DigiPlex Group Information Security Management Manual

Document Number:	Revision:	Issue Date:	Owner
IT-MAN-01-00-DGS	C	September 2018	ICT Director

1.0 Introduction

This Information Security Management Manual defines the aims, objectives, policy and the documentary framework, of the Information Security Management System within the DigiPlex Group.

1.1 Scope

The Scope of this Manual applies to all activities, departments and site locations within DigiPlex . It is the principal document that defines the Information Security Management System in support of Group Policy and describes the mechanisms for achieving these objectives. The Scoping Document, IT-POL-03-00-DGS, further defines the scope.

This Document sets out the Information Security Management Policy and viewpoint of DigiPlex Group and is supported by a Management System with a collection of procedures. Each Site within DigiPlex Group may support this Manual with additional site specific plans, procedures, work instructions as appropriate.

2.0 Objective

The objective of information security management is to ensure that information that has a commercial or personal value:

- is protected against unauthorised access or disclosure
- maintains its integrity
- remains available to authorised users
- is correct and up-to-date

It is DigiPlex's objective to protect its critical information assets and personal data from all threats, whether internal or external, deliberate or accidental. This objective supports the Group's business objectives, legislative and customer requirements.

DigiPlex will regularly identify and assess the risks associated with all our information resources including personal data and take appropriate action to prevent, or reduce the impact of, events that could affect the achievement of our business objectives.

DigiPlex will comply with applicable security requirements relating to the protection of information, personal data and equipment covered by legislative, customer or third party restrictions.

DigiPlex will demonstrate achievement of the individual components of this Policy document through the preparation of documented procedures, the reporting and review of information security at all levels of the business and a monitoring and audit programme to ensure that the processes are being implemented.

3.0 Principles

In all business areas, the Site Managers and the IT will carry out information security risk assessments regularly, record the findings and take appropriate management actions in a timely fashion. In particular, the following activities will be undertaken:

- threat assessment performed on all information types

- assessment of the sensitivity of information held or handled
- assessment of risks at all locations where information is created, stored or handled including customer and company premises, home offices and mobile systems
- regular review and update of information system vulnerabilities
- preparation of contingency plans for high risks
- early identification of emerging risks and initiation of risk reduction or mitigation action.
- National Threat Assessment
- Cyber Assessments published by CERT or equivalent

A threat is a force, organisation or person that seeks to gain access to, or compromise, information. A threat can be assessed in terms of the probability of an attack and by looking at the nature of the threat, its capability and technical resources. The threat to security should be addressed under the following headings:

- National Threat Assessment
- Cyber Threat Reports
- hardware theft
- failure or interruption of vital services
- system overloads
- misuse of system resources by authorised users
- hardware or software malfunction
- computer hackers or fortuitous access
- failure to dispose of paper or other information-containing media in a secure fashion
- overhearing of telephone conversations
- espionage (commercial, economic, journalistic, criminal)
- environmental contamination
- natural disasters and acts of war
- pressure groups, saboteurs and terrorist organisations.

The vulnerability of a system or facility holding information is its weaknesses that may result in loss, damage or disclosure of information assets. Vulnerability can be assessed in terms of the means by which the weakness could be exploited.

The sensitivity of information is a subjective judgement of its value. "Confidential" and "Highly Sensitive" information must be clearly identified, marked and protected in accordance with its sensitivity.

Impact of loss is a measure of the effect or cost in the information was disclosed, lost or made unavailable or untrustworthy.

4.0 Commitment

DigiPlex is committed to continually:

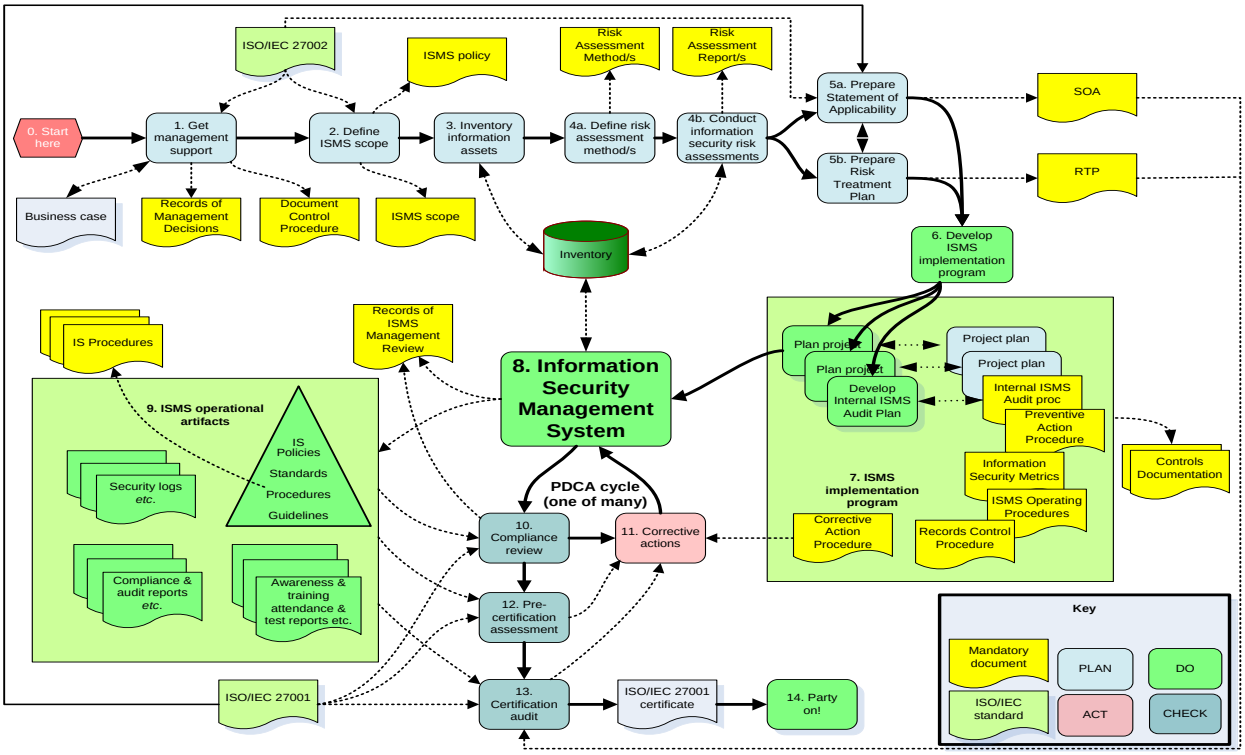
- Developing a framework to implementing, maintaining, monitoring and improving security including the structure of risk and risk management.
- Establish and measure our performance against objectives and or targets so that we can continually improve our performance and meet the needs of our customers.
- Define the information systems our employees, customers and contractors need to do their work.

- Define the processes and procedures for the operation and delivery of Information Security, to meet our needs and our customers
- Effective marketing of information security to all managers, employees, and other parties to achieve awareness.
- Providing appropriate awareness, training, and education
- Establishing an effective information security incident management process.
- Implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement.
- Introducing Information Security solutions that are based on technology, that are reliable, resilient and secure.
- Comply with all local legislation to ensure that DigiPlex does not infringe copyright, Patent or other licensing laws or loss of data.

5.0 Management System Overview & Requirements

5.1 ISMS Structure and Overview

This diagram below illustrates the primary components and their relationship to the DigiPlex ISO27001 Information Security Management System.



5.2 Statement of Applicability

Information security is implemented via an appropriate set of controls, which, in practice, are a combination of policies, standards and processes; organisational structures and physical or technical measures.

The selected controls from the ISO27001 Standard are documented in the Statement of Applicability (SOA), IT-PROC-01-02-DGS. Controls are only defined as not applicable where they are outside of the scope, identified as not required from Risk Assessment output results or where the responsibility for management of the identified risk has been outsourced to a third-party.

The Statement of Applicability identifies controls which are relevant to all areas of the ISMS and separately identifies controls which apply to limited areas of the ISMS.

Further information is contained within DigiPlex Group's Procedure IT-PROC-01-00-DGS –Asset Identification and Risk Assessment Procedure

5.3 Document and Record Management

Professional document management and record update/retention is critical in the arena of security risk management; particularly as such documents may have to be admissible in a Court of Law in the event of a security-related prosecution.

Due to the nature of security risk management, it is important to understand that many security related documents contain sensitive and restricted information and will require protection in their own right. Where documents can be made more widely available to staff, this is enabled.

The Statement of Applicability lists all documents relevant to the scope of this ISMS. All documents are controlled in accordance with the Control of Documents Procedure.

Further information is contained within DigiPlex Group's Procedure QA-PROC-01-00-DGS –Document Control and QA-PROC-02-00-DGS Control of Records.

5.4 Risk Management

Risk assessment is a fundamental part of our management system. Decisions regarding information security developments and how we interpret the results of instant reviews, and audits (internal and external) are based on this process.

Our decision to adopt controls from within the ISO standard are based upon the risk assessment process. Control exclusions, exclusions from the scope, and any risks that we decide to accept are all justified through the risk assessment.

This approach that DigiPlex takes to identifying and managing security risk is, in summary:-

- Identify the equipment/ systems in question (aka information security assets)
- Assess the security risks against these, using an approved and documented risk assessment methodology, including conducting a threat and vulnerability analysis.
- Produce a Risk treatment/corrective action plan or select baseline controls
- Implement the controls and procedures required in the Risk Treatment/corrective action Plan or apply baseline
- Then monitor and improve.
- Involve business managers in the risk identification process
- Identify and assess threats to information and IT systems
- Identify and assess vulnerabilities to information and IT systems
- Identify and assess the possibility of occurrence
- Identify the potential business impact of security failures
- Identify control requirements arising from such threats
- Link control improvements to business risk

- Provide management with an understanding of the DigiPlex's exposure to security breaches
- Result in action plans to reduce exposure

This risk assessment is a continual process which is subject to regular updates and management review, and is central to information security planning and decision-making.

Further information is contained within DigiPlex Group's Procedure IT-PROC-01-00-DGS –Asset Identification and Risk Assessment.

6.0 Organisation of Information Security

6.1 Internal organisation

6.1.1 Information security roles and responsibilities

Security roles and responsibilities identified below shall also be documented in individual job descriptions as appropriate. In particular, this shall apply to employees, contractors and third parties with greater responsibilities for information security e.g. the Information Security Manager, and DigiPlex IT's system owners and database administrators. This shall be the responsibility of HR and relevant Line Managers.

6.1.2 CEO

The CEO is responsible for ensuring that the Group is run in secure manner, which meets the relevant legislative, mandatory and any contractual requirements. In addition is also responsible for providing sufficient resources to line management to ensure that the procedures are capable of implementation and provide for effective control of identified risks. This responsibility will be exercised through the Senior Leadership Team.

6.1.3 Senior Leadership Team

The Senior Leadership Team have overall responsibility for the Information Security issues within the Group. They also have responsibility for implementing and monitoring the management systems and for ensuring that management resources are directed in the implementation of Policies.

In particular they ensure that:

- The resources made available to implement the Management Systems, provide sufficient capability to ensure the effective control of risks.
- They lead by example in the implementation of Policies and Management Systems.
- Ensure that sufficient resources, time effort, and finance are made available to allow all persons to carry out their responsibilities effectively.
- Ensure that all relevant personnel receive adequate and appropriate training and awareness, and their competence to carry out their assigned security tasks.

6.1.4 Information Security Manager

On behalf of the Senior Leadership Team, the ICT Director will assume the role of Information Security Manager (ISM). The ISM shall be responsible for documenting and maintaining policies in line with DigiPlex's business and security requirements and addressing security breaches and incidents, and ensuring overall policy compliance.

Ensuring the Information Security Management System (ISMS) resources and requirements are established, it is effectively implemented and maintained. In particular is to ensure that:

- The Information Security Management System (ISMS) is reviewed and revised, as and when necessary through regular monitoring and reviews.
- Ensure effective communication of the information security policies
- Ensure that all information regarding Security incidents of a serious nature is escalated within the Group to ensure all appropriate response actions are taken.

6.1.5 ICT Director

The ICT Director shall be responsible for the security of the DigiPlex IT network and information systems. The IT Director shall also be responsible for implementing appropriate IT security standards, controls, procedures and guidelines. In addition is responsible for maintain groups' Information Security Risk Register.

It is the responsibility of IT Director to provide all personnel with access to DigiPlex systems with annual information security awareness training briefings. The training should equip these personnel with the knowledge required to assess information security requirements, propose information security controls and ensure controls function effectively. The following items should be covered:-

- Password and User ID practices
- Social engineering
- Internet access guidelines
- E-mail usage guidelines
- Who to contact for additional information
- Information classification guidelines
- Monitoring policies
- Legal responsibilities
- Back-up and Restore

6.1.6 Security Manager

The Security Manager or nominated person shall be responsible for the Physical Access Security of the DigiPlex Datacentres. The Security Manager shall also be responsible for implementing appropriate Access security standards, controls, procedures and guidelines.

6.1.8 Information System Owners

Information System Owners are members of staff who shall be responsible for the security of DigiPlex's information assets. The responsibilities of Information System Owners shall include on-going evaluation and control of risks to information assets under their protection. Information System Owners shall ensure that access to information systems under their management is strictly controlled, and shall implement measures to avoid fraud and forgery e.g. using segregation of duties.

6.1.9 HR Manager

The HR Manager shall be responsible for providing support for human resources security, including responsibilities for pre-employment, during-employment and post-employment security requirements. In addition shall be responsible for ensuring that Personnel Data complies with Data Protection legislation.

6.1.10 Line Managers

All line managers shall be responsible for ensuring that their staff are aware of and comply with this policy. Staff using computer systems and media shall be trained in their use before access is granted. Line Managers shall ensure that access to information systems is strictly controlled and that HR, DigiPlex IT, Information System Owners (as relevant) are immediately notified when staff leave DigiPlex or change job functions.

6.1.11 Quality and Compliance Manager

The Quality and Compliance Manager shall be suitably qualified and/or experienced to ensure and shall have responsibility for the following:

- Maintain and update the register of legislation
- Advising on compliance with current legislation.
- Undertake Compliance Audits.
- Providing reports on the performance of the ISMS to senior management for review, and identification of improvement requirements.

6.1.12 All Users

All users with access to DigiPlex's information and information processing facilities shall be responsible for information security and ensuring that no breaches of information security result from their actions. Users shall familiarise themselves with our policy and its supporting sub-policies.

6.2 Segregation of duties

A fundamental element of internal control is the segregation of certain key duties. The basic idea underlying Segregation of Duties is that no employee or group of employees should be in a position both to perform and to conceal errors or fraud in the normal course of their duties. In general, the principal incompatible duties to be segregated are:

- Custody of assets.
- Authorisation or approval of related transactions affecting those assets.
- Recording or reporting of related transactions.

DigiPlex shall segregate the duties of its staff where feasible. In particular, for activities and transactions of a very critical and sensitive nature, e.g. financial transactions,

DigiPlex shall ensure that implementation, approval and auditing duties are appropriately segregated. Information System Owners and Line Managers shall be responsible for segregating duties in line with DigiPlex's business and security requirements.

DigiPlex IT shall ensure that 'IT administrator' roles are restricted as far as possible, and are regularly monitored and audited. Information system access shall be logged and monitored depending on risk.

6.3 Contact with authorities

In order to protect itself from security risks such as criminal damage, fire and flooding, and Internet risks, DigiPlex shall maintain appropriate contacts with relevant authorities such as the police, the fire brigade, its Internet Service Provider (ISP), telecommunications providers and utilities and seek clarification and guidance (e.g. Specification for fencing, fire systems etc). DigiPlex's security incident procedures and business continuity plans shall include requirements for contact details for contacting such authorities as appropriate.

6.4 Contact with special interest groups

DigiPlex shall maintain appropriate contact with external information security specialists to ensure that it is keeping abreast of the latest information security risks and protection measures. In particular, the Information Security Manager and DigiPlex IT shall maintain ongoing contact with experts in security threats and vulnerabilities, and security patches and solutions.

6.5 Information security in project management

Information security shall be integrated into DigiPlex's project management lifecycle to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character, e.g. a project for a core business process, IT, facility management and other supporting processes.

6.6 Mobile devices and teleworking

6.6.1 Mobile device policy and Teleworking

Mobile workers include all users who use and access DigiPlex's (and its customers') information and information processing facilities whilst not located on a DigiPlex site e.g. workers who are located at home, in hotels and conferences, and workers who are travelling. Mobile workers shall be responsible for the physical protection of DigiPlex's information processing facilities (e.g. laptops) in their possession.

DigiPlex IT shall be responsible for implementing controls for secure remote access to DigiPlex's network, protection against malicious software attacks e.g. viruses, secure personal firewalls, and secure Internet access. Mobile workers shall be responsible for ensuring that back-ups of DigiPlex's information stored on mobile devices are performed at regular intervals to avoid loss or corruption of information.

7.0 Human Resource Security

7.1 Prior to employment

7.1.1 Screening

All permanent and temporary staff shall be recruited using **DigiPlex's Group Procedure HR-PROC-01-00-DGS, HR Procedures.** This process includes appropriate background verification checks which shall be carried out before making any appointment. Checks shall be in accordance with relevant laws and appropriate to the role and information being accessed.

As a minimum, checks shall include two references, an identification check (e.g. production of passport, birth certificate or driving licence), a nationality and immigration status check, and confirmation of qualifications.

For posts processing very sensitive information e.g. When staff has access to sensitive data the customer may require selected staff to be vetted to their requirements.HR shall be informed of all intentions and all candidates are subject to suitable screening e.g. via a formal agreement between DigiPlex and the Customer.

7.1.2 Terms and conditions of employment

HR shall ensure that terms and conditions of employment state responsibilities for information security i.e. the requirement to comply with this information security policy. These shall be signed up to by employees before employment commences.

7.2 During employment

To ensure that employees and contractors are aware of and fulfil their information security responsibilities the following requirements apply:-

7.2.1 Management responsibilities

Management shall ensure that employees, contractors and third party users (for whom they are responsible) are adequately informed of their responsibilities to adhere to this policy.

7.2.2 Information security awareness, education and training

All users shall be made aware of and shall understand this manual (and supporting policies, procedures and guidelines) before access is granted to DigiPlex's information. Regular reminders, and awareness and education of policy changes shall also be provided.

Line Managers shall be responsible for ensuring that their staff are properly trained, **see HR-PROC-01-00-DGS, HR Procedures.** DigiPlex's Information Security Management Committee and Information Security Manager shall be responsible for ensuring that an on-going training and awareness programme is fully implemented.

7.2.3 Disciplinary process

HR have documented a Disciplinary procedure **HR-PROC-01-00-DGS**. This procedure shall apply to all permanent and temporary staff, and disciplinary action including dismissal may be taken in the event of a breach of this policy.

7.3 Termination and change of employment

To protect DigiPlex's interests as part of the process of changing or terminating employment. Line Managers and HR shall be responsible for ensuring that employees and contractors exit DigiPlex or change employment in an orderly manner. Similar responsibilities for third parties shall lie with those who are responsible for employing third parties.

Further information is contained within DigiPlex Group's Procedure IT-PROC-02-00-DGS –IT Access Control Policy and Process and SEC-PROC-01-00-DGS -DNAS DRAS Security ID Card Applications and Onsite Security Requirements.

8.0 Asset Management

8.1 Responsibility for assets

8.1.1 Inventory of assets

DigiPlex shall implement and maintain records of its information assets within a Asset Register. This document shall identify all valuable information assets that belong to DigiPlex, and shall be maintained by DigiPlex's IT Manager.

Information System Owners shall regularly notify the IT Manager of any required additions or changes to the Assets.

Inventories shall be created and maintained of all IT assets purchased and used by DigiPlex i.e. all hardware, software and telecommunications equipment. Inventories shall include up-to-date details of asset owners, users and locations, as well as asset serial numbers and purchase dates.

A procedure shall be established to ensure that the inventory register is kept up-to-date and audited on a regular basis.

8.1.2 Ownership of assets

Information System Owners shall be responsible for the security of the DigiPlex's information assets within their business areas. DigiPlex IT shall be the owner of all IT assets that belong to DigiPlex.

8.1.3 Acceptable use of assets

DigiPlex shall document and implement requirements for the acceptable use of information and information processing facilities. The requirements shall be regularly reviewed and maintained to ensure that they continue to meet DigiPlex's needs. All users shall be responsible for complying with DigiPlex's requirements for the acceptable use of assets. In support of this policy, detailed requirements for the acceptable use of IT assets are documented in DigiPlex's Acceptable Use Policy as well as its Internet and E-mail Usage Policies, all of which shall be formally issued to all users.

8.1.4 Return of Assets

DigiPlex shall ensure that all employees, contractors and third party users that no longer require access to DigiPlex's information and information processing facilities shall return all of DigiPlex's assets e.g. laptops, electronic badges, and other hardware, software and information, in a timely and orderly manner. All users shall facilitate the timely return of DigiPlex's assets that have been given to them during their employment.

8.2 Information classification

8.2.1 Classification of information

DigiPlex has devised and implemented an information classification, labelling and handling policy, IT-POL-04-00-DGS. This Policy identity's protective marking classes for categorising DigiPlex's information according to its sensitivity, potential impacts upon unauthorised disclosure, and the access restrictions that apply. Information System Owners (and creators of information on their behalf) shall classify and label information for which they are responsible according to the procedures.

8.2.2 Labelling of information

The information classification, labelling and handling procedures shall also document security requirements within each information class for copying, storing, processing, transmitting and disposing of information in any format e.g. electronic, media and paper. All users of the DigiPlex's (and its customers') information shall ensure that it is securely handled according to its classification label in line with the procedures.

8.2.3 Handling of assets

To protect DigiPlex's information from unauthorised disclosure or misuse, information stored on removable media and in hardcopy documentation shall be securely handled in line with the DigiPlex's Information Classification requirements.

8.3 Media handling

8.3.1 Management of removable media

Care shall be taken to protect all removable media (removable disks, tapes, CDs, DVDs, and USB devices e.g. memory sticks and flash drives) and hardcopy documentation containing the DigiPlex's information.

Measures shall be taken to ensure secure storage, transit, copying, reuse and disposal of media and hardcopy documentation.

Manufacturers' guidelines shall be applied for the protection of removable media. Users shall ensure that removable media and hardcopy documentation are securely handled in line with the DigiPlex's Information Classification requirements.

Depending on the information classification, and when necessary and practical, authorisation from a user's Line Manager shall be required before removable media and hardcopy documentation are removed from DigiPlex's offices, and a record of such removals shall be kept by the Line Manager in order to maintain an audit trail.

Information stored on removable media that needs to be available longer than the media lifetime shall also be stored elsewhere to avoid information loss due to media deterioration.

8.3.2 Disposal of media

Removable media and hardcopy documentation shall be securely disposed of when no longer required, in line with DigiPlex's Information Classification requirements. Users shall seek advice from DigiPlex IT where necessary. All removable media containing DigiPlex's non-public information shall be securely wiped (data shall be removed or overwritten) before disposal, however if this is not possible, the media shall be destroyed to prevent access to data.

8.3.3 Physical media transfer

To protect against unauthorised access, misuse or corruption during transportation, information stored on removable media and in hardcopy documentation shall be securely handled in line with DigiPlex's Information Classification requirements, e.g. by use of appropriate packaging, recorded delivery, and reputable couriers. All users shall comply with these requirements.

9.0 Access Control

9.1 Business requirements of access control

9.1.1 IT Access control policy

All access to DigiPlex's information (including its customers' information) and information processing facilities shall be restricted on a 'need-to-know' basis. As far as possible, each user shall access information using a unique user ID and password. This policy shall be enforced by Information System Owners and DigiPlex IT.

9.1.2 Physical Access control policy

Users shall only be provided with access to DigiPlex's Datacentres that they have been specifically authorised to use, in line with Security ID Card Applications and Onsite Security Requirements, SEC-PROC-01-00-DGS -DNAS DRAS Security ID Card Applications and Onsite Security Requirements

9.1.3 Access to networks and network services

Users shall only be provided with access to DigiPlex's network services that they have been specifically authorised to use, in line with the Access Control process, IT-PROC-02-00-DGS. Access to DigiPlex's network services shall be managed by DigiPlex IT based on business requirements. Only DigiPlex IT (and suitable personnel appointed by them) shall have privileges to access and change network configurations.

9.2 User access management

9.2.1 User registration and de-registration

Access Control process, IT-PROC-02-00-DGS describes the registration and de-registration of all user accounts, and the granting of access to DigiPlex's network, information systems, and Internet and e-mail facilities.

Records of user registration, de-registration and access privileges shall be maintained. Where possible, each user shall be given a unique user account only accessible to the individual user, to enable full tracking of user actions. A user shall not share any user (network, operating system or application) account with another user without prior authorisation from DigiPlex IT, relevant Information System Owners and the user's Line Manager.

Line Managers shall be responsible for informing DigiPlex IT and relevant Information System Owners of all registration, access and de-registration requirements as soon as possible, and DigiPlex IT and relevant Information System Owners shall be responsible for approving and implementing these requirements. De-registration procedures are addressed within Access Control process, IT-PROC-02-00-DGS.

DigiPlex IT shall ensure that, as far as possible, all operating system users have a unique user ID for their individual use only, so that activities can be traced to the individual responsible. This shall include use of unique user IDs for system administrator access too.The default authentication technique shall involve use of strong passwords (by following the guidelines in User Password Management above), however, there may be justification for use of stronger authentication techniques e.g. remote network 'system administration' access that uses two-factor authentication (such as hardware tokens) is required for access to DigiPlex's payment card data environment.

9.2.2 User access provisioning

DigiPlex IT, Information System Owners and Line managers shall assign or revoke access rights granted to user.

Authorisation shall be obtained from the owner of the information system for the use of the information system.

The Line Manager shall verify that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties and shall periodically review access rights with owners of the information systems or services.

DigiPlex IT shall ensure that access rights are not activated before authorisation procedures are completed and maintain a central record of access rights granted

9.2.3 Management of privileged access rights

Access privileges shall be limited to a level that ensures that each user is able to perform their job function (but no further functions). They are implemented via the procedures Access Control process, IT-PROC-02-00-DGS.

9.2.4 Management of secret authentication information of users

Information System Owners and IT shall be responsible for ensuring that secure authentication methods such as use of user IDs and strong passwords are used to access business information systems (applications).

Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on. Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption) and protected from unauthorised access.

Whenever feasible, DigiPlex IT and Information System Owners shall implement password controls that include enforcement of password strength (via length and format), regular password changes, inability to re-use previously used passwords, and user account lockout after a small number of bad password attempts.

9.2.5 Review of user access rights

User access rights shall be subject to formal review on a regular basis. Information System Owners and DigiPlex IT shall undertake regular checks to verify that user access rights are being properly managed, and unnecessary rights shall be removed. Special access privileges (including ‘IT administrator’ access) shall also be reviewed yearly.

9.2.6 Removal or adjustment of access rights

DigiPlex Line Managers and HR shall ensure that all employees, contractors and third party users that no longer require access to the DigiPlex’s information and information processing facilities shall no longer be able to access DigiPlex’s non-public information and information processing facilities. The procedure identified under Starters/Leavers/Movers shall include responsibilities (and the completion of a form) for the removal of access rights. In addition, DigiPlex IT shall check every month for unused user accounts, and disable them subject to approval from relevant Line Managers.

9.3 User Responsibilities

9.3.1 Use of secret authentication information

Users shall be responsible for keeping their passwords confidential at all times, and shall not disclose passwords to anyone, including DigiPlex IT staff and their Line Managers. Written down passwords shall be discouraged, unless documentation is completely inaccessible to other persons

9.4 System and application access control

9.4.1 Information access restriction

Access to DigiPlex's electronic information (including information stored in applications, file servers, e-mail systems, and web systems) and application functions shall be strictly controlled by DigiPlex IT and Information System Owners. This shall include use of unique user IDs to enable accountability for user actions, restricted privileges based on job functions, and secure password management by applying policy in User Access Management. Access to information shall be controlled in line with DigiPlex's Information Classification requirements.

9.4.2 Secure log-on procedures

Operating system access control applies to all computers that have an operating system e.g. servers, PCs, and laptops. DigiPlex IT shall ensure that log-on procedures are secure and do not provide unnecessary information that could enable unauthorised access e.g. provide clues about valid user IDs or the operating system version (and therefore its vulnerabilities). Operating system and network account log-on procedures shall also include an enforced user acknowledgement to comply with local Computer Misuse legislation. All successful and unsuccessful log-on attempts shall be logged and monitored.

Information System Owners and DigiPlex IT shall consider implementation of session (e.g. database transaction) time-outs after a defined period of inactivity where applicable i.e. where the requirement is justified by risk to information security.

Information System Owners and DigiPlex IT shall consider implementation of connection time limitations where applicable (where the requirement is justified by risk to information security). For example, third party support access shall be limited to specific times according to DigiPlex's requirements.

9.4.3 Password management system

System access shall be protected by use of secure password management, by following the guidelines provided by the system owner.

9.4.4 Use of privileged utility programs

DigiPlex IT shall ensure that operating system utility programs that might be capable of overriding system and application controls are restricted by use of appropriate authentication and access controls (or completely removed).

9.4.5 Access control to program source code

Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) shall be strictly controlled, in order to prevent

the introduction of unauthorised functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property.

10.0 Cryptography

10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.1.1 Policy on the use of cryptographic controls

DigiPlex IT shall be responsible for all cryptography controls (encryption and digital signatures) used by DigiPlex for the storage and transmission of sensitive information. No cryptography shall be used without the authorisation of DigiPlex IT. Appropriate cryptographic controls shall be applied to protect the confidentiality and integrity of information when justified by risk assessment, and DigiPlex's Information Classification requirements.

10.1.2 Key management

When cryptography is implemented by DigiPlex, cryptographic keys shall be securely managed throughout their lifecycle, from generation and distribution through to their usage, revocation, archiving and destruction. DigiPlex IT shall be responsible for ensuring that appropriate procedures and controls are implemented and documented, and that they are in line with PCI DSS requirements when appropriate.

11.0 Physical and environmental security

11.1 Secure areas

11.1.1 Physical security perimeter

For DigiPlex's offices, security perimeters shall be defined by the use of physical access controls, and secure, lockable windows and doors. Fire escapes shall be controlled to avoid unauthorised access. Support Services shall be responsible for the provision of adequate physical security perimeters, and defining and implementing relevant procedures. All users that have authorised access to DigiPlex's offices shall protect against access by unauthorised persons, including tailgating.

11.1.2 Physical entry controls

Physical entry controls shall be defined by the authorised use of physical access controls i.e. use of electronic key fobs / electronic swipe cards / digital key pads / physical keys. All visitors to DigiPlex's offices shall report to the reception area, sign in to a visitor's book, always wear a visitor's badge for identification, be escorted at all times whilst within the DigiPlex's offices, and sign-out of the visitor's book upon departure. Staff shall challenge any unrecognised and unescorted person within DigiPlex's offices. In addition, DigiPlex shall use CCTV to monitor entry points into its offices.

11.1.3 Securing offices, rooms and facilities

Secure, lockable rooms shall be used to protect functions with special security requirements e.g. computer rooms and rooms that host network equipment. Secure, lockable cabinets shall be used to store all sensitive information whilst left unattended e.g. sensitive information

belonging to HR and DigiPlex IT, as well as unattended laptops, Smart Phones, and computer media.

11.1.4 Protecting against external and environmental threats

DigiPlex's offices shall be adequately protected from physical security threats such as fire and flooding. Support Services shall be responsible for the provision of adequate site controls e.g. timely contact with the Emergency Services, and defining and implementing relevant procedures e.g. building evacuation, and dealing with suspicious packages. All users shall ensure that they are familiar with DigiPlex's controls and procedures. DigiPlex IT shall address risks associated with critical computing and networking equipment. The Business Continuity Management Team shall be responsible for defining and implementing a DigiPlex-wide business continuity management strategy and plan that include consideration of external and environmental threats.

11.1.5 Working in secure areas

DigiPlex ensures that only the required users are granted access to secure areas to key personnel for safety reason to personnel and protection to the buildings assets. All Vacant areas are secure and physically locked. Photographic, audio or video or other recording equipment, such as cameras in mobile devices is not allowed unless authorised.

11.1.6 Delivery and loading areas

All deliveries shall be made to reception areas. External delivery and collections people shall not enter the DigiPlex's offices unless escorted. All users who are responsible for collecting deliveries shall ensure that they are inspected for tampering and damage, and signed-for upon arrival, and are immediately moved to a more secure area.

11.2 Equipment

11.2.1 Equipment siting and protection

DigiPlex IT shall be responsible for IT equipment siting and protection. All computer servers and core network equipment shall be located in secure computer and communication rooms with strict access controls over and above those used to access other areas within DigiPlex's offices. The computer and communications rooms shall be locked when DigiPlex IT's staff members are not present. To prevent equipment overheating, they shall have adequate air conditioning, which shall be properly maintained according to the manufacturer's standards.

11.2.2 Supporting utilities

DigiPlex shall ensure adequate protection against electrical power failures and disruptions. DigiPlex IT shall be responsible for implementing agreed contingency arrangements for IT equipment in line with the DigiPlex's business continuity plans. Critical computer and network equipment shall be fitted with Uninterruptible Power Supply (UPS) technology, which shall (as a minimum) enable controlled system shutdowns in the event of a power failure.

11.2.3 Cabling security

DigiPlex shall ensure adequate protection against damage or interference of power and telecommunications cabling that carries data or supports information services.

Facilities shall be responsible for the security of DigiPlex's core power and telecommunications cabling systems within its offices, whilst DigiPlex IT shall be responsible for all other cabling

that interfaces with computing and network equipment. In all cases, IT industry best practice standards shall be implemented. All core cabling shall be in conduits if surface mounted, otherwise within the framework of the building, and not accessible to unauthorised people. Power cables shall be segregated from communications cables to prevent interference. Colour coded cabling and equipment labelling shall be used to minimise human errors

11.2.4 Equipment maintenance

All equipment used to support the storage and processing of information shall be adequately maintained according to manufacturers' maintenance schedules. All IT equipment maintenance shall be formally authorised and managed by DigiPlex IT. Computer and network equipment shall be covered by warranties or third party maintenance agreements. Wherever possible, new equipment shall be purchased with a warranty agreement. Only authorised personnel shall carry out repairs and service equipment. Documented records of all equipment faults and maintenance shall be retained.

11.2.5 Removal of assets

All of DigiPlex's IT equipment and software shall only be taken off-site following authorisation by DigiPlex IT/ Line Manager, whilst DigiPlex's information shall only be taken off-site following authorisation from the relevant Information System Owner or Line Manager.

All Site based IT equipment (and software) taken off-site shall be signed for by the person taking the equipment to acknowledge responsibility for its welfare. DigiPlex IT shall countersign to authorise such off-site usage.

When no longer needed, all IT equipment (and software) shall be returned to DigiPlex IT and signed in by the borrower and DigiPlex IT staff. Upon return, equipment and software shall be immediately moved to a secure storage area. Likewise, when no longer needed, all information shall be returned on-site and securely stored as appropriate.

11.2.6 Security of equipment and assets off-premises

All authorised users shall be responsible for protecting off-site IT equipment (that belongs to DigiPlex) from physical security threats. Equipment taken off-site shall be locked away and kept out of sight when left unattended. Users shall ensure that unauthorised persons are not able to view DigiPlex's information on display screens, and (as a minimum) shall protect access to unattended equipment by use of an enforced password.

Users shall also ensure that off-site information (that belongs to DigiPlex) is securely handled in line with DigiPlex's Information Classification requirements.

11.2.7 Secure disposal or re-use of equipment

All of DigiPlex's information and software shall be securely wiped (removed and overwritten) from IT equipment before its disposal or re-use (the latter as appropriate). All equipment disposal and re-use shall be formally authorised and managed by DigiPlex IT, who shall devise appropriate standards and procedures.

11.2.8 Unattended user equipment

Users shall protect their DigiPlex IT equipment from unauthorised access when left unattended. DigiPlex IT shall implement standard computer screen locking mechanisms that disable access after a defined length of user inactivity i.e. 15 minutes or less time.

11.2.9 Clear screen and secure desk policy

Clear Screen and Secure Desk Policy IT-POL-06-00-DGS has been implemented by use of the controls listed under Unattended User Equipment above. In addition, users shall ensure that all valuable and sensitive mobile equipment e.g. laptops, computer media and hardcopy information are removed from their desks when left unattended, and are appropriately stored

in locked areas or facilities e.g. locked cabinets, and that access to 'container' keys is properly controlled. Users shall comply with the DigiPlex's Information Classification requirements.

12.0 Operations Security

12.1 Operational procedures and responsibilities

12.1.1 Documented operating procedures

Documented operating procedures for information systems shall be up-to-date and regularly maintained by relevant Information System Owners, Line Managers and DigiPlex IT to enable continuous, error-free and secure processing of information systems. Procedures shall include secure build instructions for IT computing and networking equipment, including software configurations. Documentation shall adequately cover error and exception handling requirements, and be comprehensive enough to ensure that DigiPlex's knowledge and expertise is maintained in the event of unexpected staff shortages and losses. Regular, formal reviews of documented operating procedures shall be scheduled to ensure that they remain up-to-date.

Up-to-date documented operating procedures shall be distributed to all users who need them to perform their job functions. Copies of relevant procedures shall also be securely stored off-site for business continuity and disaster recovery purposes.

12.1.2 Change management

Service Change management procedures, **OPS-PROC-01-00-DGS** shall be implemented for all significant changes to information processing systems and related documentation. All such changes shall be initially assessed for business, security and availability impacts, formally planned and communicated to those with vested interests, documented, tested and approved, and contingency measures shall be available in case of failure to correctly implement the changes.

DigiPlex IT shall be responsible for IT change management, including changes to the network infrastructure and information systems, hardware and software, and related documentation.

12.1.3 Capacity management

Information processing and storage capacity requirements shall be understood prior to operational implementation of new or changing information systems, including networking capacity requirements. Capacity monitoring shall take place to identify poor performance of or disruption to information processing facilities. Information System Owners and DigiPlex IT shall be responsible for identifying new or changing business requirements for capacity management.

DigiPlex IT shall be responsible for implementing and maintaining capacities that meet these requirements. Formal procedures and controls shall be used for identifying, implementing and monitoring capacity requirements.

12.1.4 Separation of development, testing and operational environments

As necessary and appropriate, DigiPlex IT shall ensure that IT development, test and operational facilities are adequately separated to reduce the risks of unauthorised access and unauthorised changes to the operational environment.

12.2 Protection from malware

DigiPlex shall ensure that it has adequate technical and procedural controls in place to protect its information and information processing facilities from malicious code attacks e.g. viruses and spyware. DigiPlex IT shall be responsible for implementing appropriate malicious code detection, prevention and recovery controls.

All computers and network devices (unless deemed unnecessary e.g. Smart Phone's and Internet and e-mail gateways (as appropriate) shall be protected by reputable, up-to-date anti-virus and anti-spyware software that provides protection against all forms of malicious code.

As appropriate, all newly acquired software shall be checked for malicious code prior to its use. Detailed advice on how users shall protect against malicious code is provided in the DigiPlex's Acceptable Use Policy, as well as its Internet and E-mail Usage Policies. All users shall be responsible for adhering to DigiPlex's policies and guidelines. Users shall report any detected or suspected malicious code immediately to DigiPlex IT and the Information Security Manager, and shall not install any unauthorised software on the DigiPlex's IT equipment.

12.3 Information Backup

Back-up and recovery procedures and technology shall be implemented to protect DigiPlex from losses or corruption of information and software e.g. due to unauthorised changes to information and software, technical failures, viruses and fire. Regular recovery tests using back-ups shall be performed by DigiPlex IT to ensure that a 'business as usual' status can be resumed as quickly as possible following a security incident occurrence. Information System

Owners shall be responsible for identifying business requirements for back-up and recovery controls (including legal, statutory, regulatory and contractual requirements for data retention), whilst DigiPlex IT shall be responsible for implementing suitable back-up and recovery controls and procedures. The successful completion of all back-ups shall be confirmed as soon as possible. Storage of back-ups shall be geographically separate from the backed-up information systems to protect against disasters such as building loss. All users shall be responsible for ensuring that all changes to information stored on local client devices such as laptops undergo regular back-ups. It is recommended that such information shall always be copied and stored onto appropriate DigiPlex servers to ensure that regular back-ups are taken. **See IT-POL-08-00-DGS Information Backup and Restore Policy for further information.**

12.4 Logging and monitoring

Objective: To record events and generate evidence.

12.4.1 Event logging

Event logs recording user activities, exceptions, and information security events shall be produced and kept for as long as the law or regulations requires.(e.g. one year minimum in relation to access to payment card data) to assist in future investigations and access control monitoring. DigiPlex shall implement standards and procedures for audit logging of network access, operating system access, and applications and information access, and shall identify events and details that need to be captured in audit logs.

Information System Owners shall be responsible for audit logging requirements for business information systems (applications), whilst DigiPlex IT shall be responsible for audit logging requirements for the IT network and security infrastructure, user 'network' accounts, server and operating systems, and corporate systems such as e-mail and Internet access.

Responsibilities include identifying and implementing audit log retention and archiving needs to comply with legal, regulatory, contractual and evidence gathering requirements.

12.4.2 Protection of log information

Logging facilities and log information shall be protected against tampering and unauthorised access, by using appropriate controls e.g. secure authentication and access controls.

Information System Owners and DigiPlex IT shall ensure that access to log information is restricted on a 'need-to-know' basis, and only to 'trusted' staff.

12.4.3 Administrator and operator logs

System and database administrator activities shall be logged. This shall be the responsibility of Information System Owners and DigiPlex IT. Where necessary, logs of administrator

activity shall be immediately copied to a secure area that is only accessible to the Information Security Manager and appointed staff, to protect against any tampering of evidence of access.

12.4.4 Clock synchronisation

DigiPlex IT shall be responsible for ensuring that the computer clocks of all information processing facilities are synchronised using an accurate, reputable time source.

12.5 Control of operational software

Software shall only become operational when the policies defined under Change Management and System Acceptance above have been applied. Only DigiPlex IT shall install or update operational software and applications, using configuration management processes.

DigiPlex IT shall ensure that all DigiPlex computer systems, e.g. servers, PCs and laptops are secure.

12.6 Technical vulnerability management

12.6.1 Management of technical vulnerabilities

DigiPlex IT shall be responsible for protecting DigiPlex from technical vulnerabilities by acquiring timely information about the vulnerabilities, evaluating DigiPlex's exposure to the vulnerabilities, and implementing appropriate measures.

DigiPlex IT shall determine suitable information sources that regularly identify technical vulnerabilities e.g. hardware and software vendors. Procedures and resources shall be established to ensure that information sources are regularly checked for new vulnerabilities.

Any actions required to address potential vulnerabilities e.g. the application of security patches shall be carried out in accordance with the Change Management and policy.

A patch management procedure shall be documented and implemented. Systems at high risk shall be identified and addressed immediately. Where a vulnerability has been identified, but no security patch is available, other controls shall be considered including turning off services or capabilities associated with the vulnerability, adapting or adding access controls, increasing access monitoring, and raising staff awareness of the vulnerability. The technical vulnerability management process shall be regularly reviewed to ensure its effectiveness.

12.6.2 Restrictions on software installation

DigiPlex IT shall manage the list of DigiPlex approved software that is running on IT systems and restrict users from installing unapproved software. If you are unsure if the software is allowed ,contact IT for direction. Periodically the IT department will publish a list of approved software such as I Tunes.

12.7 Information systems audit considerations

Objective: To minimise the impact of audit activities on operational systems.

Information systems audit controls

Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimise the risk of disruptions to business processes. Procedures for the management of information systems audits shall be documented and implemented by the Information Security Management Committee and the Information Security Manager.

13.0 Communications Security

13.1 Network security management

13.1.1 Network controls

Controls shall be implemented to achieve and maintain security in the DigiPlex's networks e.g. use of secure firewalls, routers and switches, authentication and access controls, encryption, and logging and monitoring of access. Special controls and logging shall be established to safeguard the confidentiality and integrity of data passing over public or wireless networks e.g. use of strong authentication and encryption. DigiPlex IT shall be responsible for network security. The requirement for network access control shall be further addressed within Network Access Control.

13.1.2 Security of network services

Service standards covering the operation of network services shall be drawn up and agreed with users, and regularly reviewed. DigiPlex IT shall be responsible for network service delivery and network security.

13.1.3 Segregation in networks

DigiPlex's network shall be segmented to protect sensitive information systems belonging to DigiPlex and its customers from unauthorised access via Internet, wireless and internal network based access. Secure firewalls (and other controls such as Virtual Private Networks (VPNs) and two factor authentication) shall be used to control remote access across the Internet. DigiPlex IT shall also use other appropriate technologies e.g. secure firewalls and Virtual LANs, to segregate the internal network where necessary.

13.2 Information transfer

13.2.1 Information transfer policies and procedures

Information exchange requirements shall be defined in DigiPlex's Information Classification requirements, as well as DigiPlex's Internet and E-mail Usage Policies. All users shall comply with these requirements.

13.2.2 Agreements on information transfer

Where necessary, agreements or protocols shall be established for the exchange of information and software between DigiPlex and relevant external parties e.g. customers and suppliers. Information System Owners (and DigiPlex IT, where appropriate) shall be responsible for managing such agreements and protocols.

13.2.3 Electronic messaging

Procedures and controls shall exist to manage e-mail and Internet access to protect DigiPlex from security threats such as viruses, unsolicited e-mails, fraud, unauthorised content and breaches of legislation e.g. computer misuse and copyright legislation. Legally acceptable controls shall be implemented to block and content check e-mails and Internet access. DigiPlex IT shall be responsible for implementing secure e-mail and Internet access controls, and for maintaining the required availability levels of these systems. All users shall be responsible for complying with DigiPlex's Internet and E-mail Usage Policies. To protect against unauthorised access to confidential information within e-mails, information shall be securely handled in line with DigiPlex's Information Classification requirements.

13.2.4 Confidentiality or non-disclosure agreements

All users that have access to DigiPlex's non-public information and information processing systems shall sign-up to DigiPlex's standard confidentiality agreement devised and maintained by HR, before access is granted. This applies equally to management, permanent and

temporary staff, and contractors. A confidentiality agreement shall be included within terms and conditions of employment that are issued and signed up to at the start of employment.

Confidentiality agreements shall address specific confidentiality requirements, ownership of information, expected duration of the agreement, terms for information to be returned or destroyed at agreement cessation, actions to be taken in case of a breach of the agreement, and the right to audit and monitor activities that involve confidential information.

14.0 System acquisition, development and maintenance

14.1 Security requirements of information systems

14.1.1Security requirements analysis and specification

Information System Owners and DigiPlex IT shall be responsible for ensuring that specifications of business requirements for new information systems, or enhancements to existing information systems include requirements for security controls, which reflect the business value of the information assets, and are derived from formal risk assessment processes. This equally applies to use of third party software and in-house developed software.

Third party software shall be reviewed and evaluated, and third party customer references shall be obtained, to ensure that security requirements are met. Adherence to this information security manual shall be a requirement of new and enhanced third party and in-house developed software. A standard shall be documented and implemented to help identify all security requirements.

14.1.2 Securing application services on public networks

Adequate controls shall be implemented such as secure authentication, encryption, access controls and access logging and auditing. Relevant Information System Owners and DigiPlex IT shall be responsible for ensuring that adequate controls are in place.

DigiPlex shall protect its web services and the integrity of publicly available electronic information from security threats such as viruses and unauthorised modification. This includes the need for secure authentication, user access management and secure software configuration. DigiPlex's web services shall offer availability levels to meet the business requirements of DigiPlex and its customers.

Web-based DigiPlex information shall be maintained and up-to-date to meet legal, statutory, regulatory, contractual and business requirements. Information Owners shall be responsible for maintaining up-to-date and relevant information and shall authorise the publication of all DigiPlex information relevant to their areas, whilst DigiPlex IT shall be responsible for implementing and maintaining appropriate procedures and controls to protect publicly available electronic information.

14.1.3 Protecting application services transactions

Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised duplication or replay.

14.2. Security in development and support processes

14.2.1 Secure development policy

Secure coding standards shall be considered and where relevant mandated for use.

Developers shall be trained in their use and testing and code review shall verify their use.

If development is outsourced, DigiPlex shall obtain assurance that the external party complies with these rules for secure development.

14.2.2 System change control procedures

Policy on change control procedures for applications' software changes is detailed under Change Management. This also includes changes to any database information made outside of an application e.g. by use of SQL (only to be done when absolutely necessary and following authorisation). **See OPS-PROC-1-00-DGS Change Management**

14.2.3 Technical review of applications after operating platform changes

When operating systems are changed, in-house developed applications (if relevant) shall be reviewed and tested to ensure there is no adverse impact on the applications' operation and security. This shall be done by implementing the Change Management process. **See OPS-PROC-1-00-DGS Change Management**

14.2.4 Restrictions on changes to software packages

Modifications to third party software packages shall be limited to necessary changes, and all changes shall be strictly controlled. No modifications shall be permitted without authorisation from the Information System Owner and DigiPlex IT.

If modifications are necessary, consideration shall be given to the risk of built-in controls and integrity processes being compromised, whether the consent of the vendor is required, the possibility of obtaining the required changes within the next vendor software release, and the impact if DigiPlex becomes responsible for future maintenance of the software as a result of the changes. All modifications shall be done by implementing the Change Management process. **See OPS-PROC-1-00-DGS Change Management**

14.2.5 Secure system engineering principles

Secure information system engineering procedures based on security engineering principles have been established, documented and applied to in-house information system engineering activities, where appropriate.

Security has been designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility.

14.2.6 Secure development environment

Where DigiPlex is developing systems/applications a secure area shall be set up a secure development environment to include people, processes and technology associated with the development to protect the entire system development lifecycle.

14.2.7 Outsourced development

When relevant, any outsourced software development shall be supervised and monitored by DigiPlex. All contractors shall be required to adhere to this information security manual. The Addressing Security in Third Party Agreements shall be adhered to. In addition, all software shall be tested and controlled by implementing the Change Management process.

14.2.8 System security testing

Any new or updated systems for the DigiPlex environment needs to be thoroughly tested and verified during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions.

For in-house developments, such tests shall initially be performed by the development team.

Independent acceptance testing shall then be undertaken (both for in-house and for outsourced developments) to ensure that the system works as expected and only as expected. The extent of testing shall be in proportion to the importance and nature of the system.

14.2.9 System acceptance testing

Prior to implementing all significant information processing changes into operations, there shall be the establishment of acceptance criteria, test plans, test results, and formal acceptance and approval of the changes. Necessary security checks shall be accounted for. Information System Owners shall be responsible for user acceptance testing and sign-off, whilst DigiPlex IT shall be responsible for IT acceptance testing and sign-off e.g. testing recovery from computer failures.

14.3 Test data

By default, live data shall not be copied and used for testing purposes without scrambling or removing any sensitive details e.g. personal information, including payment card details.

When it is impractical to do this, measures shall be taken to protect test data from unauthorised access, using physical and logical security controls that provide the same levels of protection as for live data. (It should be noted that live payment card numbers cannot be used for testing purposes). All copies of sensitive live data shall be formally authorised by Information System Owners and DigiPlex IT.

The DigiPlex Information Classification requirements shall be taken into consideration when using sensitive live data as test data. All copies of sensitive live data shall be erased as soon as possible following testing. Information Systems Owners, DigiPlex IT and users involved in testing shall be responsible for the protection of system test data.

15.0 Supplier relationships

15.1 Information security in supplier relationships

15.1.1 Information security policy for supplier relationships

The DigiPlex policy covers the security requirements to mitigate the risks associated with supplier's access to DigiPlex's assets. An agreement needs to be in place to mandating information security controls to specifically address supplier access to DigiPlex's information.

15.1.2 Addressing security within supplier agreements

Information security and relevant service delivery requirements shall be incorporated within formal agreements for any third party e.g. service provider, customer and business partner that accesses, develops or supports DigiPlex's information and information processing facilities. This shall include who is responsible for data content storage, and retention times and the authority to dispose for data.

This shall also include third parties providing DigiPlex with outsourcing or facilities management arrangements (if relevant), where DigiPlex information and software is accessible to such third parties. All relevant contracts with third parties shall draw attention to compliance with this policy. Third party agreements shall address specific confidentiality requirements, ownership of information, hardware and software (as relevant), legal obligations e.g. data protection and copyright, expected duration of the agreement, terms for information to be returned or destroyed at agreement cessation, actions to be taken in case of a breach of the agreement, and the right to audit and monitor activities that involve DigiPlex's information and information processing facilities

15.1.3 Information and communication technology supply chain

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Supplier agreements for organisations that supply information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships.

If suppliers outsource to additional third parties they shall ensure that contractors utilised in the supply chain meet DigiPlex's security requirements.

15.2 Supplier service delivery management

To maintain an agreed level of information security and service delivery in line with supplier agreements we need to monitor review and manage the changes of our supply chain.

15.2.1 Monitoring and review of supplier services

All those with responsibility for managing third parties e.g. DigiPlex IT and Information System Owners, shall regularly assess whether third parties are honouring their agreements using formal procedures.

15.2.2 Managing changes to supplier services

Changes to the provision of third party services, including information security procedures and controls, shall be managed, taking account of the criticality and sensitivity of business systems and processes involved, and re-assessment of risks. This shall be implemented by those with responsibility for managing third parties.

16.0 Information Security incident management

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.1 Responsibilities and procedures

Examples of information security incidents include information system failures, incomplete and inaccurate data, virus attacks, unauthorised access to an information system, computer misuse, fire and theft. The DigiPlex Group Procedure OPS-PROC-06-00-DGS, Incident Management, is to be used for managing all information security incidents (and security events). This ensures that DigiPlex is able to respond as soon as possible to security incident occurrences, identify security incident causes, resume a 'business as normal' status as quickly as possible, produce suitable remedies to prevent reoccurrences of security incidents, and gather and securely handle required evidence needed for production in a court of law or for disciplinary cases.

This procedure ensures that relevant staff are involved as quickly as possible, and that effective communication surrounding incident management exists within DigiPlex. DigiPlex IT, HR, Information System Owners shall ensure that procedures within their own areas of responsibility are documented and implemented.

16.1.2 Reporting information security events and Weaknesses

The Information Security Manager shall ensure that all information security incidents, including security events (e.g. a door that has been left open) that could have led to a security incident are reported. Users shall immediately report security incidents and events (actual or suspicious) to appropriate personnel by following the DigiPlex Group Procedure Incident Management **(**OPS-PROC-06-00-DGS)

16.1.3 Assessment of and decision on information security events

Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents.

DigiPlex IT shall assess each information security event using the event and incident classification scale and decide whether the event shall be classified as an information security incident.

Classification and prioritisation of incidents can help to identify the impact and extent of an incident.

Results of the assessment and decision shall be recorded in detail for the purpose of future reference and verification.

16.1.4 Response to information security incidents

Information security incidents shall be responded to by a nominated point of contact and other relevant persons of DigiPlex or external parties.

The response shall include collecting evidence, conducting information security forensics analysis, escalation, ensuring that all involved response activities are properly logged for later analysis, communicating the existence of the information security incident dealing with information security weakness(es) found to cause or contribute to the incident.

16.1.5 Learning from information security incidents

The Information Security Management Committee and Information Security Manager shall ensure that procedures are established to regularly review security incident (and security event) occurrences in order to introduce improvements and prevent further occurrences. There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. A summary of security incident occurrences and impacts shall be included in regular reports to DigiPlex's Senior Leadership Team.

16.1.6 Collection of evidence

Procedures shall include responsibilities and procedures for the secure collection, retention and presentation of evidence for a court of law, should this be necessary. DigiPlex shall ensure that the evidence conforms to the rules for evidence laid down in the relevant jurisdiction(s). The procedures shall involve DigiPlex's Legal (for legal requirements) and the Police as necessary.

17.0 Information security aspects of business continuity management

17.1 Information security continuity

17.1.1 Planning information security continuity

Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security. These shall in classified according to priority.

The Business Continuity Management Team shall ensure that this process is properly managed. Information System Owners and DigiPlex IT shall have a complete understanding of business impacts resulting from losses or unavailability of DigiPlex's IT network and information systems.

17.1.2 Implementing information security continuity

A managed process shall be developed and maintained for business continuity throughout DigiPlex that addresses the information security requirements needed for business continuity. The Business Continuity Management Team shall ensure that information security is included in the business continuity management process.

DigiPlex shall ensure that it has defined and implemented an organisation-wide business continuity management strategy and plan, based upon the outputs of on-going risk assessments, and which take into account the relative importance of each information system belonging to, or provided by DigiPlex. Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required timescales following interruption to, or failure of, critical business processes.

These requirements shall be managed by DigiPlex's Business Continuity Management Team, who shall maintain the overall business continuity plan. Information System Owners shall document their own business continuity plans. They shall have a complete understanding of their dependencies on IT, sites and buildings, staff and third parties, and the costs involved. DigiPlex IT shall ensure that disaster recovery plans are in place to support business continuity management requirements for IT.

Disaster recovery plans shall include any necessary off-site arrangements with third party service providers for critical systems. The business continuity and disaster recovery plans and copies of DigiPlex's information and software shall be securely stored and managed at two separate physical locations (at least), which are at a suitable distance apart to counteract disasters such as an aeroplane crash.

Business Continuity Planning Framework

The Business Continuity Management Team shall ensure that a single framework of business continuity plans is maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

DigiPlex will manage a disruptive event and will maintain its information security to a level, based on management-approved information security continuity objectives

17.1.3 Verify, review and evaluate information security continuity

Procedures shall be in place to regularly test, review and update business continuity and disaster recovery plans, to ensure that they are up-to-date and effective. The Business Continuity Management Team shall be responsible for ensuring that the overall business continuity plan is regularly tested, reviewed and maintained. Information System Owners and DigiPlex IT shall support this process by regularly testing, reviewing and maintaining their own plans. Regular testing of business continuity and disaster recovery plans shall be undertaken according to a planned timetable which has been approved by DigiPlex's Senior Leadership Team.

17.2 Redundancies

To ensure availability of information processing facilities. The redundancy levels of the key information processes shall be identified as well as the infrastructure they rely to meet availability requirements and reduce the business impact.

Based on the Business Impact Assessments, DigiPlex shall identify the business requirements for the availability of information systems. Where the availability cannot be guaranteed remediation plans should be drawn up.

Where applicable, redundant information systems shall be tested to ensure the failover from one component to another component works as intended.

18.0 Compliance

18.1 Compliance with legal and contractual requirements

18.1.1 Identification of applicable legislation and contractual requirements

DigiPlex shall regularly review new and changing legislation that affects its information security policy, and shall immediately implement relevant changes. Legal shall be responsible for providing advice and guidance to ensure that DigiPlex complies with its legal, statutory, regulatory and contractual obligations. The Information Security Management Committee shall regularly review legal obligations that influence this policy, and the Information Security Manager shall update policy as and when necessary. Information Systems Owners and DigiPlex IT shall maintain records of all legal, statutory, regulatory and contractual requirements relating to the IT network and information systems under their responsibility. **Further**

information is contained within DigiPlex Group Procedure MAN-PROC-04-00-DGS– Company Legal Register

18.1.2 Intellectual property rights

If not otherwise agreed, DigiPlex holds the rights to intellectual property to its employees.

All users shall comply with intellectual property rights and copyright legislation and contracts. Software used with DigiPlex's information processing systems shall only be used in line with the terms and conditions set.

DigiPlex IT shall manage software assets and licenses in line with the asset register requirements. DigiPlex IT shall use formal procedures to manage and protect software and licenses. Only appropriately licensed copies of commercial software shall be used and a register of licences shall be held by DigiPlex IT, with evidence of ownership.

Software and licenses shall be regularly audited for legal compliance. Users shall not copy and distribute software and hardcopy documentation that is copyright protected without authorisation from their Line Managers and DigiPlex IT.

18.1.3 Protection of records

DigiPlex shall implement and maintain records of its information assets to protect information from loss, destruction and falsification.

The policy and schedule shall address all legal, statutory, regulatory, contractual and business requirements of DigiPlex for the retention and disposal of information. They shall indicate information retention timescales, suitable methods of information storage, and information disposal requirements. This includes requirements for application data, documents, files, and audit trails, and valuable information that are stored in electronic, media and hardcopy formats. DigiPlex's Information Classification requirements shall be taken into consideration.

18.1.4 Privacy and protection of personally identifiable information

HR shall have responsibilities for implementing its legal requirements for data protection. This includes notifying the required regulators about DigiPlex's use of personal data, and documenting data protection policy, procedures and guidelines. Information System Owners shall immediately notify HR of any changes in their processes that involve personal information and that have legal consequences.

18.1.5 Regulation of cryptographic controls

DigiPlex IT shall ensure that cryptographic controls are used in compliance with all relevant agreements, laws, and regulations.

18.2 Information security reviews

18.2.1 Independent review of information security

DigiPlex's approach to managing information security, including policy implementation, effectiveness and compliance levels, shall be independently reviewed and documented at regular intervals, or when significant changes to the security implementation occur, via an internal audit programme.

18.2.1.1 Internal Audit

The Quality and Compliance Managerwill undertake Compliance Audits within Departments and on Operating Sites within the DigiPlex Group to ensure that statutory requirements, contractual requirements and good practice is being adhered to. The system audit on DigiPlex Group to ensure compliance with procedure will be undertaken at announced dates.

The Senior Manager or nominated representative of the area being audited will be made aware of the remedial measures required and will implement the necessary works. The Senior Manager will sign off the form to ensure the identified issues have been addressed.

18.2.1.3 External Audit

In addition to the audits carried out internally, we may be subject to inspections by Statutory Agencies, and / or the Client.

Further information is contained within DigiPlex Group Procedure QA-PROC-03-00-DGS – Management System Audits; QA-PROC-04-00-DGS– Internal Audits, QA-PROC-05-00-DGS- External Audits

18.2.1.4 Non-Conformance Action

All audit reports shall specify the corrective action (if any) necessary as a result of the audit. A programme for the corrective action shall be agreed by the audit team with the Line Manager/Supervisor as appropriate and a return visit made, after completion of the programme, to ascertain compliance. A supplementary report shall be issued detailing the results of the corrective action.

Further information is contained within DigiPlex Group Procedure QA-PROC-06-00-DGS, Incident, Non- conformances, Preventive and Corrective Action

18.1.2.5 Reviews

Continuous improvement in the Information Security Management is the goal. It is recognised that communication, such as by informing staff members of successes as well as failures, plays a vital part in motivating them to improve performance. To this end the ISMS provides for continuous Management Review to assess the degree of compliance with the performance standards and the effectiveness of the system. DigiPlex's Information Security Manager, supported by DigiPlex IT (as appropriate) shall be responsible for ensuring that this requirement is fulfilled. The results of these independent audits shall be reviewed by DigiPlex's Senior Leadership Team.

Further information is contained within DigiPlex Group Procedure MAN-PROC-07-00 –DGS Management Review

18.2.2 Compliance with security policies and standards

Information System Owners and Line Managers shall ensure that all security procedures within their areas of responsibility are carried out correctly to achieve compliance with this security policy, and its procedures and controls. All areas within DigiPlex shall be subject to review by the Information Security Manager to ensure compliance with this manual.

18.2.3 Technical compliance review

Information systems and the IT network shall be regularly checked for compliance with this manual, the Payment Card Industry Data Security Standard (as relevant), and with other security implementation standards, as defined by reputable information security industry sources, and taken on by DigiPlex to protect its information systems.

DigiPlex's network infrastructure and information processing systems shall be subject to regular independent technical compliance checks e.g. penetration testing and port scanning, including whenever significant changes are being implemented into the operational environment. These checks shall be carried out by a competent, authorised person(s) or third party organisation with specialist technical expertise. DigiPlex IT shall ensure that technical compliance checking is regularly undertaken.