of service requests by priority opened this month • Total number of open incidents by severity • Total number of open tickets by age • Service request response and resolution performance against SLA • Trends of: ○ Service requests opened by priority for last 12 months ○ Service request response and resolution by severity for last 12 months	Monthly
SR03	Customer Satisfaction (CSAT)	• Customer satisfaction score of service (based on resolution of tickets) • Customer satisfaction score from the VIP stakeholders (bi-annual) • Details for unsatisfactory customer scores	Monthly

ICT Services Governance Services

[SUBJECT TO CONTRACT/CONTRACT DENIED]

SR04	Availability Management	Availability Management Report that includes: Percentage availability (uptime minus downtime as a % of the overall uptime allowed for, in any given period) of defined environments. Trend over the last 12 months	Monthly
SR05	Change Management	Change Management Report including: • Total number of changes by category (Standard, Normal, Emergency) • Number of Successful changes • Number of rolled back changes • Number of change related incidents • Number of unauthorised changes • Number of changes submitted to TAB for approval • Number of changes approved at TAB • Number of changes submitted to CAB for approval • Number of changes approved at CAB Trends for: • Number of changes by category • Number of Successful changes • Number of rolled back changes • Number of change related incidents	Monthly
SR06	Access Management	Access Management Report for all environments. User account transactions including: • Number of new user account requests • Number of user account changes • Number of accounts disabled • Number of user accounts deleted • Number of accounts with elevated permission changes Total number of active accounts including: • NTA users (normal accounts) • NTA users (administrator accounts) • Supplier Users (normal accounts) • Supplier Users (Administrator accounts) • Service Accounts • 3rd party users by party Trend of above over last 12 months	Monthly
SR07	Event Management	Delivery of filtered Event Management Report for operational and security events; • by Severity/Risk Magnitude • by Threat by Risk Category	Monthly

[SUBJECT TO CONTRACT/CONTRACT DENIED]

		- by Risk Decision (Accepted, to be Treated/Mitigated, etc.), - by Date Identified by environment.	
SR8	Problem Management	Problem Management Report showing changes to Problems for this month including new Problems identified and Problems successfully remediated categorised by Problem severity and age.	Monthly
SR9	Compliance Certification and Assurance	Compliance Certifications and Assurance Report, that contains relevant accreditations and regulatory assurance reports, including reports from key Supplier Suppliers containing: - any information security certifications such as ISO 2700X certifications; - any PCI compliance attestations such as any PCI Self-Assessment Questionnaires (SAQs), PCI Attestations of Compliance (AOC) reports or any Reports on Compliance (ROC) reports; - any NIS 2 compliance attestations; - any External Vulnerability Assessment on physical premises and ICT environments (including Cloud environments) used in the performance of the ICT Managed Services; - any Assurance Reports on Controls e.g. SOC2 or ISO 31000; - any Quality Reports certifications such as ISO 9000; - other Technical and Organisational measures (TOMS); - any assurance reports in compliance with EU AI Act	Annually
SR10	Risk Management	Risk Management Report and Risk Log. Risk report to reflect: - any risks or new risks that the Supplier has identified; - any risks that are becoming an issue and need to be resolved; - any risks that can be closed; and/or - any other amendments that the Supplier reasonably believes should be made to the risk log. - Summary of the risks showing the number by risk rating (RAG), number opened, closed or modified during the last month.	Monthly

[SUBJECT TO CONTRACT/CONTRACT DENIED]

SR11	License Compliance	Overall resource usage for Licenced resources e.g. applications / users Notification for pending expiry of a system/application license where the Supplier is directly responsible for and those that the Supplier is monitoring within the next three (3) months. The number of notifications of expiry of a system licence those where the Supplier is directly responsible for and those that the Supplier is monitoring within the last month. Number and details of uses of application exceeding available number of licenses within the past month.	Monthly
------	--------------------	--	---------

ICT Service Operations Services

SR12	System Health Check (RAG Report)	ServiceNow ISC System Health Check Report showing health and remediation actions for: • Security Compliance Status • Penetration Testing & Vulnerability Assurance • Platform Availability • Platform Health • Error Management • Backup & Recovery Assurance • Upgrade Readiness and Upgrade compliance. • Integration Health • ACL & Data Segregation Compliance • Security Incidents & Data Breaches • Disaster Recovery Testing Status • Licence & Subscription Compliance • Data Retention & Purge Compliance • Platform Performance Trends s).	Monthly
SR13	Malware Management	ServiceNow "Malware Management Report" to include: • Coverage and Currency information showing the version of malware defence software and currency of malware defence signatures/definitions across the NTA ServiceNow instances	Monthly

[SUBJECT TO CONTRACT/CONTRACT DENIED]

		- Malware Defence information; showing malware events identified and actions taken by Severity by Category by System/Host. - Malware Defence Remediation information showing; Environments with out-of-date software, signatures and definitions, and events or incidents raised as business risks.	
SR14	Patch Management	ServiceNow "Patch Management Report" that includes: - Missing patches by age, by Severity, by Environment - Patching Delta information showing patching level changes for the preceding month including new patches identified, patches successfully deployed, patches not deployed, patches raised as incidents by environment. - Patch Resolution Time compliance by severity level and interface - Patching exceptions (risk accepted)	Monthly
SR15	Vulnerability Management	ServiceNow "Vulnerability Management Report" that includes: - Vulnerabilities - by Severity - by Category - by Release Date - by Date Identified - by environment; - Details of vulnerability changes for the preceding month including new vulnerabilities identified, vulnerabilities successfully remediated, vulnerabilities not remediated, vulnerabilities raised as business risks by environment; - Vulnerability Resolution Time compliance by Severity level; - Vulnerability exceptions (risk accepted / not patchable) and - Open vulnerabilities by age.	Monthly

Security Monitoring Operations Services

[SUBJECT TO CONTRACT/CONTRACT DENIED]

SR16	Security Operations Monthly	Monthly ServiceNow Security Health Report, detailing: • Instance Security Center (ISC) Compliance Score of 90% and over • Summary of Data Export anomalies.	Monthly
SR17	Security Operations Weekly	Weekly Security Operations Reports including: • Number of incidents/ offences detected & closed showing true or false positives and criticality. • Summary of new threat intelligence received, and relevant threats identified, • Licence and EPS used summary. • List of new assets onboarded and decommissioned from QRadar • Overview of fine tuning and use case creation and optimisation requests and status in previous week.	Weekly
SR18	Security Monitoring	Security Monitoring Report to include: • Incidents/Offences currently open referencing appropriate details e.g. Status, Severity, Details, Priority, Date Opened and age, • Incidents / offences closed in the past 24 hours	Daily
SR19	Security Improvement Roadmap	Provision of on-going and timely advice, guidance and innovation including • Evaluation of current security posture (infrastructure, applications, processes) • Overview on key risks and remediation efforts • Suggestions for potential security posture improvements • Initiatives planned and timelines for implementation.	Quarterly

Data Protection

SR20	Data Protection	Data Protection Report including the following • Number of instances where the Supplier became aware of the accidental or unlawful destruction, loss, alteration, unauthorised	Monthly
------	-----------------	---	---------

[SUBJECT TO CONTRACT/CONTRACT DENIED]

		disclosure of, or access to data, including personal data, transmitted, stored or otherwise processed by the Supplier or its sub-processors. Number of subject access requests compiled, processed (any requests to update or delete (if applicable) a Customer's personal data) and provided to the NTA.	
--	--	--	--

Governance Reports

SR21	Privacy Impact Assessment	Template supplied by NTA for all systems which hold NTA data to ensure that adherence to the NTA Governance process and GDPR is confirmed.	Annual
SR22	Technical and Organisational Measures (TOMS)	Template supplied by the NTA to ensure GDPR elements at the supplier (and sub-suppliers) adhere to the NTA Governance process for GDPR.	Annual
SR23	Supplier / ServiceNow Cyber Response Plan	Detailed response plan that is activated in the event of a Malware (e.g. ransomware) event in the supplier environment, or the ServiceNow environment to enable the isolation from NTA systems (including a kill switch process) and protection of NTA data	Annual
SR24	AI Impact Assessment	Template supplied by NTA for all systems which have AI elements to ensure that adherence to the NTA Governance process and the EU AI Act is confirmed.	Annual
SR25	Risk Register and Management	Risk register showing risks identified by the supplier and the NTA and actions relating to those risks	Monthly
SR26	Exit Management Plan	As defined in Schedule 6	Annual
SR27	Supplier / ServiceNow DR / BC test results	Confirmation that an annual Disaster Recovery and or Business Continuity test has been completed and high-level results / report on degree of success.	Annual

[SUBJECT TO CONTRACT/CONTRACT DENIED]

Appendix D – Milestone Certification Procedure

1. Introduction

- 1.1. The Operator is required to certify the Milestones in accordance with the following certification procedure (the “**Certification Procedure**”).

2. Certification Procedure

- 2.1. The Operator shall develop and agree with the NTA the form of each Certificate relevant to each Milestone.
- 2.2. Each Certificate issued shall be provided by the Operator in digital format, signed by the Operator.
- 2.3. The effective date for Certificates issued under the Certification Procedure shall be the date upon which when such Certificates have been returned as Acknowledged by the NTA.
- 2.4. The Operator shall provide to the NTA, and maintain throughout the Term, a register recording the current status of all Certificates.
- 2.5. Following counter signature by the NTA, a copy of each Certificate shall be retained by both the NTA and the Operator.

3. Operation of the Certification Procedure

- 3.1. In respect of each Milestone, the Operator shall provide a certificate to the NTA certifying that it has completed the documents, activities or deliverables to which the particular Milestone relates in accordance with this Agreement or as otherwise specified by the NTA (each a “Certificate”).
- 3.2. On receipt of a Certificate from the Operator, the NTA shall return the Certificate signed by the NTA with one of the following responses:
 - (a) “**Acknowledged**”, on the basis that there is no objection to the Certificate and supporting documentation supplied to the NTA;
 - (b) “**Acknowledged with Comments**”, on the basis that the NTA has comments on the Certificate or supporting documentation supplied to the NTA which shall be supplied to the Operator; or
 - (c) “**Rejected**”, on the basis that the NTA does not accept the Certificate or supporting documentation supplied to the NTA and full details of the reasons for such rejection shall be supplied to the Operator.
- 3.3. In the event that a Certificate is returned as Acknowledged with Comments or Rejected by the NTA, the Operator shall amend the Certificate or supporting documentation in accordance with the comments or reasons for rejection provided by the NTA and continue to re-submit amended Certificates in

[SUBJECT TO CONTRACT/CONTRACT DENIED]

accordance with the Certification Procedure, until the NTA returns the Certificate as Acknowledged.

3.4. The Operator shall submit any further information relating to the Service as may be considered by the NTA as necessary in connection with a Certificate.

3.5. Digital copies of the relevant supporting documentation including designs, results or reports, shall be issued with each Certificate.

4. Index of Certificates and Permits

4.1. The Operator shall submit each of the following Milestone Certificates:

- (a) Milestone One: (*Delivery of Plans & Design Completion*) Certificate;
- (b) Milestone Two: (*Service and Technical Readiness*) Certificate;
- (c) Milestone Three: (*Operational Readiness*) Certificate;
- (d) Milestone Four: (Operational Services Start) and
- (e) Milestone Five: (Completion of Transition Services) Certificate;

(together, the “**Milestone Certificates**”).

5. Milestone Certificates

5.1. The Operator shall submit a Milestone Certificate in respect of each Milestone (along with any necessary supporting documentation), certifying that the activities required for the completion of the relevant Milestone as set out in this Schedule, have been successfully achieved.

5.2. Subject to the provisions of section 6 of this Appendix, where a Milestone Certificate has not been returned signed as Acknowledged by the NTA, the Operator may continue with the activities required under the following Milestone solely at its own risk (unless otherwise agreed in writing with the NTA).

6. Operating Permit

6.1. The NTA shall, subject to the satisfaction of the requirements set out in this section, issue permit allowing the Operator to commence the provision of the Operational Services (the “**Operating Permit**”).

6.2. Once the Milestone Certificate submitted in respect of Milestone Five is returned by the NTA signed as Acknowledged or Acknowledged with Comments, the Operator may apply to the NTA for an Operating Permit including: (i) an outline of the Operator’s proposed Operational Services Start Date; and (ii) the Operator’s plan to establish and implement the activities which are required to commence the Operational Services, without having any impact on the services provided by the Outgoing Service Providers.

6.3. If the NTA is satisfied with the Operator’s plan for commencement of the Operational Services, it may issue an Operating Permit to the Operator setting out the Operational Services Start Date.

6.4. Within five (5) Working Days of receipt of the Operating Permit from the NTA, the Operator shall acknowledge receipt by returning a copy of the Operating Permit in digital format signed by the Operator Representative.

[SUBJECT TO CONTRACT/CONTRACT DENIED]

6.5. Paragraphs 6.1-6.3 of this Appendix above and the issue of the Operating Permit by the NTA shall be without prejudice to the Operator's obligations to ensure that all operational, technical and procedural issues identified by the NTA prior to or following the Operational Services Start Date are dealt with to the satisfaction of the NTA.

[SUBJECT TO CONTRACT/CONTRACT DENIED]

Appendix E – Current NTA ServiceNow Architecture

NTA ServiceNow Architecture

