Total Telecoms

Information Security Management System

17th Nov 2017

PROPRIETY INFORMATION NOTICE TO PERSONS RECEIVING THIS DOCUMENT

This document is the property of Total Telecoms and is delivered on the express condition that it is not to be disclosed, reproduced in whole or in part by anyone other than Total Telecoms, without its written consent: and that no right is granted to disclose or so use any information contained in said document. This restriction does not limit the right to use information obtained from another source.

This document contains a subset of Total Telecoms ISMS policies and forms.

Contents

Control of Records (ISMS 2.0)

1.0 Scope

All records created as part of complying with the requirements of the management system are controlled under this procedure. Documents which specify how the management system will work are controlled in line with ISMS 1.0.

2.0 Responsibilities

Owners are responsible for identifying the records that will be generated by the processes or assets for which they are responsible, or which should be generated to indicate conformity with the management system, and for ensuring that they are controlled in line with this procedure. Records must remain legible, readily identifiable and retrievable.

3.0 Procedure

3.1 Every record established under this procedure must be identified by means of a sticker which identifies the object as being a record within the ISMS. This sticker must identify Total Telecoms, the classification of the information contained in the record, the owner of the information and the date it was generated (or covers).

3.2 The existence of the record must be referenced in the procedure or work instruction which leads to its existence.

3.3 Where necessary, records can be given serial numbers in respect to the specific process to which they relate.

3.4 The retention period for the record is determined by overall approach to document and record retention.

3.5 Records are subject to the levels of protection appropriate to information of their classification level (i.e. at least the same as that of the asset to which they relate or the information they contain) and they are therefore protected, stored, maintained and disposed of in line with the requirements of the management system.

Network Service Level Agreement (ISMS 3.0)

1 Scope

All Servers, Routers, Firewalls, Switches or any other equipment used for networking and communications within Total Telecoms.

2.0 Responsibilities

The IT Director is responsible for ensuring all equipment is maintained and appropriately configured, that appropriate redundancy and failover measures are in place, and that procedures are in place to restore failed critical equipment to full working order within 4 hours.

3.0 Procedure

3.1 Total Telecoms guarantees 99.9% accessibility to all routing devices within the organisation's network.

3.2 Total Telecoms also guarantees 99.9% server uptime for all critical servers within the organisation's network.

4.0 Exclusions

Certain scenarios are beyond the control of Total Telecoms and therefore are not considered within the scope of this SLA.

4.1 Routine Maintenance: Total Telecoms may on occasion need to perform maintenance on network hardware, including servers and routing devices. This might include rebooting a server or routing a device, or temporarily suspending or restarting a service within a server. Such maintenance is quick and will be kept to a minimum to avoid interruptions to users. Where possible routine maintenance will be schedule at off peak times so as to provide minimum interruption.

4.2 Pre- Scheduled Maintenance: Total Telecoms may on occasion need to perform lengthier maintenance on its network hardware. This might involve installing software patches on a server, replacing memory and hard drives on a server, or replacing an entire server or network device. In the event this type of maintenance is required, Total Telecoms will pre-notify all users who will be affected by this outage and if possible schedule the maintenance to be performed at the quietest time of the week.

4.3 Malicious Attacks: Total Telecoms does many things to ensure the security of its network. There may however be certain situations in which an attack aimed at its network (such as Dedicated Denial of Service - DDoS) or other form of disabling activity outside of our control results in network interruption and/or service. In such a case, Total Telecoms will do everything possible to stop the attack and/or return the network to normal operating parameters, but we cannot offer a guaranteed resolution time.

Information Security Responsibilities Policy Statement (PCI 4.6)

All employees and contractors are responsible for the security of Total Telecoms information and must acknowledge that they have read and understood Total Telecoms information security policies and procedures.

Overall responsibility for information security is assigned to the IT Director.

1. IT Director is responsible for creating and distributing security policies and procedures.
2. IT Director is responsible for determining the scope of PCI DSS/Data Protection compliance initially and at least annually thereafter, taking into account PCI DSS/Data Protection guidance on Scope of Assessment for Compliance with PCI DSS/Data Protection Requirements.
3. IT Director is responsible for undertaking an annual formal risk assessment.
4. IT Director/IS Administrator is responsible for monitoring and analysing security alerts and distributing to appropriate information security and business unit management personnel.
5. IS Administrator is responsible for reviewing logs daily.
6. IT Director is responsible for the creation of system (including firewall and router) configuration standards and maintaining their accuracy.
7. IS Administrator is responsible for logical management of network components.
8. IS Administrator is responsible for testing security systems and processes, e.g. vulnerability scans, penetration testing, wireless device identification.
9. IT Director/IS Administrator is responsible for ensuring the network diagram is accurate.
10. IT Director is responsible for creating and distributing incident response and escalation procedures.
11. The HR Department is responsible for performing background checks on potential employees/staff, which includes screening of personnel who have access to confidential data or more than one card number at a time or who will have access to the cardholder data environment. Notify the IT Department when an employee’s contract is terminated, or when a new employee arrives.
12. Training Manager is responsible for employees’ training and awareness upon hire and at least annually.
13. IS Administrator is responsible for administering user account and authentication management.
14. IT Director/IS Administrator is responsible for monitoring and controlling all access to data.
15. IT Director is responsible for managing and monitoring the PCI DSS and Data Protection compliance of all associated third parties with whom cardholder/personal data is shared, ensuring they adhere to the PCI DSS/Data Protection requirements and contractually acknowledge that they are responsible for the security of cardholder/personal data which they possess.

Call Recordings Policy (PCI 5.2.1)

1.0 Scope

This policy applies to all Call Recordings containing cardholder data or personal data of any description which Total Telecoms is responsible for, or which it receives or processes for any reason.

2 Responsibilities

All employees involved in receiving, processing, storing or in any way using cardholder data or personal data are responsible for ensuring that these policy requirements are met.

3 Justification

Voice recordings in the contact centre are required for business reasons, such as agent training, quality control, regulatory requirements or confirmation of verbal contractual agreements.

It is a violation of PCI DSS requirement 3.2 to store any sensitive data, including card validation codes and values after authorisation even if encrypted.

It is therefore prohibitive to use any form of digital audio recording for storing CAV2, CVS2, CVV2 or CID code after authorisation if that data can be queried.

Where technology exists to prevent recording of these data elements, such technology should be enabled.

4 Procedure

4.1 Access to call recordings is restricted on a need-to-know basis.

4.2 Physical access to call recordings is restricted.

4.3 Call recordings should be retained for as little time as possible (PCI 15.2 – Data retention and disposal).

4.4 No cardholder data will be recorded. All Credit Card processing is completed through RealCredit (www.realcredit.com). RealCredit provide PCI-DSS Level 1 compliant card payment services.

4.5 Where RealCredit is not an option Pause & Resume is to be used to ensure no cardholder data is recorded.

Information Security/Data Protection Policy (PCI 5.1)

It is the policy of Total Telecoms to treat all data we obtain on behalf of us and our clients in a safe and secure manner. Notwithstanding, it must be recognised that all employees with access to client and consumer data treat all data with the same safety and security measures as outlined in this policy.

In compliance with the Data Protection Act 1988/Data Protection (Amendment) Act 2003/GDPR 2018; Total Telecoms will at all times respect the personal data kept by us by complying with the following provisions.

- We will obtain and process data in a fair, lawful and transparent manner.
- The data shall be recorded accurately and kept up to date where necessary.
- The data shall be kept only for lawful purposes.
- The data shall not be used or disclosed in any manner other than lawful purposes.
- The data shall be adequate, relevant and not excessive for the purposes for which it is required.
- The data shall not be kept for longer than is necessary.
- The data shall not be transferred outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of protection.

The appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure, destruction, accidental loss or destruction.

Data Security

In order to abide by the above Total Telecoms and its employees will adhere to the following points:

- All call recordings will be kept in a safe and secure manner and only accessible by a person of authority.
- All data relating to any client will be kept in a safe area accessible by a person of authority.
- All data relating to any consumer/customer must be disposed of in a safe manner (shredded).
- All diaries/journals/notebooks containing data shall be kept in secure area outside of working hours.
- No data shall be given to a third party without the consent of a person of authority or the owner of the data.

Abuse of Data

If an employee abuses data he/she may be subject to disciplinary action. An example would be disposing of customer information in a careless manner or divulging customer information to a third party.

Ultimately, abuse of data can lead to the termination of an individual’s employment following application of established procedures.

The Board of Directors and management of Total Telecoms, located at Unit 1, Waterfront Business Park, Little Island, Cork are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance (including compliance with PCI DSS and GPRD) and commercial image.

Information and information security requirements will continue to be aligned with organisational goals and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

Total Telecoms current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks (including those related to cardholder data, as set out in our cardholder data policy, PCI DOC 5) through the establishment and maintenance of an ISMS.

The risk assessment is a formal process that identifies threats and vulnerabilities, is reviewed quarterly (or whenever there are significant changes in assets or the risk environment) and this identifies how information-related risks are controlled.

Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, access control, application and system development security, operational security, network security, physical security, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, and information security incident reporting and response are fundamental to this policy. Control objectives for each of these areas are documented and are supported by specific, documented policies and procedures.

All employees of Total Telecoms and all vendors, contractors and business partners are expected to comply with this policy and with the policies and procedures that implement this policy. All employees, and certain external parties, will receive or be required to provide appropriate training.

The ISMS is subject to continuous, systematic review and improvement and this policy is reviewed at least annually and updated to reflect changes in business objectives and/or the risk environment.

Total Telecoms is committed compliance with PCI DSS, Data Protection Act 1988/Data Protection (Amendment) Act 2003/GDPR 2018.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan at least annually.

In this policy, **information security** is defined as:

preserving

This means that management, all full-time or part-time employees, sub-contractors, project consultants and any external partners or other parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts and within the PCI DSS Roles and Responsibilities document) to preserve information security, to protect cardholder data and personal data, to report security breaches (in line with the policy and procedures) and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in Data Protection Act 1988/Data Protection

(Amendment) Act 2003/GDPR 2018 disciplinary policy. All employees will receive information security awareness training and more specialised employees will receive appropriately specialised information security training.

*the **availability***

This means that information and associated assets should be accessible to authorised personnel when required and therefore physically secure. The computer network(s) must be resilient and Total Telecoms must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems, information and data. There must be appropriate business continuity plans.

confidentiality

This involves ensuring that information (including cardholder/personal data) is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to Total Telecoms information, proprietary knowledge and its systems including its network(s), website(s), extranet(s) and intranets.

*and **integrity***

This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorised modification, of either physical assets or electronic data other than as required in documented procedures for the protection of individual information or cardholder data. There must be appropriate contingency including for network(s), website(s), extranet(s)] and data back-up plans, and security incident reporting. Total Telecoms will comply with PCI DSS, Data Protection Act 1988/Data Protection (Amendment) Act 2003/GDPR 2018 and must comply with all relevant data-related legislation in those jurisdictions within which it operates.

*of the **physical (assets)***

The physical assets of Total Telecoms including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

*and **information assets***

The information assets include information and cardholder data printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, back-up tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, ‘data’ also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.).

*of **Total Telecoms***

Total Telecoms and such partners that are part of our integrated network and have signed up to our security policy and have accepted our ISMS.

The **ISMS** is the Information Security Management System, of which this policy, the Information Security Manual ('the Manual') and other supporting and related documentation are a part, and which has been designed to meet the requirements of PCI DSS v3.2, Data Protection Act 1988/Data Protection (Amendment) Act 2003/GDPR 2018.

The **Payment Card Industry (PCI) Data Security Standard (DSS)**, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The **PCI DSS** consists of 12 requirements, of which all requirements are addressed within individual policies and procedures;

1. Install and maintain a firewall configuration to protect cardholder data (PCI 10.19 - Firewall and Router Policy)
2. Do not use vendor-supplied defaults for system passwords and other security parameters (PCI 11.2 - Password Policy)
3. Protect stored cardholder data (PCI 5.0 - Cardholder Data Policy)
4. Encrypt transmission of cardholder data across open, public networks (PCI 12.2 – Key Management)
5. Use and regularly update anti-virus software (PCI 10.12 - Controls Against Malware)
6. Develop and maintain secure systems and applications (PCI 12.3 -Application & System Development Software)
7. Restrict access to cardholder data by business need-to-know (PCI 11.3 User Access Management)
8. Assign a unique ID to each person with computer access (PCI 11.7 Network Access Control Policy)
9. Restrict physical access to cardholder data (PCI 9.1 Physical Security Policy)
10. Track and monitor all access to network resources and cardholder data (PCI 10.18 Monitoring Procedure)
11. Regularly test security systems and processes (PCI 10.10 Testing Systems and Processes)
12. Maintain a policy that addresses information security (PCI 5.2 Information Security Policy)

A **SECURITY BREACH** is any incident or activity that causes or may cause a break-down in the availability, confidentiality or integrity of the physical or electronic information assets of Total Telecoms.

Managing Service Providers (PCI 6.8)

1.0 Scope

Total Telecoms does not currently share cardholder or personal data with external service providers (e.g. service providers for backup tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modelling purposes). If in the future Total Telecoms does share cardholder or personal with an external service provider then any external parties with whom Total Telecoms shares data are subject to this procedure.

2.0 Responsibilities

2.1 All relationship owners who are responsible for services provided by third party service providers are required to ensure that external parties have entered into a formal service provider agreement under this procedure which acknowledges that the service provider is responsible for the security of cardholder or personal data the service provider possesses.

2.2 Relationship owners are responsible for ensuring that service providers comply with PCI DSS, Data Protection Act 1988/Data Protection (Amendment) Act 2003/GDPR 2018 and that this compliance status is monitored at least annually.

2.3 The IT Director maintains a list of service providers with whom Total Telecoms has approved contracts.

3.0 Procedure

3.1 Where there is a business need for working with a service provider, Total Telecoms ensures that its cardholder and personal data security is not reduced; service providers are required to comply with PCI DSS, Data Protection Act 1988/Data Protection (Amendment) Act 2003/GDPR 2018.

3.2 Total Telecoms carries out due diligence to identify risks related to external party access.

3.3 The due diligence process identifies and documents, for each service;

a) The corporate status of the organization, including its registered address and related information;
b) The financial status of the organization, by means of a credit status check;
c) The performance of the organization, by means of at least two written references from existing customers;
d) The quality and security practices of the organization, by checking the validity of its current certificates to ISO/IEC 27001 (information security), ISO 9001 (quality management) and ISO/IEC 20000 (IT service management);
e) Details of court cases, complaints and any other issues that might be addressed by an extensive Google search.

Technology Usage Policy (PCI 7.2)

1.0 Scope

This policy applies to all usage of the following critical technology/ies: remote access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage.

2.0 Responsibilities

The IT Director is responsible for explicitly authorising the use of the above named critical technology (Item 1.0).

3.0 Procedure

a) Use of Item 1.0 technology must be authenticated with user ID and password or another authentication item (for example, token). If 2 factor authentication is available then (if reasonable) this authentication technique must be used.

b) The IT Director retains a list of all instances of the Item 1.0 technology and of the personnel authorised to use the technology.

c) All physical devices that fall into this category are labelled with details of their owner, contact information and purpose.

d) The acceptable uses of the Item 1.0 technology are as follows:

   a. Accessing or storing any form of electronic file, record or communication.
   b. Business Use Only.
   c. Employees are to use only the types of service for which they have been authorised.
   d. No user is allowed access to Item 1.0 technology using other user's credentials.
   e. Employees are not permitted to share credentials with anyone.

e) The Acceptable network locations for the Item 1.0 technologies is as follows:

   a. Total Telecoms –Unit 1, Waterfront Business Park, Little Island, Cork.

   b. Fairhill Business Centre, Killarney, Co. Kerry.

f) In respect of the Item 1.0 technologies, only the following company approved products may be used:

   a. See ISMS 7.4 – Company Approved Products.

g) Wherever the remote access technologies are deployed, sessions must be automatically disconnected after 15 minutes of inactivity.

h) Where required by vendors or business partners, remote access technologies may only be activated when needed by vendors and business partners, with immediate deactivation after use.

i) For personnel accessing cardholder or personal data via remote-access technologies, it is prohibited to copy, move, or store cardholder data onto local hard drives and removable electronic media, unless explicitly authorized by the IT Department.

j) Where proper authorisation has been given, cardholder or personal data must be protected in line with PCI DSS requirements as set out in these procedures.

Training Programme (PCI 8.0)

1.0 Scope

All individuals who will work with cardholder/personal data or have access to the cardholder/personal data environment are subject to this procedure.

2.0 Responsibilities

2.1 The Training Manager is responsible for planning the annual training programme and for ensuring this includes PCI DSS and data protection training.

2.2 Individual Directors, Managers and Team Leads are required to release their staff to undergo training as set out below.

3.0 Procedure

3.1 All individuals who will be allowed to access cardholder or personal data or the cardholder/personal data environment are required to attend PCI DSS and Data Protection security awareness training when they join Total Telecoms and, thereafter, at least annually.

3.2 This awareness training is provided by means of classroom training.

3.3 Records are retained of attendance at training courses. These records are in the form of classroom sign-in sheets and these records are stored in HR.

3.4 This security awareness programme provides multiple methods of training awareness – from e-learning and screensavers through memos, internal letters, and general briefings to wall posters.

3.5 All employees are required to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy (PCI 5.1).

Physical Security Policy (PCI 9.1)

Physical Security

1.0 Physical Security Perimeter

Total Telecoms uses security perimeters to protect areas that contain information, information processing facilities cardholder data and personal data.

2.0 Physical Entry Controls

2.1 Secure areas are protected by appropriate entry controls, lock and key, numeric key-pad and ID badge to ensure that only authorised personnel are allowed access.

2.2 Visitors are authorised, clearly distinguished by their badges from employees and forced to surrender their visitor identification badge on exit. Unbadged visitors are challenged and removed from secure areas.

2.3 A visitor log is maintained to record physical access to the facility as well as for computer rooms and data centres where cardholder/personal data is stored or transmitted. Logs are retained for a minimum of six months.

3.0 Securing offices, rooms and facilities

Total Telecoms has designed and applied physical security for buildings, offices, rooms and facilities.

4.0 Protecting against external and environmental threats

Total Telecoms has designed and applied physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or manmade disaster.

5.0 Working in Secure Areas

5.1 Total Telecoms has designed and applied physical protection and guidelines for working in secure areas.

5.2 CCTV Cameras or other access control mechanisms are used to monitor sensitive areas. Data from cameras/other mechanisms is stored for at least three months (ISMS 10.6 CCTV Policy).

5.3 Physical access to CCTV cameras, access control mechanisms, network jacks, wireless access points, gateways and handheld devices is restricted.

6.0 Public access, delivery and loading areas

Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises are controlled and isolated from information processing facilities to avoid unauthorised access.

Equipment Security

1.0 Equipment placement and protection

Equipment is sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

2.0 Supporting utilities

Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.

3.0 Cabling security

Power and telecommunications cabling carrying data or supporting information services is protected from interception or damage.

4.0 Equipment maintenance

Equipment is correctly maintained to ensure its continued availability and integrity.

5.0 Security of equipment off-premises

5.1 Security is applied to off-site equipment taking into account the different risks of working outside Total Telecoms premises. Disk encryption must be enabled on all equipment that is capable of supporting disk encryption technology.

5.2 Backup media must be stored in a secure location.

5.3 Backup media storage arrangements are reviewed annually to ensure they are still adequate.

6.0 Secure disposal or reuse of equipment

All items of equipment containing storage media are checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

i. Use secure containers to collect media for destruction.
ii. Cross-cut shred, incinerate, or pulp hardcopy materials so that cardholder/personal data cannot be reconstructed.
iii. Electronic media must be securely wiped, degaussed or physically destroyed.
iv. All media must be secured against loss or copying; this includes controls for physically securing all media (including but not limited to computers, removable electronic media,

7.0 Classification of media

7.1 All media are marked in line with the security classification of the information they carry. The protective marking scheme consists of 5 markings. In descending order of sensitivity, they are: Top Secret, Secret, Confidential, Restricted and Protect. Cardholder/personal data, user access and data and similar sensitive data are classified as confidential.

7.2 Media may only be distributed in line with their classification and to individuals authorised to receive them.

7.3 Media containing confidential information may only be communicated by secure means: by confidential courier.

8.0 Removal of property

8.1 Equipment, information or software may not be taken off site without prior authorisation.

8.2 Tracking information is recorded for all physical media that is taken off site. Tracking information is recorded in Media Asset Tracking Spreadsheet (ISMS 5.0). The IT Director is responsible for ensuring all data is recorded and maintained.

Testing Systems and Processes Procedure(PCI 10.10)

1.0 Scope

Systems, processes and software within Total Telecoms cardholder/personal data environment are in the scope of this policy.

2.0 Responsibilities

The IT Director is responsible for ensuring the procedures documented here are adhered to.

3.0 Procedure

3.1 The IS Administrator is responsible for testing for the presence of wireless access points by using a wireless analyser '*Confidential*' on a quarterly basis. This testing will detect and identify WLAN card inserted into system components, portable wireless devices connected to system components (for example, by USB, etc.) and wireless devices attached to a network port or network device. Unauthorised wireless devices are immediately reported to the IT Director, are removed and those responsible for their installation may be subject to the organisation's disciplinary policy.

3.2 Internal and external network vulnerability scans are undertaken at least quarterly and following significant changes (e.g. new system component installations, changes in network topology, firewall rule modifications, and product upgrades) in the network.

External vulnerability scans are undertaken quarterly by '*Confidential*'.

Internal scans are undertaken quarterly by IS Administrator with the use of software tools including:

- '*Confidential*'
- '*Confidential*'
- '*Confidential*'
- '*Confidential*'

If the scans do not produce passing results (failures scored greater than a 4.0 by the CVSS), remediation work is undertaken followed by rescans until passing results are obtained and all 'High' vulnerabilities have been closed down.

3.3 Intrusion Detection systems (IDS) and/or Intrusion Prevention systems (IPS)- '*Confidential*' are in use to monitor all traffic in the data environment and alert IT personnel to suspected compromises. IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.

3.4 File-integrity monitoring software ('*Confidential*') is deployed within the data environment to alert IT personnel to unauthorised modification of critical system files, configuration files, or content files including system executables, application executables, configuration and parameter files, centrally stored, historical or archived, log and audit files. The software is configured to perform critical file comparisons at least weekly.

Controls against malware (PCI 10.12)

1.0 Scope

All Total Telecoms information assets, including hardware, software, mobile devices and peripherals including memory devices, PDAs, mobile phones and all employees, contractors, temporary workers and third parties who use, work with or connect to organisational information processing facilities are within the scope of this procedure.

2.0 Responsibilities

2.1 The IT Director is responsible for monitoring software and systems for breaches of the anti-malware policy or this procedure.

2.2 The IT Director is responsible for the installation and maintenance of Total Telecoms selected anti-malware software, and for the configuration of firewall(s) and gateway(s) as well as for ensuring that the IT Department have adequate technical training and skills to carry out assigned tasks under this procedure.

3.0 Procedure in respect of malware

3.1 The anti-malware software is capable of detecting all known forms of malware, including viruses, Trojans, worms, spyware, adware, and rootkits.

3.2 The anti-malware software is installed on all organisational information systems and devices, including workstations, laptops, servers, gateways and firewalls, and is configured with automatic updating in respect of the software and the virus definitions, and to carry out regular scans of the network environment.

3.3 The anti-malware software generates an audit log which is stored in line with the requirements of PCI 10.18.

Monitoring Procedure (PCI 10.18)

1.0 Scope

This procedure is applicable to all system components within the cardholder/personal data environment.

2.0 Responsibilities

The IS Administrator within Total Telecoms is responsible for monitoring all activities within the cardholder/personal data environment.

3.0 Procedure

3.1 Total Telecoms uses *'Confidential'* to meet the criteria set out within the procedures.

3.2 Automated audit trails are implemented and active on all system components to reconstruct the following events:

- All individual accesses to cardholder/personal data
- All actions taken by any individual with root or administrative privileges
- Access to audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialisation of the audit logs
- Creation and deletion of system-level objects.

3.3 For all events (defined above) the following audit trail events are recorded:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource.

3.4 All critical system clocks and times are synchronised using Windows Time Service and NTP. Specific procedures for obtaining time are as follows: Domain Controller obtains its time from external source ie.pool.ntp.org using NTP, Other servers and workstations in the Domain synchronise time with the Domain Controller using Windows Time Services. Any device that is not Active Directory aware obtains its time from ie.ntp.org using NTP.

3.5 Time data is protected and sources of time updates are also secured via Group Policy.

3.6 Only those with a job-related need are authorised to view audit files.

3.7 Audit trail files are protected from unauthorised modifications via access control mechanisms.

3.8 Audit trail files are promptly backed up to a centralised log server.

3.9 Logs from external-facing technologies are offloaded to the centralised log server.

3.10 The Network Administrator is responsible for reviewing logs for all system components on a daily basis; any exceptions are followed-up.

3.11 File-integrity monitoring/change-detection software is used on logs to ensure that existing log data cannot be changed without generating alerts.

3.12 Audit trail history is retained for 12 months, with a minimum of three months immediately available for analysis.

Firewall and Router Policy (PCI 10.19)

1.0 Scope

All firewalls and routers within, or connected to, Total Telecoms network.

2.0 Responsibilities

The IS Administrator is responsible for the configuration and maintenance of Total Telecoms firewall and routers and as further described in 3.8 below. The IT Manager is responsible for approving configuration changes to firewall and routers.

3.0 Requirements

3.1 Firewall locations

A firewall is required and is present at each internet connection and between any demilitarised zone (DMZ) and the internal network. Perimeter firewalls are installed between any wireless networks and the cardholder/personal data environment. These firewalls are identified on the current network diagram (see 3.7 below). These firewalls are configured to deny, or control, any traffic (which has a valid business justification) from the wireless environment into the cardholder/personal data environment.

3.2 Firewall & router configuration

3.2.1 Firewalls are configured, on the basis of the scope assessment and the analysis of cardholder/personal data flows, to restrict inbound and outbound traffic to that which is necessary for the cardholder/personal data environment and to restrict connections between un-trusted networks and system components. All other inbound/outbound traffic is specifically denied, e.g. using an explicit ‘deny all’.

3.2.2 Firewall and router configuration files are secured and synchronised, in that running configuration files and startup configuration files (used during reboot), have the same, secure configuration.

3.2.3 The firewall performs stateful inspection (dynamic packet filtering), ensuring only established connections are allowed into the network.

3.2.4 IP masquerading is implemented on all firewalls and routers to prevent internal addresses from being translated and revealed on the Internet, e.g. Network Address Translation (NAT).

3.3 Changes to firewall & router configurations

All proposed changes to network connections, and to firewall and router configurations, must be approved in advance. The request for any changes must be made by submitting ISMS 10.2 (Rule set for Boundary Router) via email to the IT Manager and these requests must describe clearly the current configuration, the proposed change, the business or technical reason for making the change, and the means by which the change will be tested to ensure that adequate security is maintained. The IT Manager will maintain incoming email requests and outgoing approvals or rejections in separate email folders. The IT Manager is responsible for maintaining records of all tests carried out to ensure that changes have not reduced required security.

3.4 Permitted Services, Protocols and Ports

Total Telecoms maintains firewall and router configurations which list services, protocols and ports necessary for business PCI 10.4 (Firewall Configuration and Control). Justification is provided for each permitted service/protocol/port. If insecure services/protocols/ports are necessary (e.g. FTP), security features are documented.

3.5 Demilitarised Zone (DMZ) requirement

- A DMZ is implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment. The following security measures are enforced to provide security to cardholder data:
- Inbound Internet traffic is limited to IP addresses within the DMZ.
- Direct routes inbound or outbound between the Internet and the cardholder data environment are not permitted.
- Internal addresses cannot pass from the Internet into the DMZ.
- Outbound traffic from the cardholder data environment to the Internet is restricted, such that outbound traffic can only access IP addresses within the DMZ (or, outbound traffic is explicitly authorised).
- The database (containing cardholder data) is segregated from the DMZ and is placed within the internal network zone.

3.6 Personal firewall software

Mobile and/or employee-owned computers with direct connectivity to the Internet, and which are used to access Total Telecoms network have personal firewall software installed which is active and is configured by Total Telecoms to specific standards and is not alterable by mobile computer users.

3.7 Network Diagram

Network diagrams ISMI 5 (Total Telecoms Network Diagram) remain current and identify all cardholder/personal data flows over the network, specifically detailing all connections to cardholder/personal data and showing all firewalls (including wireless connections).

3.8 Roles and Responsibilities

Total Telecoms IS Administrator is responsible for the logical management of network components.

Specific tasks include:

- Maintenance of the network diagram.
- Changes to firewalls and routers are requested and authorised by the IT Manager.
- Configuration of devices, including documenting permitted protocols and services.
- Ensuring the requirement that there is a review of firewall and router rule sets, at least every six months.
- Undertaking daily monitoring of logs from devices.

System Configuration Procedure (PCI 10.21)

1.0 Scope

All system components within, or connected to, Total Telecoms cardholder/personal data environment are within the scope of these procedures.

2.0 Responsibilities

The IS Administrator is responsible for the configuration and maintenance of Total Telecoms system components and for ensuring that these requirements are met during the configuration of all system components.

3.0 Requirements

3.1 Prior to installing a system on the network, all vendor-supplied defaults (including but not limited to passwords, simple network management protocol (SNMP), and community strings) are changed and unnecessary accounts eliminated.

3.2 Wireless environments have the following measures implemented on all wireless devices:

- Wireless devices cannot (under any circumstances) be allowed access to the cardholder/personal data environment. Wireless access devices must be installed on a completely separate network segment.
- Vendor defaults changed, including encryption keys, passwords/passphrases and SNMP community strings.
- Once an individual, who had knowledge of the keys, leaves Total Telecoms, these keys are immediately changed.
- Firmware is updated to support strong encryption for authentication and transmission (e.g. WPA2).

3.3 Configuration standards have been developed for all systems.

3.4 These configuration standards are updated as new vulnerabilities are identified as reflected in the publication of a revised industry standard.

3.5 System configuration standards are applied whenever new systems are configured.

3.6 Only one primary function per server is implemented. Total Telecoms has addressed server functions to ensure those which require different security levels, or that may introduce security weaknesses to other functions are not present upon the same server.

3.7 Where virtualization technologies are used, only one primary function is implemented per virtual system component or device.

3.8 All unnecessary and insecure services, protocols & daemons are disabled, or if required for business purposes, are justified and documented as to the appropriate use of the service within the specific configuration standard and appropriate security features (technologies such as SSH, SFTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP) have been identified, documented and implemented.

3.9 Common security parameter settings are included in the system configuration standards, and system administrators are required to have knowledge of these common settings.

3.10 All unnecessary functionality, including scripts, drivers, features, subsystems, file systems, and unnecessary web servers are removed from system components.

3.11 All non-console administrative access to systems is encrypted using Network Level Authentication or SSL/TLS.

3.12 Where Total Telecoms uses shared hosting providers, it ensures that these providers protect Total Telecoms hosted environment and cardholder/personal data in line with the specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.

Access Control Policy (PCI 11.1)

1. Total Telecoms controls access to information on the basis of business and security requirements, including the PCI DSS.

2. Access control rules and rights to applications, expressed in standard user profiles, for each user are clearly stated, together with the business requirements met by the controls.

3. The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.

4. The access rights to each application take into account:

    a. The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the systems and network(s).

    b. Data protection and privacy legislation, Total Telecoms statutory objectives and contractual commitments (including the PCI DSS) regarding access to data (including cardholder data) or services.

    c. The 'need to know' principle (i.e. access is granted at the minimum level necessary for the role).

    d. The principle that 'everything is generally forbidden unless expressly permitted' (set to 'deny all').

    e. Rules, that must always be enforced, are distinguished from guidelines that are not always enforced.

    f. Prohibit user-initiated changes to user permissions.

    g. Enforce rules that require specific permission before enactment.

    h. Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

5. Total Telecoms has standard user access profiles for common roles in the organisation.

6. Access rights are consistently managed across the network(s).

7. User access requests and changes to access rights are subject to formal authorisation, to periodic review and to deletion, all in line with documented procedures.

8. Changes to user accounts are logged and the logs are subject to quarterly review by the IT Manager.

Access Management (PCI 11.3)

1.0 Scope

The access rights of all users/user groups to cardholder/personal data or to any of Total Telecoms information assets, systems or services are managed in accordance with this procedure. Total Telecoms operates a single sign-on process using Microsoft Active Directory. The access control system must have a default ‘deny-all’ setting.

2.0 Responsibilities

The IS Administrator is responsible for administration of allocated and authorised user/user group access rights in conformity with the policy.

The Head of HR is responsible for initiation and administration of new and changed user access requests (User Agreements) and user training.

Directors, Managers and Team Leaders are responsible for authorising access requests as being in line with business and organisational security policy and procedure.

Asset owners are responsible for authorising access requests to their information assets as being in conformity with the security requirements of the asset.

The IT Manager is responsible for reviewing user access rights in line with the review requirements of the ISMS.

3.0 Requirements

3.1 User registration and deregistration

3.1.1 Every user has their own individual user ID.

3.1.2 User Agreements contain statements of access rights and statements indicating that users have understood and accepted the conditions of access.

3.1.3 Every user proposed access right is documented in a User Agreement, which details the cardholder data/systems/services/applications/information assets to which access is to be granted, together with the level of access that is to be granted, taking into account the Access Control Policy (PCI 11.1) and the standard user profiles. If a user is to be granted access rights other than the standard ones, then the specific additional authorisation of the IT Manager is also required.

3.1.4 The Manager and the system/asset owner authorise access to the system/asset.

3.1.5 The User Agreement is then signed by the user and passed to the IT Manager and the username/user ID is created and administered.

3.1.6 The IT Department maintains a list of authorised users, administers changes in access rights and removes users.

3.1.7 The disciplinary policy will be invoked in cases of attempted unauthorised access.

3.2 Privilege management

3.2.1 Privileges are allocated to a different username than that allocated for normal use and are assigned on the basis of the individual's role/job classification and function.

3.2.2 The available access privileges for each of Total Telecoms operating systems, applications and other systems are documented.

3.2.3 Privileges are allocated on a least privilege, need-to-use and event-by-event basis; the request for allocation of a privilege is initiated in an e-mail from the user concerned to the IT Manager which sets out the specific privilege required, the reasons why the privilege is required and the length of time for which it is required.

3.2.4 Access controls are implemented via an automated access control system Microsoft Active Directory.

3.2.5 The IT Manager retains a log of all privileges authorised and allocated and checks on a quarterly basis that they have been de-activated as specified in the original request.

3.2.6 The IT Manager checks via the log management system on a monthly basis that unauthorised privileges have not been obtained.

3.3 Password management

3.3.1 The allocation of passwords is formally controlled and all staff are informed about authentication procedures as part of their User Agreement (PCI 11.4, Individual user agreement).

3.3.2 Access authorisation and user password responsibilities are documented in signed User Agreements (PCI 11.4), which are also used to record modification of user rights and eventual deletion of the user.

3.3.3 User passwords are unique and are initially issued with a unique temporary password which users are forced to change at first logon. These passwords are issued via the Active Directory user manager.

3.3.4 Group, shared, or generic accounts and passwords are strictly prohibited.

3.3.5 Password changes every 90 days are enforced, re-use of passwords is prohibited for 24 subsequent attempts, and seven-character alphanumeric passwords are required. Password must meet the standard Microsoft Active Directory complexity requirements.

3.3.6 Repeated access attempts are limited by locking out the user ID after not more than six attempts. The lockout duration is set to thirty minutes or until an administrator enables the user ID.

3.3.7 If a session has been idle for more than 10 minutes, the user must re-enter their password to reactivate the terminal.

3.3.8 Users who need to be issued with a replacement password must first obtain the written authorisation of their Manager who is required to confirm the identity of the user; this written authorisation must be presented to the IT Department before a new unique temporary password can be issued.

3.3.9 Passwords are stored on the Domain Controller, are stored separately from application system data and are protected by Hashing.

3.3.10 Remote access to the network is by means of two-factor authentication or secure VPN.

3.3.11 The default passwords on all new equipment are changed to conform with the Total Telecoms password requirements before the equipment is brought into service.

3.3.12 Access rights are terminated immediately for individuals whose employment is terminated. HR is responsible for informing the IT Department when an individual leaves the organisation. This is done by emailing a copy of ISMS 6 (Employee termination form) to the IT Manager.

3.3.13 If an account has been inactive for 90 days, the account is terminated.

3.3.14 Vendors are only allowed to access specific systems for specific, pre-agreed time periods.

3.3.15 Access to any database containing cardholder/personal data must be authenticated, queries of, and user actions on (for example, move, copy, delete), the database are allowed through programmatic methods only, and database and application configuration settings restrict user direct access or queries to databases to database administrators only.

3.4 Review of access rights

3.4.1 Access rights are reviewed annually and their adequacy is confirmed; any changes that need to take place are actioned.

3.4.2 User access rights are reviewed when a user’s role or location within Total Telecoms changes in any way. If the access rights need to change, a new user agreement is issued, in line with this procedure, setting out those access rights.

Network Access Control Policy (PCI 11.7)

Total Telecoms protects its networked services from unauthorised access, ensuring that appropriate interfaces are in place between Total Telecoms network, any external third party network, the Internet and that appropriate authentication mechanisms are applied for users and equipment and that control of user access to information services is enforced.

1. The networks and network services, and their access rights, which are allowed to be accessed, are detailed.

2. Authorisation procedures are used to ensure that users only have access to those services and networks which are appropriate for their role and to their business needs.

3. Management controls and procedures are used to protect access to network connections and network services.

4. There are specific procedures for controlling access to network services.

5. As a minimum, the following security steps are required in respect of wireless technology, modems and routers used in respect of any part of an organisational network on which cardholder/personal data is processed:

    a. Such equipment may only be purchased from approved vendors and in line with approved types and models
    b. Explicit management authorisation is required prior to deployment of all such equipment
    c. User authentication is required before any user or service can connect to the network
    d. For every such device, there must be an approved list of users and services that have authorised access to the device, and this list must be maintained
    e. Each such device must be clearly labelled with contact details and name of the owner of the device, and its purpose must be also be marked on it
    f. Each such device may only be used for the purposes and in the location for which authorisation was obtained
    g. Remote-access technologies must automatically disconnect after a 15 minute period of inactivity
    h. Remote-access technologies for vendors may only be activated when specifically required and must be de-activated immediately after use;
    i. When accessing cardholder/personal data via remote-access technologies, cardholder data may not be copied, moved, or stored onto local hard drives, removable computer media or external media
    j. Implement two-factor authentication or secure VPN for remote access to the network by employees, administrators, and third parties.

Responding to Information Security Incidents (PCI 13.2)

1.0 Scope

All reports of information security weaknesses or events relating to any of Total Telecoms information assets and events that should have been reported but were not are within the scope of this procedure. In addition, any events or weaknesses detected through monitoring systems, alerting systems, security systems, intrusion systems and prevention systems fall within the scope of this procedure.

2.0 Responsibilities

2.1 Users are required to report information security weaknesses and events to the IT Manager.

2.2 Owners of monitoring and alert services are responsible for reporting those events (or sequences of events) that fall within the scope of this procedure.

2.3 The IT Manager is responsible for coordinating and managing the response to any reported weakness or event, including documentation of all emergency steps taken, evidence collection, and closing out the event, as well as for ensuring that the plan is modified in the light of experience and lessons learned and to incorporate security industry developments and changes.

2.3 The IT Manager is responsible for communication and contact strategies in the event of a compromise including notification of the payment brands.

2.4 All technical staff and other employees, contractors or third parties, are required to support the IT Manager in dealing with an event or weakness.

2.5 The IT Manager authorises access to live systems or data. Asset owners carry out actual accesses to live systems or data in dealing with an incident.

2.6 The IT Manager is responsible for the contingency planning components of the Working Instructions identified in 3.5 below, and for ensuring that this incident response plan is tested at least annually.

2.7 The Training Manager is responsible for providing whatever training is necessary for all employees with responsibilities under this procedure to carry them out. Specifically, those staff with designated responsibilities in terms of the 24/7 incident response must have thorough training that enables them to provide the required service effectively.

3.0 Procedure

3.1 A 24/7 incident response service is available. The incident response service is available for 24/7 incident response and monitoring coverage for any evidence of unauthorised activity, detection of unauthorised wireless access points, critical IDS alerts, and/or reports of unauthorised critical system or content file changes.

3.2 The IT Director logs all information security reports immediately upon receipt, allocating to each a unique number and uses this log to ensure that all reports are analysed and closed out.

3.3 All information security events and weaknesses are, immediately upon receipt, assessed and categorised, with reasons, by the IT Manager. Initially, there are four categories: events, weaknesses, incidents and unknowns. ‘Events’ are occurrences that, after analysis, have no or very minor importance for information security; ‘vulnerabilities’ are weaknesses that, after analysis, clearly exist as significant weaknesses compromising information security; ‘incidents’ are occurrences of events (series of events) that have a significant probability of compromising Total Telecoms information security; ‘unknowns’ are those reported events or weaknesses that, after initial analysis, are still not capable of allocation to one of the four categories. The ‘unknowns’ are subject to further analysis to allocate them to one of the other three categories as soon as possible.

3.4 The prioritisation for responses, when there are multiple event reports to deal with, is: incidents, unknowns, vulnerabilities, events. When there are multiple event reports in each category, the IT Manager prioritises responses in the light of the criticality of the business systems and information assets at risk, the danger of further compromise to Total Telecoms information security, and the resources at his disposal. Incidents involving high-value or business critical systems are immediately reported by the IT Manager.

3.5 If systems containing cardholder/personal data are compromised, this matter is to be immediately reported to the acquirer/payment card brands or Clients. Visa’s Incident response procedures are as follows:

- Contact Visa immediately
- Do not access or alter compromised systems, i.e. do not log on, or change passwords
- Do not turn the compromised systems off. Instead, isolate them from your network and unplug any network cables
- Preserve all logs and similar electronic evidence
- Perform a back-up of your systems to preserve their current state – this will also facilitate any subsequent investigations
- Log all actions taken.
- Specific work instructions set out the necessary containment and corrective action and standing contingency plans in respect of the following types of information security incident:
    - Systems failure and loss of service
    - Malware, including viruses
    - Denial of service
    - Errors resulting from poor data
    - Breaches of confidentiality
    - Breaches of information integrity
    - Misuse of information systems
    - Non-standard incidents.
    - The contingency plans include:
    - Business recovery procedures
    - Disaster recovery procedures
    - Data backup procedures.

3.6 The IT Manager seeks additional input from qualified technical staff, as necessary and where he considers the standing instructions to be inadequate, to analyse and understand the incident and to identify appropriate actions to contain it and to implement contingency plans.

3.7 The IT Manager invokes actions as set out in the standing work instructions plus additional activity that he considers necessary to contain and recover from the incident, and to implement contingency plans. Where necessary, the IT Manager coordinates activity with other organisations and for informing credit card companies, clients and other relevant authorities. The IT Manager confirms that the affected business systems have been restored and that the required controls are operational before authorising a return to normal working.

3.8 Once the incident is contained, and the required corrective action is completed, the IT Manager reports to the Managing Director with a summary of the incident, identifying the cause of the incident and analysing its progress, trying to identify how Total Telecoms could have responded earlier or more effectively, or preventative action that might have been taken in advance of the information, the effectiveness of the containment and corrective actions and the contingency plans, and how the incident was closed out (see 3.9 below).

3.9 The IT Manager is responsible for closing out the incident: this includes any reports to external authorities; analysis of legal requirements for reporting compromises/incidents, initiating disciplinary action by referring the incident to the Head of HR; planning and implementing preventative action to avoid any further recurrence; collecting and securing audit trails and forensic evidence; initiating any action for compensation from software, service or outsource suppliers, and communicating with those affected by or involved in the incident about returning to normal working and any other issues.

3.10 The IT Manager prepares a quarterly report which identifies (from the event reporting log) the number, type, category and severity of information security incidents during the preceding months, the cost of containment and recovery, and the total cost of the losses arising from each incident, and recommends (where appropriate) additional controls that might limit the frequency of information security incidents, improve Total Telecoms ability to respond, and reduce the cost of response.

3.11 All the incident reports from the period since the last management review are taken into account at the next one, to ensure that Total Telecoms learns from the incidents and that the incident response plan itself is improved on a continuous basis.

Retention and Disposal Policy (PCI 15.2)

1.0 Scope

This policy applies to all storage and disposal of cardholder/personal data within Total Telecoms, of which retention must be limited to that which is required for business, legal, and/or regulatory purposes.

2.0 Responsibilities

All employees are responsible for ensuring this policy is abided to, deviations from this policy should be reported to the IT Manager.

3.0 Requirements

3.1 Storage of cardholder/personal data is kept to a minimum in line with legal, regulatory, and business requirements.

3.2 Sensitive authentication data is not stored post authorisation. Sensitive authentication data consists of either the full contents of track 1 or 2, the card verification code or value, or the personal identification number (PIN) or encrypted PIN block.

3.3 Data retention periods are determined by reference to specific legal or contractual requirements. Data is securely disposed of when its identified retention period is completed, in line with the table below:

Type of data	Retention Period	Disposal Process
e.g. Electronic storage on database	e.g. 2 years (regulatory reasons)	Programmatic (automatic) process to remove, at least on a quarterly basis, data that exceeds business retention requirements / or / reviews conducted at least on a quarterly basis
e.g. Hardcopy data (receipts/faxes)	2 Years	Cross-cut shredded
e.g. Hard drives (back-up)	3 Years	Secure wipe program/degauss
e.g. Tape Media (back-up)	3 Years	Physically destroy
e.g. System and network logs	At least one year	-

3.4 On at least a quarterly basis, the organisation systematically removes and destroys all cardholder/personal data that has exceeded its retention period, and to review and ensure remaining stored cardholder/personal data to ensure that it remains within the formal retention requirements.

3.5 Wherever the PAN is stored, whether electronic or on paper, it is masked. The first six and last four digits are the maximum number of digits that may be displayed.

3.6 Wherever the PAN is stored (including in logs, removable media, etc), it is made unreadable by means of cryptography.

3.7 Cardholder/personal data is never stored on removable media OR where cardholder/personal data is stored on removable media and is protected by means of disk encryption, logical access is managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys are not tied to user accounts.

3.8 When removable physical storage media (including documents, faxes, and electronic media) are no longer required (i.e. they have passed their retention periods), they are destroyed as set out in PCI 9.1.

CCTV Policy (ISMS 10.6)

1.0 Scope

This policy applies to the operation and management of CCTV by Total Telecoms in the following location;

- Unit 1, Waterfront Business Park, Little Island, Cork.

2.0 Purpose

2.1 CCTV equipment has been installed to maintain the security of Total Telecoms locations. It is intended to act as a deterrent to unauthorised access and may also be used to assist in any investigation where unauthorised access has occurred.

2.2 CCTV equipment has been installed to assist in enforcing health and safety standards. It is intended to act as a deterrent to any individual acting in a dangerous or reckless manner that could endanger either themselves or others and may also be used to investigate any injury that occurs.

2.3 CCTV equipment has been installed to assist in the prevention and investigation of illegal activity occurring at Total Telecoms locations. This includes theft, violence, damage of property and any other illegal activity.

2.4 CCTV equipment will NOT be used for the day-to-day monitoring of any individual. However, in the event of a dispute, Total Telecoms reserves the right to review CCTV footage if it will assist in resolving said dispute.

3.0 Storage

3.1 All recordings are stored in a physically secure location.

3.2 Access to recording software is password protected and only accessible to authorised individuals and only for the purposes outlined above.

4.0 Location

All cameras are clearly visible and there are no concealed cameras in operation in any Total Telecoms locations. Signage has also been put in place to advise employees and visitors that a CCTV system is in operation.

Document Owner and Approval

The IT Director is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the management system.

A current version of this document is available to all members of staff on the corporate intranet.

This procedure was approved by the Managing Director on 17th-Nov-2017 and is issued on a version controlled basis under his/her signature.

Signature: **Date:**