



3rd Party Information Security Policy

Version Control

Version	Date	Owner	Comments
1.0	15/09/2017	Bruce Hopkins	1 st release – customised for specific project
1.1	13/10/2017	Bruce Hopkins	Updated for general release
1.2	31/01/2018	Bruce Hopkins	Data Handling Requirements section added
1.3	05/02/2018	Bruce Hopkins	Amendments from Legal included
1.4	17/01/2022	Bruce Hopkins	Minor updates to align to current policy
1.5	01/06/2023	Bruce Hopkins	Minor updates to align to current policy

Approval

Date	Approved by	Comments
01/06/2023	Bruce Hopkins	

Table of Contents

1. Introduction.....	3
1.1. Purpose & Scope	3
2. Policy Compliance Requirements	3
2.1. Requirement for a Formal Agreement	3
2.2. Implementation & Compliance	3
2.3. Infrastructure, Systems & Coding	3
2.4. Incident Response & Reporting	3
2.5. Breaches of Policy	4
3. General User Security & Awareness Policy	4
3.1. Security Awareness Communications	4
3.2. Confidentiality.....	4
3.3. Internet User Policy	4
3.4. Laptop & Portable Devices.....	4
3.5. E-mail & Teams Usage Policy	5
4. Data Security & Handling Policy	5
4.1. Data Handling Requirements	5
4.2. Data Classification – Sensitive Data	5
4.3. Data Retention – Data Protection Act	6
4.4. Data Privatisation / De-Personalisation.....	6
4.5. Data Encryption.....	6
4.6. Data Disposal & Media Destruction.....	6
5. User Access Management	7
5.1. Systems Support & Administration.....	7
5.2. General User Account Policy	7
5.3. Generic or Service Accounts (inc. System Administrators)	7
6. Network Security Policy.....	7
6.1. Network Design / 3 rd Party Connectivity	7
6.2. Remote Access to daa Networks	8
7. New IT System or Service Policy.....	8
7.1. Project Management / Service Delivery Requirements	8
7.2. Systems Design & Deployment.....	8
7.3. Top 10 Security Design Principles	8
8. Systems Administration.....	9
8.1. Malicious Software Prevention	9
8.2. Internet Services Protection	9
8.3. Vulnerability & Patch Management	10
8.4. Backup Security Policy.....	10
9. Physical Security of IT Facilities & Equipment	10
9.1. General Site Security Requirements	10
9.2. IT Facilities Security Requirements.....	10

1. Introduction

1.1. Purpose & Scope

- 1.1.1. The purpose of this policy is to ensure that all 3rd party suppliers of services to daa are made aware of daa's IT Security requirements.
- 1.1.2. This policy may be provided to 3rd parties with access to daa data, information or systems, or to 3rd parties that are tendering for the provision of products or services that may involve access to daa data, information or systems, and that are subject to Non-Disclosure Agreement.
- 1.1.3. This policy is applicable to all daa systems and data, including
 - All infrastructure, operating systems, databases or applications that are owned by daa, including systems that may be hosted or housed by a 3rd party
 - All data provided to a 3rd party or made available to a 3rd party by daa.

2. Policy Compliance Requirements

2.1. Requirement for a Formal Agreement

- 2.1.1. A formal contractual agreement must exist between daa & 3rd party organisations before any access to data or systems (including, but not limited to, remote access) is granted.
- 2.1.2. All 3rd parties given access to daa systems or data must be approved suppliers as per daa IT Security and/or Procurement procedures.
- 2.1.3. Any changes to this policy to allow for supplier specific deviations must be approved by IT Security and recorded in the contractual agreement with the supplier.

2.2. Implementation & Compliance

- 2.2.1. All 3rd parties with access to daa information or systems must implement security policies & procedures to ensure that they comply with the requirements of this policy document.
- 2.2.2. daa reserves the right to review systems to ensure compliance with this policy via reasonable access to knowledgeable personnel to discuss the controls in place.
- 2.2.3. Where required as part of the service, the 3rd party shall be able to demonstrate compliance throughout the term of the agreement by providing independent assurance, such as via ISO27001 certification.

2.3. Infrastructure, Systems & Coding

- 2.3.1. All systems must be security tested or checked for compliance against a defined set of rigorous security standards and practices. These should include current good practices such as the Open Web Application Security Project (OWASP) Top 10 Web Application Vulnerabilities.
- 2.3.2. All systems shall be securely hardened and maintained as per industry standards and/or vendor guidance. Any identified non-compliances must be addressed in a timely manner.

2.4. Incident Response & Reporting

- 2.4.1. All 3rd parties must have documented Security Incident Response and Data Breach procedures in place.
- 2.4.2. These procedures must include ownership of incidents, and clear escalation and incident response steps, including a commitment to promptly notify daa of any actual unauthorised disclosure of Personal Data, as required under Data Protection law.
- 2.4.3. Any security incidents that may impact daa, such as the theft of daa equipment or data, or unauthorised access, must be reported to daa IT Security in a timely manner.
- 2.4.4. Where the incident may involve criminal or serious policy breach, all data or documents should be preserved intact and not modified – this is necessary to facilitate proper investigation. This may include, but is not limited to, computer files, log files, paperwork, computer hardware, CCTV tapes, backup tapes or other media.

2.5. Breaches of Policy

2.5.1. In the case of 3rd party users of daa systems, violation of policy may be regarded as a breach of contract by the 3rd party. Suspicion of illegal activity will be reported to the appropriate authorities for investigation. All users are obliged to disclose to daa Management any activity that they become aware of that may involve, when using daa-owned systems and networks:

- Any criminal activity or improper conduct involving daa data, or breach of confidentiality
- Failure to comply with a legal obligation which may result in liability or damage to daa's reputation
- Financial malpractice, money laundering, corruption or fraud involving daa systems or data
- Any attempt to conceal any of the above.

3. General User Security & Awareness Policy

3.1. Security Awareness Communications

3.1.1. 3rd Party users must be made aware of the security policy requirements of working with daa systems or information. Awareness should be performed in a structured and ongoing manner.

3.1.2. Awareness training must be provided to all users that have access to daa systems. Training must be provided on a periodic basis and training records maintained.

3.2. Confidentiality

3.2.1. All daa contractors or 3rd parties working on daa systems or data must be aware that use of daa information systems may be subject to monitoring. daa reserves the right to review use of our systems to ensure compliance with policy, regulatory & legal requirements.

3.2.2. daa contractors or 3rd parties must hold in strict confidence and not disclose to other 3rd parties any and all information disclosed to them or created by them during the period working on daa systems or data.

3.2.3. daa contractors or 3rd parties must not make copies of any confidential information except as authorised by daa. In addition, all confidential information in their possession or control (paper, electronic or any other format) must be returned to daa upon termination of the contract or service, or where requested.

3.2.4. daa contractors or 3rd parties must not remove any documents which contain any confidential information or tangible items which belong to daa or any 3rd parties from daa's premises without prior authorisation by an appropriate daa manager.

3.2.5. daa contractors or 3rd parties must not use any proprietary or confidential information of any former employer or other 3rd party in breach on any previous confidentiality agreement.

3.3. Internet User Policy

3.3.1. daa contractors or 3rd parties accessing the Internet via daa systems or using daa equipment should be aware that Internet browsing is subject to monitoring. daa reserves the right to review Internet browsing to ensure compliance with policy, regulatory & legal requirements.

3.3.2. Access to web sites containing illegal or inappropriate content is prohibited. Inappropriate material includes potentially illegal, defamatory, abusive, obscene, profane, racist, sectarian or pornographic words, pictures, or any materials which may cause offence or annoyance to any reasonable person.

3.3.3. Violation of copyright is prohibited – 3rd parties are expected to ensure that they read & comply with any copyright notices on any materials used.

3.3.4. Posting to social media websites, bulletin boards or discussion websites / forums in the name of daa or purporting to represent the views of daa is prohibited unless specifically authorised to do so.

3.3.5. Posting to websites or discussion forums in a manner that may disparage daa policies, services or personnel or that is likely to bring the name of daa into disrepute, is prohibited.

3.4. Laptop & Portable Devices

3.4.1. daa contractors & 3rd parties using portable devices such as laptops, tablets, smartphones, or USB memory sticks containing daa information must take steps to protect the security of daa data.

3.4.2. daa contractors & 3rd parties using portable devices must adhere to the following:

- Copying sensitive data (as defined below) onto a laptop, tablet, smartphone or portable disk is prohibited unless the data is encrypted.
- Copying or uploading daa corporate or customer data to a consumer cloud app or other unauthorised cloud service such as WeTransfer is prohibited.
- Leaving daa laptops or portable devices unattended or insecurely stored is prohibited.
- Laptops, CDs, USB keys, reports or other portable materials may only be brought outside the 3rd party approved working areas for authorised business purposes.

3.5. E-mail & Teams Usage Policy

3.5.1. daa contractors & 3rd parties granted access to daa e-mail or messaging applications (Teams or similar applications) are obliged to use the services in a responsible and lawful manner.

3.5.2. The content of all e-mails and messages sent via daa's mail platform is the property of daa. daa reserves the right to review the contents of e-mails and messages to ensure compliance with policy, regulatory & legal requirements.

3.5.3. daa contractors & 3rd parties must not use e-mail or messaging applications for the transmission or distribution of inappropriate materials. Inappropriate material includes pornographic, defamatory, abusive, obscene, profane, racist, sectarian or illegal words, pictures or any materials which may cause offence to any reasonable person.

3.5.4. daa contractors & 3rd parties must not use free e-mail or messaging applications systems like Gmail for daa business purposes or set up auto-forwarding of e-mail from daa systems to external systems.

4. Data Security & Handling Policy

4.1. Data Handling Requirements

4.1.1. All daa's corporate, personnel and customer data or information must be treated as confidential and handled appropriately. daa contractors & 3rd parties must follow defined data handling policies and procedures that are appropriate to the sensitivity of the data.

4.1.2. All 3rd parties acting on behalf of daa are expected to exercise caution and due diligence in their delivery of services to daa that involve the processing or storage of daa data or information, in any form, including printed report, USB stick, hard-drive, PC, laptop, server, database, or cloud storage system.

4.1.3. Where daa data or information will be processed or stored on IT systems managed or owned by the 3rd party, or by agents acting on their behalf, appropriate access controls must be in place, including but not limited to, an authorised username & password.

4.1.4. All daa's corporate, personal, or data or information must be secured in access-controlled areas (i.e. offices or other areas accessed using an access code, swipe card, or other access control system).

4.1.5. Where daa information is transferred outside access-controlled areas (whether on device, disk, or in printed form), the information must be transferred via secure channels using established procedures.

4.1.6. daa data or information must never be left unattended in public areas and must be secured in an appropriate container if left unattended in a vehicle at any time.

4.2. Data Classification – Sensitive Data

4.2.1. daa's corporate, personnel and customer data is a critical asset and must be protected. For the purposes of this policy, we define 'sensitive data' as including, but not limited to:

- Personal data provided to daa by an employee, customer, or passenger that is defined as sensitive under General Data Protection Regulations.
- Financial details related to daa, a customer, employee, passenger, or another company, including bank account or credit card numbers, pricing or payment data.
- Regulatory, law enforcement or any operational policies or procedures related to airport operations or security-sensitive areas of our business.
- Technical designs, project plans, or systems / service configuration or management documentation that may be used to circumvent security controls.

- Maps, diagrams, procedures or plans describing daa emergency response, access control or related procedures.

4.2.2. Where systems store sensitive data, additional security steps must be taken – these may include:

- Encryption of the data in transit using transport layer security
- Encryption of the data at rest using bulk / disk level encryption and / or file-level encryption
- Use of access controls to limit access to specified individuals or teams
- Use of multi-factor authentication (MFA) to access the data
- Preventing the data from being displayed on screen
- Logging all attempts to read or access the data.

4.3. Data Retention – Data Protection Act

- 4.3.1. All system owners, data owners, or systems administrators are responsible for ensuring that the servers, computers, databases or other systems / devices are managed in accordance with the Data Protection Acts and GDPR.
- 4.3.2. All system owners, data owners, or systems administrators are responsible for ensuring that retention policies are defined and implemented for any personal data.

4.4. Data Privatisation / De-Personalisation

- 4.4.1. For the purposes of this policy, the terms 'privatisation' or de-personalisation means the removal of any personal data from a database or file in order to keep it confidential.
- 4.4.2. Data must not be transferred or copied from a production system or network to a Test or Development system or network unless sensitive details are removed or masked prior to transfer.
- 4.4.3. The only exceptions to this policy are daa-approved 3rd parties with the relevant data-specific contracts or other agreements in place (such as data processing agreements).
- 4.4.4. Data privatisation processes must remove or mask data fields prior to being transferred or copied from a production system unless the data have been specifically identified by daa as exempt from privatisation.

4.5. Data Encryption

- 4.5.1. All sensitive data must be encrypted if stored on any portable device (e.g. USB key or CD), or in transit (e.g. via e-mail, post or courier, or if transmitted across the Internet in any way).
- 4.5.2. Where password-based encryption is used, the password must never be transmitted in the same way as the encrypted file (e.g. if the file is e-mailed, the password should not be e-mailed).
- 4.5.3. Where encryption must be used, strong cryptography and robust procedures must be used, as set out by current industry standards / best practices.

4.6. Data Disposal & Media Destruction

- 4.6.1. All 3rd party teams must ensure that appropriate destruction / disposal procedures are implemented over any systems that process or store daa data. All systems must be managed in accordance with the requirements of the most sensitive data stored in the system.
- 4.6.2. All redundant, retired or end-of-life disks or media must be disposed of in a secure manner by the authorised team in the relevant daa or 3rd party site. This includes:
- All server drives, SAN drives, PC drives, or laptop drives
 - All magnetic tapes or optical drive arrays used for backups
 - All CDs, DVDs, USB drives or other devices used to transport files or data.
- 4.6.3. The authorised site management team in the relevant daa or 3rd party site must either securely wipe all data, or physically destroy the media prior to disposal of the equipment housing the data.
- 4.6.4. Sensitive data must be deleted or destroyed as soon as possible when no longer required. Data should only be retained in where a specific requirement has been identified and agreed with an authorised daa representative via an appropriate formal contractual agreement.

5. User Access Management

5.1. Systems Support & Administration

- 5.1.1. All 3rd party personnel with access to any systems that process or store daa data must ensure that appropriate user access procedures are implemented. Access procedures must include segregation of duties between development, test & operations.
- 5.1.2. All 3rd parties with access to any systems that process or store daa data must ensure that appropriate user awareness training is provided to all their personnel that have access to daa systems. Training must be provided on a periodic basis and training records maintained.
- 5.1.3. All accounts should be locked / disabled on the departure of the user. A lapsed / unused account review must be performed every 3 months and any accounts unused for 90 days or more must be disabled.
- 5.1.4. An up-to-date list of the accounts on a system must be maintained – this must contain an auditable record of the account authorisation i.e. who approved/authorised the access.
- 5.1.5. Account passwords must be encrypted while being stored on computer or transmitted over the network. Password lists should never be stored in an unsecured format.

5.2. General User Account Policy

- 5.2.1. Individual users, and, in the case of 3rd parties, their organisations, are accountable for all actions undertaken using their user login accounts. Systems and data must only be accessible via a login account assigned to a specific user. Users may not use another person's password or user account.
- 5.2.2. Users must not leave a computer unattended while logged into a daa system – unattended servers or clients must always be locked to prevent misuse of the logged in account.
- 5.2.3. All user account passwords must require a strong password of 8 or more characters that contains a mix of lower-case letters, upper case letters, numbers & symbols.
- 5.2.4. Password reset procedures must include confirmation of the user's identity and forced change of password following reset.
- 5.2.5. Accounts should automatically lock after a maximum of 5 failed login attempts. All operating system login attempt failures must be logged.
- 5.2.6. The password must be changed after a maximum of 90 days from last change. Users should be prevented from reusing their last 3 passwords or from changing their passwords several times in 1 day.

5.3. Generic or Service Accounts (inc. System Administrators)

- 5.3.1. Any account that is not assigned to a named user for their sole use is called a 'generic account'. A service account is a generic account that is intended for use by a service, not by users or administrators.
- 5.3.2. Where generic or shared accounts are in use, the 3rd party must maintain records of account assignment to specific persons.
- 5.3.3. Shared generic accounts may be used for 3rd Line Support provided that such accounts are approved by the relevant daa system / business owner.

6. Network Security Policy

6.1. Network Design / 3rd Party Connectivity

- 6.1.1. All personnel involved in designing, implementing, or managing daa networks must ensure that appropriate procedures are implemented to comply with this policy.
- 6.1.2. All activities relating to designing or implementing connections between 3rd party networks and daa networks must consult with, and have formal approval from, the daa IT Security team.
- 6.1.3. All connections between daa networks and 3rd party networks must be protected by appropriate security controls, including, but not limited to:
 - Encryption of data in transit – data moving between systems to be encrypted (e.g. by a VPN).

- Stateful firewalls that deny services not explicitly permitted.
 - Application of security hardening standards (e.g. anti-virus software, security patching etc).
 - Compliance with accepted security practices such as ISO27001.
- 6.1.4. Changes to network infrastructure or configuration must be subject to change management procedures. All network designs and configuration must be documented and maintained.

6.2. Remote Access to daa Networks

- 6.2.1. Multi Factor Authentication (MFA) must be used when gaining access to daa systems or data to support applications or infrastructure (e.g. via SecureID fob, Microsoft MFA or similar).
- 6.2.2. Accounts must not be shared unless approved by daa (e.g. for 3rd Line Support purposes).
- 6.2.3. All users should be aware that remote access to daa corporate systems is subject to monitoring. daa reserves the right to review access to ensure compliance with policy, regulatory & legal requirements.

7. New IT System or Service Policy

7.1. Project Management / Service Delivery Requirements

- 7.1.1. All 3rd parties involved in managing or delivering projects must ensure that appropriate security measures are implemented. This should form part of the formal contractual agreement that will exist between daa & the relevant 3rd parties.
- 7.1.2. All system or service specifications, including responses to procurement processes must comply with daa's IT Security policy requirements, including the policies set out in this document. This must be factored into the costs and cannot be deemed an 'optional extra' or change request.
- 7.1.3. All deployment specifications must include security principles & procedures – the network location, security zone & hardening requirements must be specified.

7.2. Systems Design & Deployment

- 7.2.1. All new IT Systems and supporting services must be implemented via a formal project that has been approved by the responsible daa Department and assessed by IT Security prior to implementation.
- 7.2.2. All systems or services to be deployed, including those deployed as managed services or cloud-based services, must conform to daa IT Security requirements and be risk assessed as part of the deployment process – this includes hosted services, websites, Infrastructure as a Service (IaaS), Software as a Service (SaaS) etc that may be branded as daa or may process or store daa data.
- 7.2.3. All systems and equipment deployed on behalf of daa must be housed & stored in secure facilities protected by appropriate procedures and access controls.
- 7.2.4. All operating systems, databases or applications must conform to appropriate security hardening standards, in accordance with current industry best practice.
- 7.2.5. Where personal or sensitive data must be migrated, transferred or copied to a test or development system, production-level controls must be implemented prior to data migration or transfer.

7.3. Top 10 Security Design Principles

- 7.3.1. All design & deployment specifications must include security principles & procedures – the network location & hardening requirements must be specified in the design – specifications must adhere to our **Top 10 Security Design Principles** as follows:
1. **All systems must facilitate unique logins for all users and administrators.** Using a service account to perform all application functions is not permitted – it prevents activity logging & implementation of user access management procedures.
 2. **Multi-Factor Authentication (MFA) is mandatory for access to personal or sensitive data from outside the daa corporate network.** While MFA is recommended for all user accounts, Multi-Factor Authentication is mandatory on user accounts for
 - Access to personal information or sensitive corporate data from outside the daa network.

- Privileged access for systems administration or support from outside the network.
- 3. **Single Sign On – application user accounts should be integrated with Active Directory** where possible – this means that password and users controls can be managed centrally by IT. Where not possible, formal user access management procedures must be in place, including Joiners, Movers, Leavers etc.
- 4. Where systems provide access to sensitive data, appropriate data security must be implemented – especially where provided via untrusted networks – these controls should include:
 - **Encryption of data in transit** – data moving between systems on external or untrusted networks must be encrypted (trusted networks must be limited to localised network segments).
 - **Encryption of data at rest** – sensitive data (Class C2 or above) needs to be encrypted while stored. All data must be encrypted if hosted in 3rd party / cloud solutions.
 - **Logical access controls** – limit access to specific users or groups via the principle of least privilege (such as RBAC, Role Based Access Controls).
 - **IP-based segregation of systems and networks** – segregate systems into functional architecture layers (infrastructure, data storage, applications) and limit system access to trusted / internal networks based on an appropriate network zoning model.
 - **Use of certificate-based access** – limit access to authorised / managed devices.
- 5. **Software build standards must be applied to operating systems and applications**, including
 - Default accounts must be secured (deleted, locked, or have their name and password changed) and service accounts must be configured to prevent user login.
 - Services & packages should be enabled only as required – all non-essential services must be disabled with only security-approved services used.
- 6. **All applications must feature logging of security events** such as failed logins, changes to key settings or configuration, and access to critical data – event data must be available for collection by daa's Security Operations Centre for monitoring.
- 7. **Segregation of duties must be implemented** as far as possible between functional architecture layers (infrastructure, data storage, applications) and between development, test & operations.
- 8. **Source code should be built securely** to avoid security vulnerabilities in custom code – guidelines such as OWASP should be applied.
- 9. All **payment card or similar financial data must be segregated** and/or subject to additional controls – current policy is not to store payment data on daa systems.
- 10. **Cyber Resilience – all services deemed critical to airport operations must be operable in the event of loss of Internet connectivity** (e.g. due to a cyber-attack).

8. Systems Administration

8.1. Malicious Software Prevention

- 8.1.1. Anti-malware software must be installed on all systems that connect to daa networks or that host daa data. Anti-malware software must be automatically updated to ensure protection from the latest threats.
- 8.1.2. Internet gateways (e.g. e-mail and web proxy servers) must have appropriate anti-malware software, configured to be updated automatically.

8.2. Internet Services Protection

- 8.2.1. All Internet-facing services must be protected by robust protection against current known Internet threats. This includes web sites, web-based applications, hosted services, Infrastructure as a Service (IaaS), Software as a Service (SaaS) etc that may be branded as daa or may process or store daa customer or corporate data.
- 8.2.2. Internet-facing service protection for websites, web apps and other 'cloud' services must provide protection technologies as specified by daa including some or all of the following:
 - Malware, Spyware, and Bot Net Blocking
 - DDoS (Distributed Denial of Service) Mitigation
 - Vulnerability Scanning and Patch Management
 - Intrusion Detection or Prevention Systems (IDS / IPS)

- Security Incident & Event Monitoring (SIEM)
- Network Firewalls and Web Application Firewalls (WAF).

8.3. Vulnerability & Patch Management

- 8.3.1. Vulnerability Management is a security practice designed to proactively prevent the build-up of security vulnerabilities within an organisation's IT infrastructure. 3rd parties must ensure that they have comprehensive vulnerability scanning and management procedures in place.
- 8.3.2. Patch management procedures must be implemented to ensure that vulnerabilities are addressed proactively, with patches rated as security critical by key vendors such as Microsoft assessed monthly.

8.4. Backup Security Policy

- 8.4.1. All daa systems must be backed up as defined by an agreed Data Retention Policy or Procedure. Records relating to backups must be completed & retained for the period that the backup is retained.
- 8.4.2. Backup and retention procedures must comply with application Data Protection laws and GDPR.
- 8.4.3. Backup media must be stored securely (e.g. in a safe or high-security facility) and transported securely.
- 8.4.4. Backups must be tested periodically. In addition to testing the backup media, the process for restoring the system should be tested periodically. Media should be retired in line with manufacturers' recommendations.
- 8.4.5. Where backups are stored in the same location as the source system, procedures must include off-site backups. These must be subject to the same security standards as on-site backups.

9. Physical Security of IT Facilities & Equipment

9.1. General Site Security Requirements

- 9.1.1. All facilities that house personnel that support daa systems or services must be physically secured areas that are only accessible to authorised parties or visitors who are accompanied by an authorised party.
- 9.1.2. A security perimeter with appropriate physical security controls must be in place between public areas and areas that house personnel that support daa systems or services.

9.2. IT Facilities Security Requirements

- 9.2.1. All network, IT and supporting systems that support daa systems or services must be housed in physically secured areas that are only accessible by authorised parties or visitors who are accompanied by an authorised party.
- 9.2.2. A security perimeter with appropriate physical security controls must be in place between public areas, general areas, and areas that house IT systems.
- 9.2.3. Power and telecommunications cabling carrying data or supporting IT services should be housed in appropriate ducting or otherwise protected from interference or damage.
- 9.2.4. Key IT facilities (such as data centres) should be
- Formally managed via ITIL-based Service Management System (SMS) or similar procedures.
 - Designed to be resilient against known threats such as natural disasters, malicious attack, or accidents.
- 9.2.5. All IT systems that support daa systems or services must be supported by an Uninterruptible Power Supply (UPS) or backup power, such as a generator. In addition, such systems should have incoming power supply redundancy with diverse routes within the supply network.