Further detail for each principle is contained in the supporting guidance document, G1772 Operational Technology Cyber Security – Operations and Maintenance.

4.2 OT Project Lifecycle Requirements

The following activities take place during the OT project lifecycle:

4.2.1 Concept Phase

4.2.1.1 The early development of a system concept, which will include initial risk assessments and cyber threat modelling.

4.2.2 Preliminary Design Phase

4.2.2.1 Developing the concept through early design activities to include the production of:

- High Level or Concept Design
- Draft Network specifications and proposed configurations
- Draft interface specifications
- Draft Cyber Security plan
- High Level Security Architecture.

4.2.3 Detailed Design Phase

4.2.3.1 Refining the preliminary design to a final design, including:

- Low Level or Detailed Design
- Network specifications and configurations
- Network traffic profile and expected communication paths
- Interface specifications
- Cyber Security plan
- Security Architecture, including Zone and Conduit model.

4.2.3.2 The design process will include consideration of incident management arrangements, secure development processes and testing arrangements.

4.2.4 Factory Acceptance Testing Phase

4.2.4.1 Functional testing of the system, including Cyber Security controls within the constraints of a factory setting. Staff and partners who are responsible for operating the system would expect to be involved in the Factory Acceptance Testing (FAT) phase so they can start to understand the system.

4.2.5 Installation Phase

4.2.5.1 The system is installed in the operational location. During this phase, staff and partners will receive Cyber Security training relating to the Cyber Security requirements, controls, and deliverables of the system.

4.2.6 Site Acceptance Testing Phase

4.2.6.1 Functional testing of the system, including Cyber Security controls within the constraints of a non-operational site setting.

4.2.6.2 Successful site acceptance testing will form the key determination of operational readiness.

4.2.7 Operations and Maintenance Phase

Documentation

4.2.7.1 The project shall provide staff and partners who are responsible for the OT system with documentation covering the design of the Cyber Security controls and their ongoing operation and maintenance.

4.2.7.2 As a minimum, the following documentation is to be provided for handover:

- Operational manuals
- Network specifications and configurations
- Baseline network traffic plan
- Cyber Security plans
- Asset Register
- High Level or Concept Design Document
- Low Level or Detailed Design Document.

Handover into Operation

4.2.7.3 The staff and partners who are responsible for the OT system must receive documentation to confirm that all the Cyber Security controls have been verified and validated as functional at handover.

4.2.7.4 The staff and partners who are responsible for the OT system must receive documentation to confirm that, where possible, identified risks and remediations have been closed out and that appropriate mitigating controls have been implemented where this has not been possible.

Training

4.2.7.5 The System Owner and Lead Maintainer must receive a comprehensive training program encompassing the entire Cyber Security program, developed security plans as well as the technical features and implementation details of the solutions developed/deployed during the project lifecycle.

Operational Lifecycle

4.2.7.6 The System Owner shall maintain an up-to-date asset register of all hardware and software components.

4.2.7.7 The System Owner shall implement and maintain the necessary processes and procedures to meet the requirements within this Standard.

4.2.7.8 The System Owner shall undertake periodic reviews of security controls, processes and procedures as identified within this Standard.

4.2.7.9 The System Owner shall undertake continuous verification and validation of Cyber

Security controls and activities

4.2.7.10 The System Owner shall review Cyber Security risks on a periodic basis and no less than every 12 months

4.2.8 Modifications and Retrofit Phase

Operation and Maintenance

4.2.8.1 Prior to any modification of an OT asset, a Cyber Security risk assessment must be conducted to confirm that any temporarily disabled security features will not significantly impact the overall security posture of the OT asset during modification.

4.2.8.2 For any OT asset modification, the overall security posture of the of the current Cyber Security plan should be considered to ensure that the maintenance of the program provides assurance that implemented controls remain in place, and continue to operate correctly, and that the program itself continues to remain effective.

Secure Supply Chain

4.2.8.3 The staff and partners who are responsible for the OT system must ensure that secure supply chain requirements apply to both hardware and software assets.

4.2.8.4 There must be an ongoing process to protect the supply chain for OT assets. This process must contain adequate plans, processes, procedures, and registers to continually demonstrate to the system owner that the supply chain remains secure.

4.2.8.5 The secure supply chain must be used throughout the project or system lifecycle.

4.2.8.6 There must be controls in place to protect the systems during their physical or logical transport ensuring that the assets are not vulnerable to subversion, including malicious code insertion, counterfeit insertion, and tampering.

4.2.8.7 The secure supply chain process must be extended to third party products which are incorporated into the system.

4.2.8.8 The secure supply chain process must address and continually demonstrate the following during the project or contract lifecycle:

- Chain of custody practises and updated documentation.
- Inventory management including the location and protection of physical and logical assets including spare parts.
- Information protection
- Secure digital products delivery
- Trusted channels and controls to ship assets including tamper-proof packaging
- Controls to detect unauthorised access and/or alteration throughout the delivery process
- Cascading of these Cyber Security requirements to the entire supply chain
- Collection and preservation of evidence demonstrating security of the supply chain.

4.2.9 Decommissioning and Disposal Phase

4.2.9.1 There must be procedures in place to address decommissioning and disposal of OT assets (including media) in a controlled and secure manner, to avoid disruption to interfacing OT assets and disclosure of sensitive information.

4.3 The Purdue model and Secure OT Design

Sections 4.4 to 4.8 of the guidance document (G1772) provide knowledge and understanding which support the good practice principles in Section 4.2 and the OT Project lifecycle requirements in Section 4.3.

5 Protecting against cyber attack

The following controls will contribute to protecting TfL's OT against cyber-attack and establish the minimum baseline of Cyber Security measures for operating and maintaining new or upgraded systems securely. The minimum baseline Cyber Security measures should be adopted when operating or maintaining any OT supporting TfL services, recognising that legacy systems may not have been designed with these Cyber Security controls in place. Hence a risk assessment to be carried out and if required, the concession processes to be followed and work to close out any gaps.

Safety critical and service critical systems will have been risk assessed at the design stage and are expected to require additional controls above the minimum baseline, for which suggestions are shown in the notes.

5.1 Identity and access control

TfL must assure good management and maintenance of identity and access control for the networks and information systems supporting TfL services.

The requirement is that the system owner will have to maintain a list of all users (humans, software processes and devices) and to determine for each control system component the required level of Identity and Access Control (IAC) protection.

Access control is the method of controlling who or what entities can access premises and systems, as well as the type and level of access that is permitted. There are three key aspects associated with access control:

- account administration
- authentication
- authorisation.

All three aspects shall work together to establish a sound and secure access control strategy. Account administration is the method associated with granting and revoking access accounts and maintaining the permissions and privileges provided under these accounts to access specific resources and functions on the physical premises, network, or system. Access accounts should be function or role-based and may be defined for individuals, groups of individuals functioning as a crew or for devices providing a function.

The detailed requirements are aligned to the headings below to group requirements under common functions and to support traceability to the NIS regulations where required.

5.1.1 Account administration

As an organisation, TfL must ensure, on an ongoing basis, that only appropriate individuals or entities have accounts that allow access and that these accounts provide appropriate access privileges.

The system owner must ensure compliance with the following minimum baseline requirements:

5.1.1.1 Access shall be granted, changed, or terminated on the authority of an appropriate manager or system owner.

5.1.1.2 A record shall be maintained of all access accounts, including details of the individual(s) and devices authorised to use the account, their permissions, and the authorising manager.

5.1.1.3 Access accounts shall be suspended or removed as soon as they are no longer needed, for example in the event of a job change. 3rd parties engaged on the support and maintenance of systems are required to notify TfL of Joiners, Movers and Leavers.

5.1.1.4 All established access accounts shall be reviewed three-monthly to ensure that the accounts only provide the minimum required permissions.

5.1.1.5 The use of default accounts and passwords is forbidden.

5.1.1.6 There shall be no default or test credentials present/enabled on the system during operation. Passwords for access accounts shall be changed from default or test credentials before the system is handed into operation.

5.1.1.7 Periodic reviews of compliance, minimum six-monthly, to the account administration process should be performed.

5.1.1.8 Implement and maintain procedures for the creation, distribution, management and administration of user accounts.

Note: For safety critical and service critical systems the following additional requirements shall apply:
5.1.1.9 Unified account management (for example, an Active Directory service supporting multiple systems within a security Zone)

5.1.2 Authentication

As an organisation, TfL must positively identify network users, hosts, applications, services, and resources for computerised transaction so that they can be given the rights and responsibilities associated with the accounts they have been granted under account administration.

The system owner must ensure compliance with the following minimum baseline requirements:

5.1.2.1 All users must be authenticated before using an application or system.

5.1.2.2 Anonymous authentication shall not be permitted.

5.1.2.3 There shall be no hard-coded credentials in the system.

5.1.2.4 Root or administrator level accounts shall not be used as main credentials.

5.1.2.5 All default credentials must have been changed by FAT.

5.1.2.6 All system administrator access accounts and application configuration access accounts shall have strong authentication practices (such as requiring strong passwords or Multi Factor Authentication (MFA).

5.1.2.7 There shall be no use of SMS for MFA (alternatives are one-time passcodes from an app like Google Authenticator or hardware MFA).

Where this is not technologically achievable, possible compensating controls could include separate physical or electronic entrance control technologies or administrative practices, such as a two-person rule. In large scale or distributed systems, the use of a centralised access control system, such as LDAP or Radius, should be considered.

5.1.2.8 After 3 failed login attempts by a local or remote user, the system will disable the associated access account for 3 hours. There may need to be exceptions for local accounts on systems where constant access is required, such as Human Machine Interfaces (HMIs) in control rooms. Such exceptions must be covered by the concessions process and be recorded in the system risk register.

5.1.2.9 After 30 minutes of inactivity, a local or remote user will be required to re-authenticate before the user can re-access the system. There may need to be exceptions for local accounts on systems where constant access is required, such as HMIs in control rooms. Such exceptions must be covered by the concessions process and be recorded in the system risk register.

5.1.2.10 The system shall not allow multiple concurrent logins.

5.1.2.11 The system shall not allow applications to retain authentication data between sessions.

5.1.2.12 All access attempts to critical systems should be recorded and retained in a log file for a minimum period of three months.

5.1.2.13 Log Files should be reviewed weekly for successful and failed access attempts as well as unusual or unexpected activity such as out of hours access or attempts to access the system by unauthorised users.

5.1.2.14 Systems should employ an authentication scheme (such as X.509) for task-to-task communication between applications and devices.

Note:	For safety critical and service critical systems the following additional requirements shall apply:
5.1.2.15	MFA for untrusted networks.
5.1.2.16	MFA for all networks.

5.1.3 Authorisation

As an organisation, TfL must grant access privileges to resources after successful authentication of the user and identification of their associated access account. The privileges granted are determined by the account configuration set up during the account administration step in the business process.

The system owner must ensure compliance with the following minimum baseline requirements:

5.1.3.1 There must be clearly documented rules that define the privileges authorised for access accounts which are aligned to the job roles for the system. These rules must follow the principles of least privilege.

5.1.3.2 The system must apply these rules to all users upon authentication.

5.1.3.3 Access accounts must be role based to manage access to appropriate information or systems for that user's role.

5.1.3.4 Safety implications shall be considered when defining roles.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.1.3.5 Unique identification and authorisation.

5.1.3.6 Hardware security for software process identity credentials.

5.1.4 Passwords

As an organisation, TfL must ensure that for control systems utilising password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.

The system owner must ensure compliance with the following minimum baseline requirements:

If an OT system does not have the capabilities to meet all the password requirements, a concession must be raised.

5.1.4.1 Maintain the systems capability of a configurable password management facility to allow passwords to be selected according to the requirements in 5.1.4.2.

5.1.4.2 Passwords must meet the following requirements:

- Minimum 13 characters long when set by a human.
- Minimum 13 characters long minimum when set by a system/service.
- The system must support a password of at least 64 characters maximum length.
- All ASCII characters (including space) shall be supported for passwords.
- The password shall not be truncated when processed.
- The chosen password shall be checked with known password dictionaries.

- The system shall allow the number of password attempts before lockout to be set (5.1.2.8 refers).
- The system shall deny the repeated use or recycling of the last five passwords.
- here shall be no complexity requirements for passwords.
- There shall be no password expiration period.
- There shall be no password hints.
- There shall be no knowledge-based authentication (e.g. who was your best friend in high school?).

5.1.4.3 Passwords shall not be stored, electronically or hard copy, in plain text. The exception to this requirement is the sharing of an initial or recovery password with an authorised user, which must be in a separate communication to the user identification.

5.1.4.4 Copies of root, administrator, and system account details, retained for emergency use, must be stored separately from the system and in a secure storage.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.1.4.5 Password generation and lifetime restrictions for human users

5.1.4.6 Password lifetime restrictions for all users

5.1.5 Wireless Access Management

As an organisation, TfL must ensure that the control system provides the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

The system owner must ensure compliance with the following minimum baseline requirements:

5.1.5.1 Maintain the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

5.1.5.2 Wireless networks shall have MAC Address filtering enabled.

5.1.5.3 Maintain the capability to authorise, monitor and enforce usage restrictions for wireless connectivity to the control system.

5.1.5.4 Wireless systems shall employ a key management system.

5.1.5.5 Wireless encryption requirements are contained in Section 5.5.5 (Encryption).

5.1.5.6 Wireless devices shall be protected with security controls, such as access control and encryption, to protect the devices from unauthorised access, modification, or use.

5.1.5.7 Where Public Key Infrastructure (PKI) is utilised, maintain the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.

Requirements 5.1.5.8 and 5.1.5.9 are only applicable to systems that provide open public WIFI networks at Stations and on passenger trains or trams.

5.1.5.8 There shall be a process to disable open public WIFI networks within 15 minutes of being requested.

5.1.5.9 There shall be a process to reenable open public WIFI networks

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.1.5.10 Hardware security for public key authentication

5.1.6 User Change Management and Access Review

As an organisation, TfL must ensure they are able to track joiners, movers and leavers in order to ensure that each individual user is only granted minimum required access rights for their role, that these rights are reviewed when they change role and revoked on leaving TfL.

It is essential that access to any OT system which supports the delivery of TfL services is authorised by the system owner or a delegated deputy (Section 5.1.1.1 refers).

System owners should conduct a regular review of user access rights for the system(s) they are responsible for and ensure those which are no longer required are revoked (Sections 5.1.1.3 and 5.1.1.4 refer).

System owners must conduct user change management and access review activities through the following minimum baseline requirements:

5.1.6.1 All human users shall be uniquely identified and authenticated.

5.1.6.2 All non-human users shall be uniquely identified and authenticated.

5.1.6.3 This identification and authentication shall be enforced on all interfaces which provide access to the control system to support the verification of the principle of least privilege.

5.1.6.4 The management of all accounts including adding, activating, modifying, disabling, and removing accounts is to only be performed by authorised users.

5.1.6.5 Users are to be managed through the use of identifiers by user, group, role, or control system interface.

5.1.6.6 Ensure to:

- change all default authenticators upon control system installation.
- change/refresh all authenticators as required; and
- protect all authenticators from unauthorised disclosure and modification when stored and transmitted.

5.1.7 Monitor Access

As an organisation, TfL must provide the capability to log and monitor all user access to any OT system, which will form an integral element of system monitoring.

The system owner must maintain compliance with the following minimum baseline requirements:

5.1.7.1 Feedback on authentication information during the authentication process shall be obscured. (For example, responding to a failed login attempt with a "login failed" message rather than "your password was incorrect" which shows an attacker they have used a valid user ID).

5.1.7.2 There shall be an enforced limit, currently three (Section 5.1.2.8 refers), of consecutive invalid access attempts for any user (human, software process or device) during a configurable time period, which is recommended to be set at thirty minutes.

5.1.7.3 Any user shall be denied access for three hours or until unlocked by an administrator when the consecutive invalid access attempts limit has been exceeded (Section 5.1.2.8 refers).

5.1.7.4 There shall be the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorised personnel.

5.1.7.5 The capability shall be maintained to enforce authorisations assigned to all users (humans, software processes and devices) for controlling use of the system to support segregation of duties and least privilege.

5.1.7.6 The capability shall be maintained for an authorised user or role to define and modify the mapping of permissions to roles for all human users, software processes and devices.

5.1.7.7 The capability shall be maintained to automatically enforce configurable usage restrictions that include:

- preventing the use of portable and mobile devices
- restricting code and data transfer to/from authorised portable and mobile devices.

5.1.7.8 The capability to log the following events shall be maintained:

- Failed log in attempts
- Automatic account reset
- Administrative account reset
- Successful logins out of normal working patterns
- Password changes
- Permission changes
- Failed attempts to connect unauthorised portable and mobile devices
- Connection of authorised portable and mobile devices.

5.1.7.9 The capability shall be maintained to forward user logging securely to a central log collector (Section 6 refers).

5.2 Data Security

TfL must protect data which is stored or transmitted electronically from actions such as unauthorised access, modification or deletion that may cause an adverse impact on essential functions.

This protection must be underpinned by a good understanding of the data that is important to the delivery of the TfL services, where it is stored, where it travels, and how unavailability or unauthorised access, modification or deletion would impact the service. This also applies to any third parties storing or accessing data important to the delivery of TfL services.

5.2.1 Identify and Understand Critical Data (Information and Documents)

As an organisation, TfL must ensure that for each OT system, there is a record of the location, type, quantity, and quality of data important to the delivery of TfL services. In addition, this record must include the context, limitations and dependencies of the data that is critical to TfL services.

Much of the information about the OT system may be stored electronically or in hardcopy outside the system and is not protected by OT authorisation controls. Unauthorised access and use of this information are a threat to OT security and this information needs to be appropriately controlled and managed.

The system owner must ensure compliance with the following minimum baseline requirements:

5.2.1.1 A document management process shall be maintained for OT information which supports the system.

5.2.1.2 Information classification levels, commensurate with S1782 Information Security Classification, shall be implemented for access and control, including sharing, copying, transmitting, and distributing of OT information.

5.2.1.3 All logical assets within the scope of the system (including, but not limited to, system design information, vulnerability assessments and network diagrams) shall be classified to indicate the protection required commensurate with the consequence of compromise. (S1782 – Information Security Classification refers).

5.2.1.4 Implement and maintain procedures, commensurate with S1782 Information Security Classification, for retention, physical and integrity protection, destruction, and disposal of all assets based on their classification, including written and electronic records, equipment and other media containing information, with consideration for legal or regulatory requirements.

5.2.1.5 Measures shall be employed to ensure long-term records can be retrieved. This could include converting the data to a newer format or retaining older equipment that can read the data.

5.2.1.6 Information that requires special control or handling shall be reviewed on a periodic, at least annual, basis to validate that special handling is still required.

5.2.1.7 Periodic, minimum annually, reviews of compliance to S1782 Information Security Classification shall be performed.

5.2.2 Understand Data Links

As an organisation, TfL must ensure that for each OT system, there is a documented and up to date understanding of the data links used to transmit data that is critical or important to the delivery of TfL services.

The system owner must ensure compliance with the following minimum baseline requirements:

5.2.2.1 A documented record must be maintained of all the data links that transfer data into or out of the system.

5.2.2.2 The record must include the context, limitations and dependencies of the data links that are critical to TfL services.

5.2.2.3 The record shall support and inform the capability to protect the integrity of transmitted information (Section 5.5.2 refers).

5.2.3 Identify Mobile Devices and Portable Media

As an organisation, TfL must ensure that all mobile devices and media that may hold data important to the delivery of the TfL services and are used to support the OT system must be identified and recorded.

Mobile devices include but is not limited to laptop computers and handheld programmers. Media assets include removable media and devices such as floppy disks, CDs, DVDs, and USB memory sticks, as well as printed reports and documents.

If an adversary gains access to backup media associated with an OT system, it could provide valuable data for launching an attack. Recovering an authentication file from the backups might allow an adversary to run password cracking tools and extract usable passwords. In addition, the backups typically contain machine names, IP addresses, software version numbers, usernames, and other data useful in planning an attack.

The system owner must ensure compliance with the following minimum baseline requirements:

5.2.3.1 The use of any unauthorised mobile device or portable media on any node that is part of or connected to the OT system shall not be permitted in order to prevent the introduction of malware or the inadvertent loss or theft of data.

5.2.3.2 Systems shall only use removable media and mobile devices where absolutely necessary and must undergo business justification and further risk assessment to provide justification for all enabled USB ports, CD/DVD drives and other removable media devices.

5.2.3.3 Where the use of a mobile device or portable media is permitted, this must be a dedicated device which is subject to an equivalent level of protective controls to the OT system that it is used to support.

5.2.3.4 There shall be a documented process to verify that a mobile device is free from malware before and after it is connected to the system (Section 5.7.1 refers).

5.2.3.5 A documented record of all authorised mobile devices and portable media which are associated with the system must be maintained.

5.2.3.6 The number of authorised removable media and mobile devices shall be kept to the absolute minimum required for system operation.

5.2.3.7 Mobile devices and portable media that will be transported between physically secure locations is to employ data at rest encryption.

5.2.3.8 Where the use of removable media is authorised and the system supports it, software shall be used to enforce removable media processes.

5.2.3.9 Mobile devices and portable media are to be secured in a locked cabinet when not in use.

5.2.3.10 Periodic reviews of compliance, minimum six-monthly, of the record of all authorised mobile devices and portable media.

5.2.3.11 Implement and maintain procedures for the actions to be taken due to the loss of mobile devices and portable media.

5.2.4 Manage Data Holdings

As an organisation, TfL must ensure that data holdings relating to OT are managed throughout the life of the system.

The system owner must ensure compliance with the following minimum baseline requirements:

5.2.4.1 A documented record shall be maintained of data holdings relating to the system which will include, but not be limited to, design documentation, operational data, system logs and backups.

5.2.4.2 Review and then remove or minimise unnecessary copies or unneeded historic data.

5.2.4.3 Data retention must be aligned to regulation, system operating requirements and security monitoring requirements. For example, if system logs are ingested into a centralised logging system, they do not need to be retained in perpetuity on the system, but only for local fault finding or recovery purposes, which would require up to a months' worth of data.

5.2.4.4 Periodic reviews of compliance, minimum six-monthly, of the record of all data holdings.

5.2.4.5 Data which is no longer required or has passed its retention period shall be deleted or destroyed in a secure manner.

5.3 Personnel Security

TfL must closely manage privileged user access to networks and information systems supporting the TfL services.

Personnel security has three related aspects. From an organisational HR perspective, it involves looking at new and current personnel to determine if they will maintain the OT security for the organisation. For new personnel, the personnel security process evaluates them prior to their entry into the organisation making sure they demonstrate behaviours consistent with their future security responsibility. For current personnel, the personnel security process establishes that they continue to demonstrate behaviour consistent with their current security responsibilities.

Personnel security requirements are also driven by concerns about training, approved staff, awareness of the system, awareness of safety and in some instances malicious activity (generally referred to as Insider Threats). For more information on Insider Threats refer to G1134: Personnel Security – Insider Threat.

From a system owner perspective, the approach is ensuring that the system has the required capabilities and processes to support the minimum baseline controls for personnel security and builds on the baseline identity and access control requirements in Section 5.1.

5.3.1 Privileged User Access

TfL must ensure that individuals who require privileged levels of user access receive additional validation and authentication.

The system owner must ensure compliance with the following minimum baseline requirements:

5.3.1.1 Privileged access shall be granted, changed, or terminated on the authority of an appropriate senior manager or system owner.

5.3.1.2 Privileged access accounts should be dedicated to a specific function and must not be used for general administrative tasks.

5.3.1.3 Privileged access accounts must use MFA.

5.3.1.4 A non-privileged user must not be able to gain privileged access rights without proper authorisation and such authorisation should only be temporary to support an urgent business need.

5.3.1.5 Enforce authorisations assigned to all users (humans, software processes and devices) for controlling use of the system to support segregation of duties and least privilege.

5.3.1.6 An authorised user or role shall maintain and modify the mapping of permissions to roles for all human users.

5.3.2 User Management

TfL must ensure that the identities of the individuals, whether employees or partners, with privileged access to networks and information systems to support the TfL services systems are known and managed.

The system owner must ensure compliance with the following minimum baseline requirements:

5.3.2.1 A record shall be maintained of all privileged access accounts, including details of the individual(s) and devices authorised to use the account, their permissions, and the authorising manager.

5.3.2.2 Privileged access accounts shall be suspended or removed immediately when they are no longer needed, for example in the event of a job change.

5.3.2.3 The capability to automatically enforce configurable usage restrictions for users shall be maintained, which includes:

- preventing the use of portable and mobile devices
- requiring context specific authorisation; and

- restricting code and data transfer to/from portable and mobile devices.

5.3.2.4 Implement and maintain procedures for the creation, distribution, management and administration of privileged user accounts.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.3.2.5 Supervisor override

5.3.2.6 Hardware security for public key authentication.

5.3.3 Role Based Access

TfL should ensure that privileged users are granted only specific privileged permissions which are essential to their business role or function.

The system owner must ensure compliance with the following minimum baseline requirements:

5.3.3.1 Duties should be segregated amongst personnel to maintain appropriate checks and balances, so that no single individual has total control over actions that change the functional operation of the OT.

5.3.3.2 Personnel should be assessed for the critical positions controlling and maintaining the OT.

5.3.4 Privileged Access Review

TfL must conduct a regular review and validation of activity by privileged and standard users to identify any unauthorised or unusual activities.

The system owner must ensure compliance with the following minimum baseline requirements:

5.3.4.1 All established privileged access accounts shall be reviewed monthly to ensure that the accounts only provide the minimum required permissions and remain a valid requirement for operating the system.

5.3.4.2 Maintain audit records relevant to privileged account security for the following categories:

- access control
- request errors
- operating system events
- system events
- configuration changes
- potential reconnaissance activity and audit log events.

5.3.4.3 Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.

5.3.4.4 Maintain sufficient audit record storage capacity for log management and system configuration. This shall be to a minimum of one year's worth of records.

5.3.4.5 Maintain timestamps for use in audit record generation.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.3.4.6 Supervisor override

5.3.4.7 Hardware security for public key authentication.

5.4 Physical Security

TfL must ensure that physical security arrangements compliment OT Cyber Security and protect the OT supporting the TfL services from direct attack.

This will create a secure environment for the protection of OT assets.

This section should be read in conjunction with established physical security standards (Listed or linked in Section 13) and in consultation with the physical security team. The intention is to ensure that physical and Cyber Security arrangements are complementary and maintained properly throughout the life of the system. This section is not intended to replace established physical security standards, but rather to highlight to TfL staff and partners where particular physical security considerations are relevant to OT systems.

Surveillance and security systems, in particular CCTV, access control systems and intruder detection systems shall comply with S1147 Surveillance and Security Systems.

An asset is any physical or logical object owned by, or operated by, TfL having either a perceived or actual value to the organisation for delivery of TfL services. OT assets are those assets that are a part of the OT, either physical or cyber or that can affect the operation of the OT.

IT assets used in support of or as part of OT systems shall comply with S1747 Physical Security of IT Equipment.

Physical security measures ensure that all assets, specifically those related to the OT of an organisation, are protected physically from unauthorised access, loss, damage, misuse, and the like. Environmental security measures ensure that the assets of an organisation are protected against environmental conditions that would make them unusable or damage the information they contain.

Physical and environmental security measures should be maintained to complement the Cyber Security measures taken to protect assets that are part of the OT and coordinated with the physical security of the remainder of the infrastructure.

It is important to include all systems in the scope and not just limit the effort to traditional computer room facilities and equipment rooms. Practical engineering judgment should be used to balance the risks when determining physical security procedures.

Physical segmentation is a key security countermeasure designed to compartmentalise devices into security Zones where identified security practices are employed to achieve the desired target security level.

The physical protection of the cyber components and data associated with the system must be addressed as part of the overall security of a system. Security at many OT facilities is closely tied to site safety. A primary goal is to keep people out of hazardous situations without preventing them from doing their job or carrying out

emergency procedures. Physical security controls are any physical measures, either active or passive, that limit physical access to any information assets in the OT environment.

These measures are employed to prevent many types of undesirable effects, including:

- Unauthorised physical access to sensitive locations
- Physical modification, manipulation, theft or other removal, or destruction of existing systems, infrastructure, communications interfaces, personnel, or physical locations
- Unauthorised observation of sensitive informational assets through visual observation, note taking, photographs, or other means
- Prevention of unauthorised introduction of new systems, infrastructure, communications interfaces, or other hardware
- Prevention of unauthorised introduction of devices intentionally designed to cause hardware manipulation, communications eavesdropping, or other harmful impact.

The system owner must ensure compliance with the following minimum baseline requirements:

5.4.1.1 Security procedures that address the physical security in the protection of assets shall be implemented and maintained for the system

5.4.1.2 At least one physical security perimeter shall be maintained to provide barriers against unauthorised access to protected assets. Critical components and systems must have at least two physical perimeters.

5.4.1.3 There must be entry controls at each physical barrier or boundary.

5.4.1.4 There shall be an auditable record of access to equipment via a security barrier or boundary.

5.4.1.5 All connections under the control of the system shall be adequately protected from tampering or damage.

5.4.1.6 Arrangements must be established to protect assets against environmental damage from threats such as fire, water, smoke, dust, radiation, corrosion, and impact.

5.4.1.7 Maintenance procedures must be implemented for all equipment assets, including auxiliary environmental equipment, to ensure proper operation through correct maintenance.

5.4.1.8 Implement and maintain procedures for monitoring, alarming and investigating when physical or environmental security is compromised.

5.4.1.9 Procedures should be implemented and audited with respect to the addition, removal, and disposal of all assets.

5.4.1.10 Implement and maintain procedures to ensure the protection of critical components during the interruption of operations, for example, due to fire, water ingress, security breach, interruption, natural or any other type of disaster.

5.4.1.11 Physical security arrangements must be reviewed on a six-monthly basis.

5.5 Network Security

TfL must ensure that the transit of data important or critical to the delivery of TfL services is protected. This includes the transfer of data to third parties.

5.5.1 Data Transfer

The system owner must ensure that:

5.5.1.1 All Conduits for data transfer have been identified according to Section 5.2.2.

5.5.1.2 Conduits shall be maintained to protect the data they are transferring. Options to protect the data include, but are not limited to:

- Encryption (See Section 5.5.5)
- Secure Tunnelling, such as VPNs (See Section 5.5.6)
- Data Diodes
- Inbound and outbound boundary (firewall) rules.

5.5.2 Data Protection

TfL must ensure that the system has the capability to protect the integrity of transmitted information.

The system owner must ensure compliance with the following minimum baseline requirements:

5.5.2.1 Maintain confidentiality of information for which explicit read authorisation is supported, whether at rest or in transit.

Staff and partners should pay particular attention to the information confidentiality relating to portable and mobile devices (for example engineering laptops and USB sticks).

5.5.2.2 Authentication information, such as passwords, should be considered confidential, and never be sent in a readable format.

5.5.2.3 The confidentiality of information at rest shall be protected.

5.5.2.4 Communications over untrusted or open networks shall be encrypted (See Section 5.5.5 Encryption for details).

5.5.2.5 Maintain the protection of the confidentiality of remote access sessions traversing an untrusted network.

Note: Encryption is a common mechanism for ensuring information confidentiality.

5.5.3 Single Points of Failure

TfL must ensure that the system has been designed to eliminate single points of failure where possible.

The system owner must ensure compliance with the following minimum baseline requirements:

5.5.3.1 As part of the handover process, the project must have identified single points where, due to failure, there is a significant risk of impact on the delivery of the TfL services.

5.5.3.2 Where possible, these single points of failure should have been eliminated during the design stages, but if this is not achievable, this must be recorded in the project/system risk register and incorporated into any response plans for the system.

5.5.4 Resilient Communications

TfL must ensure there are alternative communication paths where there is a significant risk of impact on the delivery of TfL services if a primary communication path is lost or interrupted.

The system owner must ensure compliance with the following minimum baseline requirements:

5.5.4.1 Communication paths where, due to failure, may have a significant risk of impact on the delivery of the TfL services must be documented, reviewed annually and compensating procedures established.

5.5.4.2 Alternative communication paths to eliminate the risk to service delivery in the primary path is lost or interrupted shall be maintained and tested. If an alternative path cannot be established, this shall be recorded in the system risk register and highlighted in any response plans for the system.

5.5.5 Encryption

TfL must ensure that the system has capability to protect the integrity of transmitted information.

This section provides the specific requirements for different methods of encryption, but it should also be noted that depending on the location or design of the system in question, alternative controls could be adopted.

The selected encryption method must provide a commensurate level of protection for the data, both at rest and in transit. This protection will be in line with the impact on TfL services if the data is compromised and will most likely have been informed by a risk or impact assessment, so the emphasis is on maintaining the level of protection through the life of the system.

Depending on the type of encryption, the system owner must ensure compliance with the following minimum baseline requirements:

5.5.5.1 For Private Key Encryption (Symmetric Key Cipher), a minimum of AES-256 must be used.

5.5.5.2 For stream ciphers, RC4 and algorithms derived from that shall not be used. AES may be used in a cryptographic mode that allows streaming provided that the key is changed in accordance with the limitations of the cryptographic mode chosen. Keys for streaming cipher modes of operation must only be used for one stream and shall not be reused.

5.5.5.3 The Electronic Codebook (ECB) and Cypher Block Chaining (CBC) block cipher mode of operation must not be used.

5.5.5.4 For key exchange, the DH (Diffie-Hellmann) algorithm must be used with a key length of at least 3072-bit (Group 15). Ephemeral Diffie-Hellmann is preferred.

5.5.5.5 For Public Key Infrastructure (Asymmetric Key Ciphers) encryption, the RSA algorithm with a key length of at least 3072-bit must be used.

5.5.5.6 For Public Key Infrastructure (Asymmetric Key Ciphers) authentication, RSA or DSA algorithms with a key length of at least 3072-bit must be used.

> DSA was originally designed for digital signatures and not for general encryption, although it can be used for general encryption purposes. NIST is trying to deprecate DSA in favour of Elliptic-Curve DSA (ECDSA) and Edwards Curve DSA (EdDSA).
>
> Consideration should be given to Elliptic Curve Cryptography (ECC) instead of RSA, such as Elliptic Curve Diffie Hellmann, since for a given approved curve, the key length is roughly halved to get the same strength of encryption.

5.5.5.7 For data hashing, SHA-256 must be used as minimum. SHA3 shall also be allowed as well as SHA2, with more than 256 bits (FIPS 202).

5.5.5.8 For file integrity checking, SHA-2 must be used as a minimum. SHA3 shall also be allowed as well as SHA2, with more than 256 bits (FIPS 202).

5.5.5.9 For 802.11-based infrastructure, WPA2 Enterprise with AES CCMP encryption and EAP-TLS 1.2 must be used as a minimum.

5.5.5.10 All encryption keys must be changed from their default value before use.

5.5.5.11 All encryption keys must be randomly generated, not human-specified; except for file-level encryption passwords specified by individual users.

5.5.5.12 Cryptographically Secure Pseudorandom Number Generators (CSPRNGs) must be used to generate encryption keys and the following CSPRNGs should be used where possible:

- RNGCryptoServiceProvider, CryptGenRandom, FIPSGenRandom or RtlGenRandom (Microsoft Windows XP Service Pack 3 or later only).
- /dev/random, /dev/urandom or /dev/arandom (preferred) (*nix-based systems).
- Any other Evaluation Assurance Level (EAL) 4+ accredited CSPRNGs.
- Any other Federal Information Processing Standard (FIPS) 186-2 compliant CSPRNGs.

5.5.5.13 CSPRNGs based on the following functions are deemed insecure and must not be used:

- Rand()
- Math.Random()

5.5.5.14 Symmetric and Private keys must be stored securely at rest using PKCS#11 or PKCS#12.

5.5.5.15 Encryption hardware should be certified to FIPS 140-2 (tamper evident) as a minimum.

5.5.5.16 Encryption hardware should be protected from physical tampering and uncontrolled electronic connections.

Cryptography also introduces key management issues since robust security policies require periodic key changes. This process becomes more difficult as the geographic size of the OT increases, with extensive OT systems being the most severe example. As site visits to change keys can be costly and slow, it is useful to be able to change keys remotely.

Note: For safety critical and service critical systems the following additional requirements shall apply: 5.5.5.17 Cryptographic integrity protection.

5.5.6 Virtual Private Networks (VPN)

TfL must ensure that any VPN used to encrypt communications is configured securely.

The system owner must ensure compliance with the following minimum baseline requirements:

5.5.6.1 When a VPN is implemented use one of the following protocols:

- Internet Protocol Security (IPsec)
- Transport Layer Security (TLS).

5.5.6.2 For remote access connections, the VPN shall include a logical break point (jump server) at an OT De-Militarised Zone (DMZ) to allow the link to be monitored.

5.5.7 Backups

TfL must ensure that there are backups of the data required to restore systems to normal operational capability (See also Section 7.2).

The system owner must ensure compliance with the following minimum baseline requirements:

5.5.7.1 Maintain secured backups of the data (systems, software, licenses, configurations, data, and other relevant information) required to allow the TfL services to operate or to restore the TfL services to an operational state within an acceptable timeframe.

Note: Automated backups are recommended to ensure that all required files are captured with reduced operator overhead.

5.5.7.2 The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be maintained without affecting normal operations.

5.5.7.3 Although not usually required for system recovery, information required for post-incident forensic activity (for example, audit logs) should be specifically included in the backup.

5.5.7.4 Where a backup contains confidential information, encryption should be considered where this will not affect any recovery operations, or the backup should be secured in a suitable lockable storage or safe.

5.5.7.5 Maintain the capability for backups to be extracted and stored securely in a separate location.

5.5.7.6 Full-bit images shall be recorded as configuration baselines for operational systems and assets. These images must be stored securely.

5.5.7.7 Verify the reliability of backup mechanisms, including the capability to conduct routine tests, at least 6-monthly, to ensure the backup process is functioning correctly and that the backups are usable.

5.5.7.8 The backups shall be accessible if an extreme event occurs.

5.5.7.9 Develop, implement and maintain procedures for the testing and verification of backups.

5.6 System Security

TfL must ensure that security is designed into the network and information systems that support the delivery of TfL services from the outset.

Staff and partners should recognise that secure design principles have been adopted to minimise the attack surface and ensure that the delivery of the TfL services should not be impacted by the exploitation of any single vulnerability. Actions taken during operations and maintenance should maintain, as a minimum, or improve, where possible, that secure envelope.

This section should be read in conjunction with the Purdue Model and secure OT architecture paragraphs in Section 4.

5.6.1 Secure by Design

TfL must employ appropriate expertise to design secure networks and information systems supporting the TfL services.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.1.1 The integrity of transmitted information shall be protected (Section 5.5 refers).

5.6.1.2 Only permitted, verified, and tested software from authorised sources shall be installed.

5.6.1.3 Port security shall be implemented on network devices to prevent the use of unused ports.

5.6.1.4 There shall be no unmanaged network devices on the system

5.6.1.5 Protection mechanisms shall be employed to prevent, detect, report, and mitigate the effects of malicious code or unauthorised software.

5.6.1.6 The protection mechanisms shall be updated on at least a quarterly basis or when an update is provided by the manufacturer.

5.6.1.7 Verify the intended operation of the security functions on a periodic basis and report when anomalies are discovered during verification and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.

5.6.1.8 Detect, record, report and protect against unauthorised changes to software and information at rest.

5.6.1.9 Maintain the system so that it validates the syntax and content of any input which is used as an input that directly impacts the action of the system.

5.6.1.10 Maintain the systems capability to set outputs to a predetermined state if normal operation cannot be maintained because of an attack.

5.6.1.11 Maintain the systems capability to identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the OT unless revealing this information is necessary for the timely troubleshooting of problems.

5.6.1.12 Maintain the systems capability to protect the integrity of sessions.

5.6.1.13 Maintain the systems capability to reject invalid session IDs.

5.6.1.14 Maintain the protection of audit information and audit tools (if present) from unauthorised access, modification, and deletion.

5.6.1.15 The number of concurrent sessions per interface for any given user (human, software process or device) shall be limited to a configurable number of sessions.

5.6.1.16 Malicious code protection mechanisms shall be maintained at all entry and exit points.

5.6.1.17 The partitioning of data, applications and services based on criticality to facilitate implementing a zoning model (Section 5.6.5 and supporting guidance refers) shall be maintained.

5.6.1.18 Maintain the systems capability to operate in a degraded mode during a Denial of Service (DoS) event.

5.6.1.19 Maintain the systems capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events.

5.6.1.20 Maintain the systems capability to limit the use of resources by security functions to prevent resource exhaustion.

Note:	For safety critical and service critical systems the following additional requirements shall apply:
5.6.1.21	Central management and reporting for malicious code protection.
5.6.1.22	Automated mechanisms for security functionality verification.
5.6.1.23	Security functionality verification during normal operation.

5.6.1.24	Automated notification about integrity violations.
5.6.1.25	Hardware and software inventory.
5.6.1.26	Discovery tooling.

Note: Where these has been implemented they shall be maintained.

5.6.2 Configuration Management / Change Control

TfL must implement configuration management processes to control modifications to hardware, firmware, software, and documentation to ensure that the system is protected against improper modifications prior to, during, and after system implementation.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.2.1 The current OT network configuration and device configurations must always be known and documented.

5.6.2.2 A formal change management process shall be used to ensure that all modifications to an OT network meet, or exceed, the security requirements as defined in the system specifications or low-level design.

5.6.2.3 Risk assessment must be performed on all changes to the OT network that could affect security, including configuration changes, the addition of network components, and installation of software.

5.6.2.4 There should be restricted access to configuration settings of OT components.

5.6.3 System and Information Integrity

TfL must maintain system and information integrity to ensure that sensitive data has not been modified or deleted in an unauthorised and undetected manner.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.3.1 There shall be controls maintained for malware detection, spam and spyware protection and intrusion detection.

5.6.3.2 An alert shall be investigated if these controls are triggered.

5.6.4 Malware Detection

TfL must ensure that malware detection products are deployed as widely as possible.

Malware detection products evaluate files on a computer's storage devices against an inventory of known malware signature files.

Anti-malware software can be deployed on workstations, servers, firewalls, and handheld devices, but may not be appropriate for operational devices.

Anti-malware tools only function effectively when installed, configured, running full-time, and maintained properly against the state of known attack methods and payloads.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.4.1 Anti-malware products must be maintained on all devices that can support it. This includes, but is not limited to, Windows, Unix, Linux systems, etc. used as consoles, engineering workstations, data historians, HMIs and general-purpose SCADA and backup servers.

5.6.4.2 Malware detection shall be maintained be this anti-malware protection and / or whitelisting. Whitelisting must:

- Prevent the execution of all unauthorised software.
- Provide an alert when unauthorised software attempts to run.
- Report the list of authorised software and versions that are on the OT assets.

5.6.4.3 Signatures and updates for anti-malware products installed on the OT Network must only be obtained from secure sources (i.e. a dedicated anti-malware distribution server, located within a DMZ outside the OT network (Section 5.6.5 refers)).

5.6.4.4 Anti-malware tools and updates shall be verified that their use does not impact system performance.

5.6.4.5 Malware protection shall be in place at all physical and logical network entry and exit points, which may also need the use of 'Sheep Dips'.

5.6.4.6 Tested and verified anti-malware tool updates and signatures must be applied at least once every 4 weeks.

5.6.4.7 Implement and maintain procedures for the for the test and implementation of anti-malware signatures and updates.

5.6.5 Network Segmentation

5.6.5.1 TfL must ensure that the networks and information systems supporting the TfL services are segregated into appropriate security Zones as defined in the Zone and Conduit model (See Section 4.6 of the supporting Guidance document).

Network segmentation and the level of protection it provides will vary greatly depending on the overall network architecture. Logically segmenting networks based on their functionality provides some measure of protection but may still lead to single-points-of-failure if a network device is compromised. Physically segmenting networks provides another level of protection by removing that single-point-of-failure case but will lead to a more complex and costly network design.

5.6.5.2 The system shall be handed over with the following requirements and the System owner must ensure these are maintained throughout the operational lifecycle of the system:

5.6.5.3 The system design shall group key OT devices into separate Zones with common security levels to manage security risks and to achieve a desired target security level for each Zone.

5.6.5.4 The system shall be separated into Zones and each Zone shall have a clearly defined security level.

5.6.5.5 There shall be enforced Conduits between Zones.

5.6.5.6 There shall be firewalls between Zones of differing security levels and firewall rules shall be reviewed at least every 12 months.

5.6.5.7 There shall be Access Control Lists (ACLs) between Zones of common security levels, which shall be reviewed at least every 12 months.

5.6.5.8 There shall be a DMZ between the IT and OT Networks.

5.6.5.9 There shall be no direct Internet access to or from the OT Network.

5.6.5.10 An OT DMZ shall be used for all outbound connectivity.

5.6.5.11 There shall be Virtual Local Area Networks (VLANs) to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

5.6.5.12 The design shall ensure there are simple data flows between systems, devices, and interfaces to enable effective monitoring.

5.6.5.13 Any connections to external networks or other systems must occur through managed interfaces consisting of appropriate boundary protection devices (for example, proxies, gateways, routers, firewalls, unidirectional gateways, guards and encrypted tunnels) arranged in an effective architecture (for example, firewalls protecting application gateways residing in a DMZ). These connections must be necessary for operational and business purposes and subject to risk assessment.

5.6.5.14 High-risk or critical systems shall be subject to a risk assessment to determine if they should be isolated from or employ a barrier device to separate them from other Zones with different security levels or risks i.e. unidirectional gateways.

5.6.5.15 The system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate the zoning model. This may require that some servers may need to be duplicated on the control system network to support normal network features, for example dynamic host configuration protocol (DHCP), domain name service (DNS) or local certificate authorities (CAs).

5.6.5.16 Systems shall only be connected to external networks where absolutely necessary and must undergo business justification and further risk assessment to provide justification.

Note:	For safety critical and service critical systems the following additional requirements shall apply:
5.6.5.17	Independence from non-control system networks.
5.6.5.18	Greater logical and physical isolation of critical networks.
5.6.5.19	Island mode (physical isolation of critical networks).
5.6.5.20	Fail close operation.
5.6.5.21	Uni-directional gateways or data diodes.

5.6.6 Zone boundary protection

TfL must ensure that the system shall provide the capability to monitor and control communications at Zone or segmentation boundaries to enforce the compartmentalisation defined in the Zone and Conduits model.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.6.1 Maintain the systems capability to monitor and control communications at Zone boundaries.

5.6.6.2 Maintain the systems capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).

5.6.6.3 In response to an incident, it may be necessary to break the connections between different network segments. In that event, the services necessary to support essential operations should be maintained in such a way that the devices can continue to operate properly and/or shutdown in an orderly manner.

5.6.6.4 System boundary protections at any designated alternate location should provide the same levels of protection as that of the primary site.

5.6.7 General purpose person-to-person communication restrictions

5.6.7.1 TfL shall ensure that the system shall provide the capability to restrict or prevent general purpose person-to-person messages from being received from users or systems external to the system.

5.6.7.2 The system owner must ensure compliance with the following minimum baseline requirements:

5.6.7.3 Maintain the systems capability to restrict email or other messaging solutions that provide internal computer-to-external computer communications using outbound messages.

These internal-to external communications may be limited to the purpose of sending system alerts or other computer-generated information messages to users or systems external to the system.

5.6.7.4 Maintain the systems capability to utilise preconfigured messages to transmit alert or status information.

5.6.7.5 Maintain the systems capability to not allow users to attach files or other information to these outbound-only messages at the time the messages are created by the system.

Note: For safety critical and service critical systems the following additional mitigations shall apply:

5.6.7.6 Prohibit all general-purpose person-to-person communication.

5.6.8 Security configuration settings

TfL shall ensure that the system has the capability to be configured according to recommended security configurations (See Section 5.6.9).

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.8.1 Maintain the systems interface that supports the management of network and security configuration settings.

5.6.8.2 Maintain the systems capability to support monitoring and control of changes to the configuration settings.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.6.8.4 Implementation of an automated check process where the current security settings are automatically collected by an agent and compared to approved settings, with changes being alerted.

5.6.9 Secure Configurations

TfL shall ensure that the system has been configured according to recommended network and security configurations, aka system hardening.

If the manufacturer's recommended configurations are different to any configurations required by this standard, the differences must be reviewed and the most restrictive configuration applied, unless this would impact the safe and reliable operation of the system.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.9.1 There shall be documentation maintained which details all applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computer systems associated with the system.

5.6.9.2 There shall be a documented list of services required for any computer system running control system applications or required to interface the control system applications. The list must include:

- All ports and services required for normal operation as well as any other ports and services required for emergency operation.
- Justification as to why each service is necessary for operation.

5.6.9.3 All software components that are not required for the operation and maintenance of the control system must have been removed prior to operation and shall not be restored during operations. This must include, but is not limited to:

- Games
- Device drivers for network devices not in use
- Instant messaging services
- Servers or clients for unused Internet services
- Software compilers in all user workstations and servers except for development workstations and servers
- Software compilers for languages that are not used in the control system
- Unused networking and communications protocols

- Unused administrative utilities, diagnostics, network management, and system management functions
- Backups of files, databases, and programs used only during system development
- All unused data and configuration files
- Sample programs and scripts
- Unused document processing utilities (Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice, etc.).

5.6.9.4 Unnecessary credentials shall be removed (preferred option) or disabled.

5.6.9.5 Unnecessary communication ports and media drives shall remain disabled by logical (software) or physical (disconnection) means or secured with an engineered barrier.

5.6.9.6 The system BIOS shall remain password protected to prevent unauthorised configuration changes, unless this is not technically possible, which must be recorded in the system risk register.

5.6.9.7 There shall be documentation covering components that have been removed and/or disabled, and justification for components that remain enabled.

5.6.10 Remote Access

TfL must ensure that the system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.10.1 Systems shall only use remote access where absolutely necessary and must undergo business justification and further risk assessment to provide justification.

5.6.10.2 Remote access services shall use secure methods such as VPN and SSH.

5.6.10.3 Remote access services must route through an OT DMZ.

5.6.10.4 An OT DMZ shall be the preferred means of controlled remote access to OT systems.

5.6.10.5 Maintain the systems capability to deny access requests via untrusted networks unless approved by an assigned role.

5.6.10.6 Telnet sessions shall not be permitted.

5.6.10.7 Dial up and line modems shall not be permitted.

5.6.10.8 Maintain the systems capability to terminate a remote session either automatically after a configurable period of inactivity or manually by the user who initiated the session (Section 5.1.2 refers).

5.6.10.9 Maintain the systems multifactor authentication scheme, with an appropriate level of strength to positively identify a remote interactive user.

5.6.11 Vulnerability Management

TfL must ensure that there is the capability to manage vulnerabilities in the network and information systems to prevent disruption of TfL services.

Individual system owners must ensure that processes are implemented and maintained to comply with the principles of vulnerability management, so that the system they are responsible for can be kept secure throughout the life of the system.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.11.1 The system shall be free of known vulnerabilities on handover to operational service. Where a vulnerability cannot be resolved, suitable alternative controls must be implemented and the vulnerability, with mitigating controls and a long-term resolution plan, recorded in the project/system risk register.

5.6.11.2 The system shall not be handed over with obsolete technology in place.

5.6.11.3 Implement and maintain a process to monitor, record and analyse publicly known vulnerabilities relevant to the system to understand the risk. This will require access to documents covering the system and network configuration, high level design and asset register.

5.6.11.4 Implement and maintain a process to ensure that both publicly announced and privately notified vulnerabilities in the system are recorded and tracked. Tracked vulnerabilities must be clearly tagged with both the OT system affected and the TfL services which could be impacted if the vulnerability was exploited.

5.6.11.5 Implement and maintain a process to ensure that vulnerabilities being tracked can be assessed, prioritised, and mitigated.

5.6.11.6 Implement and maintain a process to implement a temporary mitigation solution for a vulnerability which is not exposed outside the system boundary/security Zone of the system.

5.6.11.7 Implement and maintain a process to manage and implement a temporary mitigation solution for obsolete and/or unsupported technology while pursuing migration to supported technology.

5.6.11.8 Any temporary mitigation, whether for a vulnerability or obsolete technology, must be risk assessed and recorded in the system risk register.

5.6.11.9 Maintain the systems capability to support regular tests or assessments undertaken to check for previously unknown vulnerabilities within the constituent components.

Due to the sensitive nature of OT networks and systems, operators need to carefully consider their approach to the testing of live OT, as system operation, availability and safety could be affected. Assurance could be gained without this additional risk by testing against non-operational environments or by testing individual components in a laboratory environment.

5.6.11.10 Vulnerabilities shall be rated according to the Common Vulnerability Scoring System (CVSS)

For guidance on a vulnerability management process see section 5.6.11 of G1772 Operational Technology Cyber Security Operations and Maintenance

5.6.12 Patch Management

TfL must ensure that there is the capability to deploy patches in the network and information systems to prevent disruption of TfL services.

Patches are additional pieces of code that have been developed to address specific problems or flaws in existing software. They can be part of a general service improvement plan from the manufacturer or can be in response to a specific vulnerability.

Individual system owners must ensure that processes are in place to ensure the systems they are responsible for comply with the principles of patch management and can be kept secure through life.

Applying patches to Operating System (OS) components creates another situation where significant care should be exercised in the OT environment.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.12.1 Systems will have been handed over into operation with the latest approved and validated software version and patch revision applied.

5.6.12.2 Implement and maintain a systematic and documented patch management process to monitor, record and analyse patches relevant to the system which must operate throughout the operating life of the system.

5.6.12.3 Patches must be thoroughly tested to determine they do not impact the safe operation of the system and do not introduce unexpected side effects. Regression testing is advised.

5.6.12.4 Patches must only be deployed from known secure sources i.e. from a patch management server.

5.6.12.5 Any patches which cannot be applied must be captured with the system risk register and mitigating controls identified and implemented

5.6.12.6 Patches must be risk assessed on a case by case basis and determined by the applicability to the system, the vulnerabilities that are mitigated, the priority of the vulnerability and the impact to the safety and reliability of the system.

5.6.12.7 Patches shall be applied in line with the configuration management / change management process.

5.6.12.8 Implement and maintain procedures for the test and implementation of patches.

5.6.12.9 Patches that have been risk assessed and deemed applicable for the system shall be applied at the earliest maintenance period and no later than the following:

Vulnerability Severity Rating	Remediation Period
CVSS Score 10	30 days
CVSS Score 8 or higher	90 days
CVSS Score 6 or higher	180 days
CVSS Score 4 or higher	365 days
CVSS Score 1 or higher	365 days

For guidance on a patch management process see section 5.6.12 of G1772 Operational Technology Cyber Security Operations and Maintenance

5.6.12.10 Implement and maintain procedures for the urgent testing and implementation of patches.

5.6.12.11 Patches that have been deemed urgent for the system shall be applied at the earliest maintenance period and no later than 30 days.

The need for urgent patching may be as a result of an imminent threat to the system and come several sources such as TfL's Cyber Security Team, from external agencies or TfL's partners.

5.6.13 Time Synchronisation

TfL must ensure that time is synchronised across all systems and services.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.13.1 Maintain the systems capability to synchronise with a dedicated time source through a secure interface.

5.6.13.2 Maintain the systems capability to protect the unauthorised modification of time sources.

5.7 Providing Secure Management

TfL must ensure that network and information systems that support the delivery of TfL services can be managed, operated, and maintained securely.

5.7.1 Secure Management

Systems shall be managed, operated, and maintained in a secure manner.

The system owner must ensure compliance with the following minimum baseline requirements:

5.7.1.1 Dedicated devices shall be used for the maintenance and security management of OT systems.

5.7.1.2 Devices which are used to manage and maintain systems shall be verified as free from unauthorised software and malware before being connected to conduct management or maintenance activities.

5.7.1.3 Systems shall only be administered and maintained by authorised privileged users.

5.7.1.4 Secure management processes and supporting technical information documented as part of the system development process and handed over with the system into operational service, shall be implemented and maintained.

5.7.1.5 Documents which support the system shall be stored and secured according to the criticality of the system or the impact of the loss of that system on the delivery of TfL services.

6 Detecting Cyber Security events

The following controls and considerations will contribute to detecting Cyber Security incidents within TfL's OT and establish the minimum baseline of Cyber Security measures for operating and maintaining new or upgraded systems securely. Where possible, the minimum baseline Cyber Security measures should be adopted when operating or maintaining any OT supporting TfL services, recognising that legacy systems may not have been designed with these Cyber Security controls in place.

Safety critical and service critical systems will have been risk assessed at the design stage and are expected to require additional controls above the minimum baseline, for which suggestions are shown in the notes.

6.1 Security Monitoring

TfL must ensure that systems have effective Cyber Security defences and the capability to detect Cyber Security events which affect, or have the potential to affect, the delivery of TfL services.

6.1.1 Monitoring coverage

TfL must ensure that data sources have been identified to support the timely identification of security events in the system.

The system owner must maintain the capability to meet the following minimum baseline requirements:

6.1.1.1 Security monitoring data shall be collected from identified data sources (Section 6.1.3 refers) to detect and identify security events in the system.

6.1.1.2 Maintain the systems capability to detect the presence of known indicators of compromise on the essential components of the system.

6.1.1.3 Monitoring shall be conducted of all privileged activity on the system for suspicious or undesirable activity.

6.1.1.4 There shall be monitoring in place on all network gateways and critical devices, where possible.

6.1.1.5 Maintain the network taps installed at the network choke point boundary between the OT system and any external systems.

6.1.1.6 Maintain the network taps installed at the network choke point boundary between the OT control system and its subordinate Zones.

6.1.1.7 Maintain the systems capability to collect essential information against critical services or applications (such as key servers).

6.1.1.8 Maintain the systems capability to detect the connection of unauthorised devices to the system.

6.1.1.9 There shall be documented reporting mechanisms such that any monitoring alert can allow for a timely response to events.

6.1.1.10 Maintain the centralised logging server.

6.1.1.11 Maintain the System log capability of being read locally and forwarded to the centralised logging server.

6.1.2 Securing Logs

TfL must ensure that logging data be held securely and read access to it should be granted only to accounts with a business need.

The system owner must maintain the following minimum baseline requirements:

6.1.2.1 Only authorised personnel can view logging information.

6.1.2.2 Maintain the systems restrictions to modify or delete logging data within the specified retention period, after which it can be deleted.

6.1.2.3 Maintain the systems capability to protect audit information and audit tools (if present) from unauthorised access, modification, and deletion.

6.1.2.4 Maintain the systems capability for authorised humans and/or tools to access audit logs on a read-only basis.

6.1.2.5 Maintain the systems capability to allocate sufficient audit record storage capacity according to commonly recognised recommendations for log management and system configuration.

6.1.2.6 Maintain the systems capability to provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.

6.1.2.7 Maintain the systems capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure.

6.1.2.8 Maintain the systems capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

It should be noted that either overwriting the oldest audit records or halting audit log generation are possible responses to audit storage capacity being exceeded but imply the loss of potentially essential forensic information.

6.1.2.9 Implement and maintain procedures to securely extract, read and manage logging data.

Note: For safety critical and service critical systems, the following additional requirements shall apply:
6.1.2.10 Audit records on write once media.

6.1.3 Generating Alerts and Audit Records

TfL must ensure that data relating to potential security alerts is captured in the monitoring data and that alerts are triggered.

The system owner must maintain the following minimum baseline requirements:

6.1.3.1 Maintain the systems capability to generate audit records about events occurring in the system.

6.1.3.2 Audit records should be sufficient in detail to monitor the effectiveness and proper operation of the security mechanisms in place on the system.

6.1.3.3 Maintain the systems capability to generate audit records relevant to security for the following categories:

- Access control
- User activity
- Request errors
- Operating system (System, User and Security) events
- Control system events
- Use or attempts to use mobile devices
- Connection of unauthorised devices
- Backup and restore events
- Configuration changes
- Potential reconnaissance activity
- Audit log events
- Anti-malware events
- Boundary device logs
- FTP Logs
- Proxy Logs
- VPN Logs.

6.1.3.4 Maintain the systems capability to provide timestamps for use in audit record generation.

6.1.3.5 Individual audit records shall include:

- Timestamp
- Source (originating device, software process or human user account)
- Category
- Type
- Event ID
- Event result.

6.1.3.6 Alerts shall be resolved to individual assets.

6.1.3.7 Actions shall be attributed to a specific human user.

6.1.3.8 Alerts shall be generated on suspicious activity linked to known Indicators of Compromise.

6.1.3.9 Security logs shall be reviewed regularly and, if possible, alerts should be reviewed almost continuously, in real time.

6.1.3.10 Security alerts shall be prioritised, investigated and appropriate action taken.

Note: For safety critical and service critical systems, the following additional requirements shall apply:

6.1.3.11 Internal time synchronisation.

6.1.3.12 Protection of time source integrity.

6.1.3.13 Non-repudiation for all users.

6.1.4 Identifying Security Incidents

TfL must ensure that security alerts are contextualised with knowledge of the threat and the systems, to identify those security incidents that require some form of response.

The system owner must maintain the following minimum baseline requirements:

6.1.4.1 Updates for all signature based protective technologies are received at least once every 4 weeks.

6.1.4.2 Maintain the systems capability for updates to be implemented at least every 4 weeks.

6.1.4.3 Security issues from a recognised source of threat information shall be prioritised, investigated and appropriate action taken.

6.1.4.4 Security alerts shall be prioritised, investigated and appropriate action taken.

6.1.5 Monitoring Tools and Skills

TfL must ensure that monitoring staff skills, tools, and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they protect.

The system owner must maintain the following minimum baseline requirements:

6.1.5.1 Ensure the requirements for monitoring coverage (Section 6) and incident response (Section 7) are maintained, with appropriate tools and techniques either as handed over into live service or with appropriate replacements adopted through formal change control processes.

Consideration should be given to aligning these tools and techniques with other systems for a more consistent and coordinated approach.

6.1.5.2 There shall be personnel who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and system performance.

This could involve additional personnel to create additional capacity or require existing personnel to be updated on the new system.

6.1.5.3 There shall be defined roles and skills/competence requirements to ensure that monitoring personnel, together with other personnel such as operators, system

administrators and third parties, are able to cover all parts of the monitoring and investigation process.

6.1.5.4 There shall be up to date documentation to inform monitoring personnel which TfL services are supported by the assets being monitored so that alerts or investigations can be prioritised appropriately.

6.1.5.5 There shall be up to date documented processes, procedures, and workflows for monitoring personnel to follow for the analysis, investigation and reporting of alerts.

6.1.6 Incident Reporting

TfL must ensure that the reporting requirements for Cyber Security incidents are clearly articulated and understood to ensure that the right information is provided to the right people in a timely manner to allow incidents to be resolved effectively.

The system owner must implement and maintain reporting processes and procedures and ensure that the system can generate the information required, reporting at the first available opportunity, to meet the following minimum baseline reporting requirements:

6.1.6.1 The theft or unexplained loss of cyber systems or assets, asset data which an attacker could use to improve the chances of a successful attack or circumvent installed security measures.

6.1.6.2 The unauthorised physical or electronic access to cyber systems.

6.1.6.3 The compromise of a Cyber Assurance of Physical Security Systems (CAPSS) verified system protecting a Railway Asset.

6.1.6.4 The occurrence of successful or suspected attempted jamming of radio communication systems such as (but not limited to) mobile phones, portable credit/debit card payment systems, radios, Global Positioning System (GPS) radio navigation systems or Global System for Mobile Communications-Railway (GSM-R).

6.1.6.5 The unauthorised addition or modification of software or data on cyber systems.

6.1.6.6 The unauthorised destruction or disruption of software or data.

6.1.6.7 The malware infection of assets or attempted cyber intrusion.

6.1.6.8 The unauthorised physical access to secure rooms.

6.1.6.9 All incident reports must be made to the TfL Security Operations Centre at the earliest opportunity.

6.1.6.10 All incident reports relating to NIS systems must be made within 72 hours to the competent authority.

6.1.6.11 All Cyber Security Incidents must be accurately recorded and reported using the standard procedure and a consistent approach. This must include, but is not limited to:

a) Time and date of the Incident

b) Reference

c) Title

d) Point of contact/who reported the Incident

e) Brief description of the Incident

f) What systems and locations are affected

g) Updated comments

h) Actions taken and resolution notes

i) Resolution categories

j) All required information to ensure that all relevant data is captured to prevent this in future or to ensure that we are prepared next time.

6.1.6.12 All activities involved in a Cyber Security Incident shall be logged for later analysis.

6.1.6.13 All Cyber Security Incidents must be logged by Incident type (service) and symptom (service component) in order to ensure Incidents are correctly handled.

6.1.6.14 All Cyber Security Incidents must have clear set severity, impact and criticality levels to ensure they are dealt with appropriately.

SEV5	Critical Incident. Critical compromise, public affected. Multiple systems/devices affected or data breach. Major disruption or publicly displayed attack.
SEV4	Major Incident. Severe impact or compromise. Severe compromise, public affected. Multiple TfL devices/users affected or data breach. Major disruption or publicly displayed attack
SEV3	High Incident High impact or compromise. Multiple TfL devices/users affected. TfL users unable to work with job-dependant services
SEV2	Medium Incident Intermittent Incidents or Security Alerts, but not critical.
SEV1	Low Information or false positive. No security impact.

6.1.6.15 System owners and subject matter experts must support and co-operate with Cyber Security to ensure correct identification and response to Cyber Security Incidents.

6.1.6.16 Digital evidence must be preserved where possible during collection, storage and examination to help with Cyber Security Incident investigations.

7 Minimising the impact of Cyber Security incidents

The following controls will contribute to minimising the impact of a Cyber Security incident on TfL's OT and establish the minimum baseline of Cyber Security measures for operating and maintaining new or upgraded systems securely. Where possible, the minimum baseline Cyber Security measures should be adopted when operating or maintaining any OT supporting TfL services, recognising that legacy systems may not have been designed with these Cyber Security controls in place.

Safety critical and service critical systems will have been risk assessed at the design stage and are expected to require additional controls above the minimum baseline, for which suggestions are shown in the notes.

7.1 Incident response and recovery planning

TfL must be prepared to restore TfL services following disruption as a result of a cyber incident and must ensure that there are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure.

Mitigation activities designed to contain or limit the impact of compromise are also in place.

An incident response plan is the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against an organisation's information systems. Response should be measured first and foremost against the "service being provided," not just the system that was compromised.

7.1.1 Business Continuity Plan

TfL must ensure that new systems and upgrades are included in the Business Continuity Plan, which will identify procedures for maintaining and/or re-establishing essential business operations while recovering from a significant disruption.

The system owner must maintain the following minimum baseline requirements:

7.1.1.1 Recovery objectives shall be documented for the systems involved, based on business needs and reviewed annually.

7.1.1.2 The impact to TfL services because of significant disruption or system loss shall be documented and reviewed annually.

7.1.1.3 Continuity plans shall be maintained, at least annually, to ensure that business processes can be restored in accordance with recovery objectives.

7.1.1.4 The business continuity plan shall be updated, at least annually, to include any learning from experience (either exercise or real) or system/process changes.

7.1.1.5 Implement and maintain backup and restore procedures that support the business continuity plan.

7.1.2 Response and Recovery Plan

TfL must ensure that cyber incident response plans are updated with new and updated systems.

The system owner must maintain the following minimum baseline requirements:

7.1.2.1 Implement and maintain the overall cyber elements of an incident response plan or dedicated cyber incident response plan that identifies responsible personnel and defines actions to be performed by designated individuals shall be updated whenever personnel or roles change. The plan must document the actions to be taken in the event of a Cyber Security incident and those listed in Section 6.1.6.

7.1.2.2 The various types of OT incidents should be identified and classified as to potential impact so that a proper response can be formulated for each potential incident.

7.1.2.3 The systems and supporting technologies required to restore operations are known, documented and in line with TfL business continuity, disaster recovery and risk management processes.

7.1.2.4 The incident response plan shall be communicated to all appropriate organisations.

7.1.2.5 The response plan shall be tested at regular intervals, at least annually, to ensure the plan remains fit for purpose and that personnel involved understand their roles.

7.1.2.6 Implement and maintain procedures to support the activities as determined by the cyber elements of an incident response plan or dedicated cyber incident response plan. The procedures must document the actions to be taken in the event of a Cyber Security incident and those listed in Section 6.1.6.

7.1.2.7 Maintain offline and hardcopies of incident response plans and procedures.

7.1.3 System recovery

TfL must ensure that the system provides the capability to recover and reconstitute to a known secure state after a disruption or failure.

System recovery and reconstitution to a known secure state means that all system parameters (either default or configurable) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are re-established, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded and the system is fully tested and functional.

The system owner must maintain the following minimum baseline requirements:

7.1.3.1 The sequence in which systems, networks and supporting technologies are recovered to restore the systems supporting the delivery of TfL services shall be known, documented, and updated to reflect system changes through life.

7.1.3.2 The interdependencies between the systems and the supporting technologies shall be understood, documented, and updated to reflect system changes through life.

7.1.3.3 The capability to switch to and from an emergency power supply without affecting the existing security state or enter a documented degraded mode.

7.1.3.4 There may be instances where compensating countermeasures such as physical door access control may be affected by loss of base power supply, in which case the emergency power supply should cover those associated systems. If this is not possible, other compensating countermeasures may be needed during such an emergency situation.

7.2 Backups

TfL must ensure that there are accessible and secured current backups of data and information needed to recover network and information systems which support the TfL services.

TfL must ensure that there are backups of all systems, software, licenses, configurations, data, and other relevant information required to enable recovery of individual devices or entire networks and systems supporting the delivery of TfL services.

The system owner must maintain the following minimum baseline requirements for backups from Section 5.5.7.

7.3 Incident lessons learned

TfL must ensure that following an incident or exercise, a root cause analysis shall be conducted to identify measures to prevent reoccurrence based upon incident or exercise.

7.3.1 Lessons Learned

TfL must ensure that lessons are learned from any incident or exercise and that documentation and processes are updated to reflect those lessons.

The system owner must meet the following minimum baseline requirements:

7.3.1.1 The details of an identified incident shall be documented to record the incident, the response and the lessons learned.

7.3.1.2 Exercise scenarios should be undertaken to ensure that different aspects of the response plan are tested on a periodic, at least annual, basis and to ensure that the collective response team gain benefit from each successive exercise. Exercises must be considered as learning opportunities and lessons identified during exercise scenarios must be fed back into the response process.

7.3.1.3 System documentation and incident response processes shall be reviewed and updated following an incident or exercise.

8 Supporting Information

8.1 Background

Cyber Security should be considered as an integral part of any review for any OT and where possible should be integrated into existing safety, environmental, operational or risk considerations. This should reflect that cyber could be a potential cause of a failure and needs to be captured as part of the response or recovery process, rather than a separate consideration.

8.2 Customer Considerations

Whilst Cyber Security for OT should not be at the forefront of customer considerations, it should form part of the wider safe, secure and reliable message.

9 Guidance

For further advice and guidance in support of this standard, contact the Cyber Security team CyberSecurityGRC@tfl.gov.uk