Information Security Manual

PHX024

Contents

1. Document Control

1.1 Purpose of this Document

Information Security Management is an essential part of good IT governance, which in turn is a cornerstone in corporate governance. An integral part of the IT governance is information security, in particular pertaining to personal information.

The Information Security Manual documents the controls required for the Information Security Management System as required by ISO27001.

Core principles for information security management, as defined in ISO/IEC 27002, are adapted to the local situation for the following areas:

- Security Policies
- Human resource security
- Access control
- Physical and environmental security
- Communications security
- Supplier relationships
- Organisation of information security
- Asset management
- Cryptography
- Operations security
- System acquisition, development, and maintenance
- Information security incident management

1.2 Intended Audience

This document is intended for interested parties in the information security management system of Phoenix.

2. Security Policies

2.1 Policies for Information

Phoenix has defined the policies required for the Information Security Management System. The Information Security Policy is based on the following requirements:

- business strategy
- regulations, legislation, and contracts
- the current and projected information security threat environment.

The Information Security Policy contains statements concerning:

- definition of information security, objectives, and principles to guide all activities relating to information security
- assignment of general and specific responsibilities for information security management to defined roles

- processes for handling deviations and exceptions.

At a lower level, the Information Security Policy is supported by topic-specific policies, which further mandate the implementation of information security controls and are typically structured to address the needs of the organisation.

The information security policies are communicated to interested parties as relevant to the intended audience, e.g. for internal staff it's through communications, security awareness training.

2.2 Review of Policies for Information Security

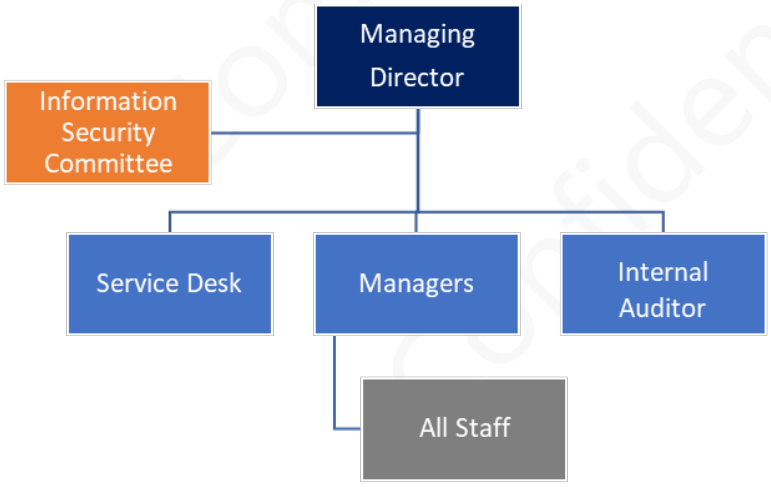
As part of the Information Security Management System the policies for information security are reviewed at twelve-month intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

The review of policies scheduled in the Information Security Schedule is covered as part of the Information Security Management Review.

3. Organisation of Information Security

3.1 Information Security Roles and Responsibilities

Phoenix top management has allocated the information security roles and responsibilities to address the requirements of the organisations Information Security Management System.



Managing Director

The MD is responsible for:

- determining the Information Security Objectives and providing adequate resources to ensure the effectiveness of the objectives
- assigning the responsibilities for Information Security
- sponsorship of the information security management system

- providing resources needed to implement the information security
- performing information security management reviews

Information Security Committee

The Information Security Committee holds primary responsibility for the information security at Phoenix ensures the information security polices and processes are established, communicated, and complied with throughout the organisation. The Information Security Committee is responsible for:

- publishing the Information Security Policy
- interpreting the business and information needs and wants of the organisation and translating them into information security activities
- ensuring that the information security management system is aligned to the strategic goals of the organisation
- ensuring information security is integrated into business planning
- developing policies, procedures, and standards to ensure the security, confidentiality and privacy of information is consistent with Phoenix information security policy
- monitoring and reporting on any information security incidents and developing strategies to prevent further incidents
- ensuring that information assets have been identified.
- implementing any changes as per the change control procedure
- ensuring the organisation's data is backed up and recovery of systems is documented and tested
- updating information asset inventory register
- defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of Phoenix information assets
- assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance
- contact with authorities
- authorising access to those who have a business need for information and ensuring access is removed from those who no longer have a business need for the information.
- Assessing risks associated with information security

The Information Security Committee consists of the following members and the list identify their roles within the Company and within the Information Security Committee:

Name:	Clare Metcalfe
Job Title:	Operations Director
Responsibility:	Head of the ISC and member of the Board – brings strong commercial knowledge plus experience of Systems Development discipline.

Name:	Trevor Hutchinson
Job Title:	Human Resources Manager
Responsibility:	BSI Liaison, brings knowledge of standards, communication, and interpersonal skills

Name:	Richard Barwick
Job Title:	Head of Service Delivery
Responsibility:	

Name:	Jane Singleton
Job Title:	Administration/Human Resources/Payroll Officer
Responsibility:	Documentation and procedures – brings knowledge of standards, organisational and communication skills

Name:	Geoff McGann
Job Title:	Governance Manager
Responsibility:	Maintenance and correlation of the standard.

Name:	Shaun Tosler
Job Title:	Infrastructure Manager
Responsibility:	Technical implementation – brings technical knowledge

Name:	Rebecca Tosler
Job Title:	Governance Administrator
Responsibility:	Administration and maintenance

Internal Auditor

The Internal Auditors are responsible for auditing the information security management system in accordance with the schedule.

The Internal Auditors are also responsible for making recommendations for reviewing the information security policies and making recommendations for improvements to the Information Security Committee.

Service Desk

System administrators are persons administrating Phoenix information systems and the information entrusted to Phoenix by other parties. Each type of information and system may have one or more system administrators. These are responsible for protecting the information, including implementing systems for access control to safeguard confidentiality and carry out backup procedures to ensure that critical information is not lost.

They will further implement, run, and maintain the security systems in accordance with the Information Security Policy.

Each system must have one or more system administrators. These are defined as follows:

System Name	Administrator(s)
Active Directory	Service Desk
Email	Service Desk
Intranet	Service Desk
External Website	Service Desk
Oasis	Kevin Wootton (Development)

Managers

Managers are responsible for:

- ensuring staff and contractors comply to the organisation's information security polices and manual
- providing guidelines for information security expectations of their employee's role within the organisation
- employees conforming to the terms and conditions of employment, which include the organisation's Information Security Policy and appropriate methods of working
- providing an anonymous reporting channel to report violations of information security policies or procedures
- ensuring staff comply with the Acceptable Use Policy

All Staff

Employees, third parties and contractors, accessing the information assets of Phoenix are responsible for:

- reporting security incidents, real or potential to the Information Security Committee
- complying with Phoenix Information Security Policy manual
- ensuring visitors are signed in and escorted while on site
- complying with Phoenix Acceptable Use Policy

3.2 Segregation of Duties

Phoenix headcount is not of a substantial size, as such segregation of systems is unachievable for all systems. Where segregation cannot be achieved additional controls such as audit logging and supervision are implemented.

Administrators have been assigned as per 4.1.

3.3 Contact with authorities

Contact with authorities is the responsibility of the Information Security Committee.

Authorities can be contacted as required relating to security incidents, business continuity, changes in law/regulations.

Authorities identified as relevant to information security include the following:

- police authority
- Information Commissioner's Office
- government agencies
- third parties

3.4 Contact with special interest groups

Maintaining appropriate contacts with special interest groups and/or specialist security forums as a means to:

- improve knowledge about best practices and stay up to date with relevant security information
- ensure the understanding of the information security environment is current and complete
- receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities
- gain access to specialist information security advice

Examples of special interest groups

- http://www.iso27001security.com/
- https://groups.google.com/forum/#!forum/iso27001security
- http://www.iso27001usergroup.co.uk/
- https://www.linkedin.com/groups?gid=143328&trk=anet_ug_parent

3.5 Information security in project management

Information security should be integrated into the organisation's project management method(s) 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. The project management methods in use should require that:

- information security objectives are included in project objectives
- an information security risk assessment is conducted at an early stage of the project to identify necessary controls
- information security is part of all phases of the applied project methodology.

Information security implications should be addressed and reviewed regularly in all projects. Responsibilities for information security should be defined and allocated to specified roles defined in the project management methods.

3.6 Mobile device policy

When using mobile devices, special care should be taken to ensure that business information is not compromised.

This is documented in the Mobile Device and Teleworking Policy.

3.7 Teleworking

When connecting from remote locations special care should be taken to ensure that information is not compromised. This is documented in the Mobile Device and Teleworking Policy.

4. Human Resource Security

4.1 Screening

Prior to employment the following background verification checks are performed for candidates:

- a verification (for completeness and accuracy) of the applicant's curriculum vitae – checked by the interviewer and HR Department
- where deemed applicable employment references are requested. The typical employment request response now consists of confirmation of dates employed, position fulfilled and reason for leaving. These typical responses are mirrored by Phoenix Software in responses relating to our former employees.
- where deemed applicable Social Media information is referenced e.g. LinkedIn
- identity verification (passport or similar document) – checked by HR, this also is required to prove eligibility to work in the UK

When an individual is hired for a specific information security role, the candidate is checked to ensure they have the necessary competence to perform the security role

4.2 Terms and conditions of employment

The contractual obligations for employees are stated in their contract of employment and Company Handbook. Contractors are required to agree and sign a Phoenix Non-Disclosure Policy.

The organisation ensures that employees and contractors agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to Phoenix assets associated with information systems and services.

Responsibilities contained within the terms and conditions of employment continue for a defined period after the end of the employment

4.3 Management responsibilities

If employees and contractors are not made aware of their information security responsibilities, they can cause considerable damage to an organization. Motivated personnel are likely to be more reliable and cause fewer information security incidents.

Poor management can cause personnel to feel undervalued resulting in a negative information security impact on the organisation.

Manager's responsibilities are listed in 4.1.

4.4 Information security awareness, education, and training

In order for the Phoenix information security program to operate, all employees and contractors are made aware of their responsibilities for information security.

Information security education and training is used to cover the general aspects such as:

- stating management's commitment to information security throughout the organisation
- the need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts, and agreements
- personal accountability for one's own actions and inactions and general responsibilities towards securing or protecting information belonging to Phoenix and external parties
- basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and orderly desks)

Initial education and training is conducted for all new starters with general updates. E learning is initiated for all staff on information security topical subjects.

Training records are maintained for all employees by the training department.

4.5 Disciplinary process

Employees who have committed an information security breach may have disciplinary action taken against them as outlined in the disciplinary process. All policies and procedures are available in the Company Handbook / SharePoint.

4.6 Termination or change of employment responsibilities

Responsibilities and actions are detailed within the Systems Access Control Policy

5. Asset Management

5.1 Inventory of assets

As part of the Information Security Policy, assets associated with confidentiality, integrity and availability of information must be identified and documented in an inventory.

The following are examples of Phoenix assets that should be taken into account on the inventory of assets:

- hardware - laptops, desktops, servers, printers, networks, mobile phones
- software - purchased software, freeware, bespoke applications

- data - not limited to electronic media (databases, PDF's, office applications, and other formats), but also in paper and other forms
- Infrastructure - offices, utilities, air conditioning - these assets can affect the availability of information
- employees - information retained by personnel is considered an asset
- Outsourced services - legal services, cleaning services, disposal services

The Inventory of Assets is the responsibility of the Information Security Committee, who in conjunction with departmental heads, will identify the assets as part of the risk assessment process.

This covers:

- software that the department uses
- people working in the department
- data stored electronically and in other forms
- equipment used by the department

The Asset Inventory is located on SharePoint.

5.2 Ownership of assets

All assets identified must be assigned an asset owner.

The owner of the asset is the person(s) that utilise the asset and who makes sure the information related to the asset is protected, for example:

- the owner of a system would generally be the system administrator
- the owner of data would generally be the person that created the data
- the employee would be the responsibility of the departmental head

The asset owner should:

- ensure that assets are inventoried
- ensure that assets are appropriately classified and protected
- define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies
- ensure proper handling when the asset is deleted or destroyed.

Owners have approved management responsibilities for the asset; however owners do not have property rights.

5.3 Acceptable use of assets

Employees and external party users using or having access to Phoenix assets are made aware of the information security requirements. They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility.

This is documented in the Acceptable Use Policy and re-enforced through staff awareness.

5.4 Return of assets

A formal process, owned by the HR department is in place to ensure that all Phoenix Software's assets, both physical and electronic, are returned at termination of employment, contract, or agreement. This is documented in the Systems Access Control Policy.

5.5 Classification of information

Phoenix provides IT services for a variety of customers across the UK. As part of information security Phoenix has adopted the following classification for the protection of assets from unauthorised access, compromise, or disclosure

Description	Examples	Marking	Can I send by email?	Can I remove from site physically or electronically?	Does it need secure disposal?
PUBLIC					
Information is not confidential and can be made public without any implication for the company. Documents are not marked as Public	• Marketing Material • Published Annual Accounts • Web Sites	None	Yes	Yes	No
COMPANY CONFIDENTIAL					
Business data relating to Phoenix employees, customers, and suppliers. A breach of confidentiality could cause serious implications to the business. Documents are marked as Company Confidential	• Emails containing company confidential data • Customer contact and account data • Customer price lists • Invoices • Phoenix created contracts • Proposals/tenders • Purchase orders • Quotes • Sales orders • Supplier costing	Yes Company Confidential	Yes – with care	Yes – with care	Yes Physical – destruction Digital – user deletion to make 'beyond use'

Description	• Examples	Marking	Can I send by email?	Can I remove from site physically or electronically?	Does it need secure disposal?
STRICTLY CONFIDENTIAL					
Highly sensitive or valuable information. Unauthorised access could influence the Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer and employee confidence. Information integrity is vital. Documents are marked as Strictly Confidential	• Accounts data and internal financial reports • All company developed software code whether used internally or sold to customers • Company business plans • Legal Documents • Password and security processes • Salaries and personnel data	Yes Strictly Confidential	Yes Auto protects by not allowing the recipient to forward, copy or print the email unless actively disabled by the sender	Yes Physical - within a sealed envelope Digital - with encryption/ password protected	Yes Physical – destruction Digital – user deletion to make 'beyond use'

5.6 Labelling of information

The asset owner is responsible for ensuring the asset is correctly labelled, this can be performed on the asset itself or the assets container. Finance/Service Desk are responsible to asset tagging physical IT devices.

Labels should be marked in an appropriate manner, for example:

- Physical items may be placed into a box with the marking on the outside
- Emails marked using the Sensitivity tags

Information identified as Public does not require marking.

5.7 Handling of assets

As part of information security it is important all staff are familiar with the handling of assets for processing, storing, and communicating information.

The following items are considered based on the classification levels:

- maintenance of a formal record of employee's assets
- copies of information are protected to a level consistent with the protection of the original information
- storage of IT assets in accordance with manufacturers' specifications
- clear marking of all copies of media for the attention of the employee

The rules in place for handling information assets are as follows:

	Unclassified	Public	Company Confidential	Strictly Confidential
Electronic Documents	No rules	Marked Public No rules	Marked Company Confidential	Marked Strictly Confidential
Systems	No rules	No rules	Access controls in place to restrict access only to relevant roles.	Access controls in place to restrict access only to relevant roles.
Paper Documents	No rules	No rules	Not to be removed from premises.	Not to be removed from premises.
Verbally transmitted (externally)	No rules	No rules	Contractual restrictions in place	Contractual restrictions in place
Email (external)	No rules	No rules	Contractual restrictions in place. TLS connection between email servers exist.	Contractual restrictions in place TLS connection between email servers exist. Does not allow forward, print, copy – read only

5.8 Management of removable media

All removable media is logged by Device Control software that runs in the anti-virus software on each company device. If removable media is used it produces an e-mail alert to the monitored mailbox managed by the Service Desk.

Where appropriate, an investigation is then made into tracing the asset back to the owner and check what the owner of the asset was doing at that time. If the action deviates from the Acceptable Use Policy, Service Desk escalate the incident to the ISC.

5.9 Disposal of media

Disposal of media is performed by a third-party company with security screened staff. There are two categories of media that require disposal.

- digital media - which is stored securely in the warehouse and collected by a third-party company who carry out media removal and asset destruction
- paper media - collected by a third-party company who carry out disposal services

Digital media devices are identified as obsolete. They are marked accordingly on the asset register and removed to the security cage in the warehouse. Once the devices are collected from the warehouse by the third-party company the assets are moved to the End of Life tab on the asset register. The asset details are provided to the management accounting team.

Certificates of destruction are supplied to complete a secure chain of custody.

Paper media classed as non-confidential is collected from the recycling bins across the company. A third-party company makes regular collections to dispose of the recyclable materials. Paper media classed as confidential is shredded by the owner.

This includes HR, Management Accounts, Payroll and Directors. The shredded paper is collected by a third-party company on a regular basis.

5.10 Physical media transfer

Media containing information must be protected against unauthorised access, misuse, or corruption during transportation.

Phoenix does not transport a large amount of physical media however when doing so the following applies:

- approved couriers are used for transporting media
- packaging is of an adequate level to protect against physical damage in line with manufacturer's guidelines
- data is encrypted where possible e.g. physically transporting removable media

6. Access Control

To limit access to information and information processing facilities Phoenix has implemented a System Access Control Policy.

The policy has taken into account the following:

- security requirements of business applications
- policies for information dissemination and authorisation, e.g. the need-to-know principle and information security levels and classification of information
- relevant legislation and any contractual obligations regarding limitation of access to data or services
- management of access rights in a distributed and networked environment which recognizes all types of connections available
- segregation of access control roles, e.g. access request, access authorization, access administration
- Multi-factor Authentication is used when accessing company and customer systems where appropriate
- requirements for formal authorisation of access requests
- requirements for periodic review of access rights
- removal of access rights
- archiving of records of all significant events concerning the use and management of user identities and secret authentication information
- roles with privileged access

7. Cryptography

7.1 Policy on the use of cryptographic controls

Cryptographic keys are used for the following:

- confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted
- authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities, and resources

Within Phoenix the use of cryptographic keys are limited to the following:

- SSL Certificates – Used by Phoenix to verify the authenticity and encrypt data during transit from externally facing websites.
- laptop encryption – Used to ensure the confidentiality of data stored on company laptops
- SSL Certificate (TLS) – Used by Phoenix Software's external email gateway to confirm
- authenticity and encrypt data during transit between third parties and Phoenix email servers.

7.2 Key management

All private keys within Phoenix are the responsibility of the Service Desk Department to manage.

Only members of the Service Desk Department have the authority to request externally generated keys on behalf of Phoenix Software.

To minimise management overhead of SSL certificates, a wildcard certificate is used for externally facing services; this is a single certificate that can be used for any hostname of the registered domain.

Laptops are encrypted. Recovery keys are stored within Sophos Safeguard and are accessible only by members of the Service Desk Department

8. Physical and Environmental Security

8.1 Physical security perimeter

Phoenix is a single office location in a detached building on Allerthorpe Business Park, York Road, Pocklington, York with limited access out of business hours.

The grounds are covered by CCTV which is serviced by SWAT.

Should third parties e.g. police, fire brigade, require access to CCTV footage, requests are directed to the HR Manager.

8.2 Physical entry controls

The building has eleven external doors all controlled by an access control system.

All visitors are required to sign in at Reception and are issued with a visitor's badge. Visitors must wait in the Reception area until their host comes to escort them.

Each employee is issued with an access fob to access the building. These are issued on their first day of employment. Loss of a fob must be reported to the HR Department immediately. The HR personnel will disable the lost fob and issue a replacement. Should the lost fob be found, it must be handed in to the HR Department.

If a fob has been forgotten but not lost, the employee must report to Reception and manually sign in and out the building throughout the day.

All employees are issued with a name badge and are encouraged to wear this for general identification purposes. If a badge is lost the employee must report to the HR Department for a replacement badge to be approved.

8.3 Securing offices, rooms, and facilities

Within the building additional security is in place for the following areas:

Name	Description	Access control
HR/Payroll Department	Used by the Human Resources/Payroll department	Secure keypad entry
Communications Room	Used for telephone system located on site.	Secure Fob Access
Main Server Room	Used for physical servers located on site.	Secure Fob Access
IT Services Office	Office for Service Desk, IT Consultants & IT Services Project Management	Secure Fob Access
Server Room – Sales Hub	Used for physical servers located on site.	Secure keypad entry

Only relevant personnel for each office have the entry codes or IT Services Department for the access via the secure fob.

8.4 Protecting against external and environmental threats

Phoenix office is a modern unit and is not situated in an area that is prone to adverse weather conditions such as flooding.

The office has been prone to a moderate level of power cuts resulting in the installation of a generator, to protect against an interrupted electricity supply.

The office is covered by intruder, fire, and smoke alarms. The intruder alarm is monitored by a dual path signalling system which incorporates BT Redcare and a GMS radio signal which notifies the relevant authorities and members of staff in the event that an alarm is triggered.

Additional controls are in place for the server room, including air conditioning, UPS backup and a gas suppression system.

The external threat protection is covered by a multi-layer approach which incorporates:

- Firewall Intrusion Protection Service
- Firewall Gateway Anti-Virus protection
- Client device Anti-Virus protection
- Client device Anti-Malware protection

Each of these 4 components have been configured to alert a shared mailbox which is monitored by the central SIEM.

Phoenix also utilise 2 internet connections in the event that a denial-of-service attack is experienced on a specific published IP address in addition to providing physical resilience of a data transport outage.

8.5 Working in secure areas

Secure areas within Phoenix have access controls to limit access. Due to this, employees should avoid working in secure areas without informing their manager.

Secure areas within Phoenix must be locked when not in use.

8.6 Delivery and loading areas

Deliveries are restricted to Reception and are controlled by Receptionists and Administration staff.

Delivery drivers are not allowed access into the building beyond Reception unless supervised by an employee at all times.

8.7 Equipment siting and protection

To reduce the risks from environmental threats and hazards the following has been considered:

- equipment is sited to minimize unnecessary access into work areas – Phoenix is a single office building with all equipment required for day-to-day use within easily accessible locations for users
- information processing facilities handling sensitive data is positioned carefully to reduce the risk of information being viewed by unauthorised persons while in use
- employees dealing with sensitive data are positioned so that their monitors are not viewable where possible
- storage facilities are secured to avoid unauthorised access
- controls are adopted to minimize the risk of potential physical and environmental threats, e.g. theft, fire, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, and vandalism
- Phoenix is a modern office building with alarms for smoke and fire

- critical systems are covered for electrical failures by the use of UPS's and generator
- guidelines for eating, drinking, and smoking in proximity to information processing facilities are established – Phoenix is a no smoking building. Food and drink are expressly forbidden in the Server and Communications room
- environmental conditions, such as temperature, are monitored for conditions which could adversely affect the operation of information processing facilities

8.8 Supporting utilities

Phoenix has put the following measures in place to protect against failures from supporting utilities:

- the air conditioning unit for the Server/Communication Rooms are sealed units which are covered by a maintenance agreement
- the septic tank is emptied every six months and the supporting pumps are covered by a maintenance agreement
- equipment will only be connected to the mains power supply if it is fit for purpose - PAT is carried on an annual basis
- UPS's are installed for all server room equipment and are tested regularly
- backup generator is installed for failure of electricity supply

8.9 Cabling security

Phoenix cabling security consists of:

- all cabling is Cat 5e and 6e
- cabling is concealed – either running under the floor or in cable coverings
- patch panels are secured against unauthorised access
- power and communication lines into the building are located underground

8.10 Equipment maintenance

To ensure the continued availability and integrity of assets, equipment in use by Phoenix must be maintained in accordance with suppliers recommended service intervals.

This includes:

- IT servers – covered by manufacturer maintenance or additional third-party maintenance
- air conditioning – covered by a regular maintenance agreement
- PAT - to ensure equipment does not suffer from electrical issues or damage to cabling
- fire and smoke alarms and extinguishers
- UPS – UPS's are tested on regular basis and covered by an adequate service contract
- generator – regular maintenance checks carried out

8.11 Removal of assets

All users of mobile devices are authorised to take equipment offsite as per the Mobile Device and Teleworking Policy.

All additional assets being removed from site must be logged in the removal of assets log once authorisation has been obtained from the asset owner.

8.12 Security of equipment and assets off-premises

This is detailed in the Acceptable Use Policy.

8.13 Secure disposal or re-use of equipment

All media containing information are securely disposed of using a third-party company to ensure all disks are physically destroyed.

For re-use of equipment the original user's data is removed prior to re-use.
The original users' data is copied back to their home directory which after twelve months it is archived off to the backup server.

8.14 Unattended user equipment

When equipment is not in use it must be secured against unauthorised access. All users must ensure unattended computer equipment is logged out or locked. Automatic password lock is configured on client devices after 10 minutes.

8.15 Orderly desk and clear screen policy

This is detailed in the Acceptable Use Policy

9. Operations Security

9.1 Change management

Changes to IT systems must be approved prior to release. This includes changes to bespoke systems, off the shelf server applications and infrastructure changes.

Change Request forms are generated for all proposed changes relating to internal services and must be approved by a Director. Change control notices within the Systems Development Team must be signed off by the project owner.

The change request forms cover the following:

- identification and recording of significant changes
- planning and testing of changes
- assessment of the potential impacts, including information security impacts of such changes
- formal approval procedure for proposed changes
- verification that information security requirements have been met
- communication of change details to all relevant persons
- fall-back procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events

Emergency changes to systems can be made with approval from the Managing Director.

9.2 Capacity management

The capacity of servers is monitored by the Service Desk department on a daily basis to ensure sufficient capacity for current and future use without impacting users.

Monitoring of the servers is performed utilising industry standard monitoring software.

9.3 Separation of development, testing and operational environments

Development and testing activities can cause serious problems, e.g. unwanted modification of files or system environment or system failure. There is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access to the operational environment.

Within Phoenix the development and testing environments are separate to the live environment.

Where possible, changes to systems and applications are performed in the testing environment prior to release.

Transfer of changes from the development environment is only be performed after testing has been completed and a change request has been approved.

9.4 Controls against malware

Phoenix has multiple levels of protection against malware, these include:

- protection against malware from the internet – Phoenix has a firewall implemented to ensure all downloads are scanned
- protection against malware from emails – all emails are scanned using industry standard software to ensure protection against malware
- local protection – all client and server operating systems are configured with local malware scanners as a last line of defence

9.5 Information backup

Backup covers all production servers to the backup server local disks – the backup server is a separate physical server.

This is designed to facilitate data recovery if we lose a single server, file, or folder. The infrastructure would still function as expected.

Backup and Replication software is utilised to allow recovery of virtual servers at the local site and also at the recovery site.

Servers are backed up on an incremental basis on a daily schedule with a full back up each Friday to local network attached storage.

Servers that run critical services are replicated every ten minutes during the daytime hours of 07:00 to 17:30 to the recovery site. This is designed to facilitate the full server recovery and give the most up to date version of the server.

The evening backup routine also copies new data from the critical servers to the recovery storage at the recovery site immediately, this is a copy of the backup only.

All backups are checked via e-mail notification in a monitored mailbox. The backup status is recorded in the Daily Infrastructure Check document.

All physical servers are backed up on a daily basis. A single server which offers hosted services has been converted into a virtual state and is left in a stand-by state. This virtual file format is replicated by industry standard software onto the recovery storage and can be mounted as required.

Backup data is retained as follows: public files are stored for two months; home and profile data is stored for two weeks. All other data is stored for one week.

Replication data is preserved for one business day at the DR location (this occurs on a two-hour frequency).

We use our DR site for an off-site copy of our data for 24 hours in case we lost our backup server or our copy backup server at head office.

All data that is backed up is not accessible by staff as access is limited to administrators only. If a restore request is made, then data is restored to the user's home drive as per the call logged.

Sensitive data is only held in our replicated databases which are not accessible by clients on the production network without a change in DNS records (authorised by the Board in a DR scenario) at head office or access to the VDI desktop at the DR site. The databases are also in a standby state unless they are brought online for access by clients.

9.6 Event logging

Event logging is configured using Group Policies applied to the domain.

Where possible, events logged should include the following information:

- user IDs
- system activities
- dates, times, and details of key events, e.g. log-on and log-off
- device identity or location if possible and system identifier
- records of successful and rejected system access attempts
- records of successful and rejected data and other resource access attempts
- changes to system configuration
- use of privileges
- use of system utilities and applications
- files accessed and the kind of access
- network addresses and protocols
- alarms raised by the access control system
- activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems
- records of transactions executed by users in applications

9.7 Protection of log information

To safeguard logs being overwritten due to capacity issues on the local server all security logs for servers within Phoenix are stored centrally using a syslog server.

This ensures that log information is retained and also protects against accidental / malicious changes to logs.

9.8 Administrator and operator logs

It is the responsibility of the Head of IT to review administrator logs where they are available, to maintain accountability for privileged access.

9.9 Clock synchronisation

Phoenix operating systems provide clock synchronisation by default with all client devices configured automatically to connect to a domain controller. Domain controllers are configured to use a trusted external time source.

The CCTV system clock operates under the Universal Time Zone (UTZ) and is checked on a regular basis for time synchronisation, age of footage, and image quality.

9.10 Installation of software on operational systems

For installation of software onto operational systems the following rules apply:

- the updating of the operational software, applications and program libraries is only to be performed by trained administrators upon appropriate approval from a Director.
- live systems only hold approved executable code and not development code or compilers
- applications and operating system software are only to be implemented after extensive and successful testing; the tests cover usability, security, effects on other systems and user - friendliness and are carried out on separate systems where applicable
- it is ensured that all corresponding program source libraries have been updated
- a configuration control system is used to keep control of all implemented software as well as the system documentation
- a rollback strategy is in place before changes are implemented
- an audit log is maintained of all updates to operational program libraries
- previous versions of application software are retained as a contingency measure
- old versions of software are archived, together with all required information and parameters, procedures, configuration details and supporting software for as long as the data is retained in the archive

Vendor supplied software used in operational systems is maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. Phoenix considers the risks of relying on unsupported software.

Any decision to upgrade to a new release takes into account the business requirements for the change and the security of the release, e.g. the introduction of new information security functionality or the number and severity of information security problems affecting this version.

Software patches are applied when they can help to remove or reduce information security weaknesses.

Phoenix uses Windows Update Services to deliver Windows critical updates, security updates, service packs and updates.

Additionally the Phoenix service desk engineer will also monitor a summary report for each server operating system against update classifications that failed or are needed on a daily basis. They will further investigate which machines still need updates and then recommend further action to the Service Desk Manager.

Physical or logical access is only given to suppliers for support purposes when necessary and with management approval. The supplier's activities are monitored.

Computer software may rely on externally supplied software and modules, which are monitored and controlled to avoid unauthorised changes, which could introduce security weaknesses.

9.11 Management of technical vulnerabilities

The Service Desk Department performs technical vulnerability scans using technical vulnerability assessment tools.

Where issues are found these are recorded on the Risk Assessment report and treated in accordance with the Risk Management Policy.

9.12 Restrictions on software installation

Within Phoenix, installation of software is performed by the Service Desk Department to ensure that software is authorised and is correctly licensed for use within the organisation.

This is detailed in the Acceptable Use Policy.

9.13 Information systems audit controls

To ensure effectiveness and accuracy of operational systems during internal audits the following rules are applied.

- audit requirements for access to systems and data are agreed with appropriate management/asset owner
- the scope of technical audit tests is agreed and controlled
- requirements for special or additional processing are identified and agreed
- audit tests that could affect system availability are run outside business hours

9.14 Cyber Security Defences

Phoenix employ a multi layered approach to defending against a cyber-attack. Perimeter protection covers:

- Intrusion Protection Services on all published resources (updated every 1 hour)
- Gateway Anti-virus (updated every 1 hour)
- Policy based routing of traffic to secondary internet connection

A secondary internet connection offers resilience to hosted web sites, mail routing and internet access and reduces the severity of a potential denial of service attack.

Anti-Malware/Virus Protection covers:

- Managed anti-virus is updated every 1 hour on servers and endpoints following definition updates.
- Managed anti-malware is updated every 1 hour on endpoints, which are polled using the same time interval.

By using separate anti-virus and anti-malware vendors Phoenix is further protected against newer threats.

10. Communications Security

10.1 Network controls

The Service Desk Department is solely responsible for network services. The following network controls are in place;

- network devices are managed by using built in software on the devices
- network devices default passwords are changed
- access to the management consoles for network devices is restricted to members of the Service Desk Department
- Wi-Fi connections in the office are protected from unauthorised access
- management activities should be closely coordinated both to optimize the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure
- appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security

10.2 Security of network services

Network services providers must have a service level agreement in place to ensure the effectiveness and accountability of network services.

Please see Information Services SLA.

10.3 Segregation in networks

The network within Phoenix is segregated as follows:

Network Name	Function
Server Network	Used for all production servers, including domain controllers and line of business
Client network	Used for client devices
Voice	Used for telecoms systems
Test & Development	Used for test and development purposes
DMZ Network	Network for externally facing servers
Mobile Devices	Mobile Devices

Phoenix facilitate two wireless networks; a wireless network for staff which connects to the client network and a visitor wireless network that has no access to any location within Phoenix but can access the internet.

Both wireless networks require authentication prior to use.

10.4 Information transfer policies and procedures

Information transfer may occur through the use of a number of different types of communication facilities, including electronic mail, voice, and video.

When transferring information all staff must be aware of their security obligations.

This is detailed in the Acceptable Use Policy.

10.5 Agreements on information transfer

Dependant on the agreement of Information Transfer type, one or a multiple of the following are taken into account.

- management responsibilities for controlling and notifying transmission, despatch, and receipt
- procedures to ensure traceability and integrity
- minimum technical standards for packaging and transmission
- reliable transport and courier companies are used
- responsibilities in the event of information security incidents, such as loss of data
- use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood, and that the information is appropriately protected
- technical standards for recording and reading information and software
- any special controls that are required to protect sensitive items, such as cryptography
- maintaining a chain of custody for information while in transit
- acceptable levels of access control

10.6 Electronic messaging

This is detailed in the Acceptable Use Policy.

10.7 Confidentiality or non-disclosure agreements

Confidentiality or non-disclosure agreements address the requirements to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements are applicable to external parties or employees of the organisation.

Phoenix confidentiality or non-disclosure agreements form a key part of all agreements with third parties, including suppliers, partners, and customers.

Only Directors and employees with direct authority from a Director have the authority to sign such agreements on behalf of Phoenix.

11. System Acquisition, Development, and Maintenance

11.1 Information security requirements analysis and specification

Information security requirements should be identified using various methods such as deriving compliance requirements from policies and regulations, threat modelling, incident reviews, or use of vulnerability thresholds. Results of the identification are reviewed by all the relevant stakeholders

Information security requirements and controls reflect the business value of the information involved and the potential negative business impact which might result from lack of adequate security.

Identification and management of information security requirements and associated processes are integrated in early stages of information systems projects. Early consideration of information security requirements, e.g. at the design stage, can lead to more effective and cost-efficient solutions.

Information security requirements also consider:

- the level of confidence required towards the claimed identity of users, in order to derive user authentication requirements
- integration with existing authentication methods e.g. Active Directory
- access provisioning and authorisation processes, for business users as well as for privileged or technical users
- the required protection needs of the assets involved, in particular regarding availability, confidentiality, integrity
- requirements derived from business processes, such as transaction logging and monitoring, non-repudiation requirements
- audit logging
- requirements mandated by other security controls, e.g. interfaces to logging and monitoring
- recovery procedures

11.2 Securing application services on public networks

All external applications that store confidential information or require user input are configured with a certificate that verifies the identity of the domain and encrypts all data transmitted.

When designing application services that are externally facing the following considerations are taken into account.

- the level of confidence each party requires in each other's claimed identity, e.g. through authentication

- authorisation processes associated with who may approve contents of, issue or sign key transactional documents
- ensuring that communicating partners are fully informed of their authorisations for provision or use of the service
- determining and meeting requirements for confidentiality, integrity, proof of despatch and receipt of key documents and the non-repudiation of contracts, e.g. associated with tendering and contract processes
- the level of trust required in the integrity of key documents
- the protection requirements of any confidential information
- the confidentiality and integrity of any order transactions, payment information, delivery address details and confirmation of receipts
- the degree of verification appropriate to verify payment information supplied by a customer
- selecting the most appropriate settlement form of payment to guard against fraud
- the level of protection required to maintain the confidentiality and integrity of order information
- avoidance of loss or duplication of transaction information
- liability associated with any fraudulent transactions
- insurance requirements

The applications in use and the security measures taken are as follows:

Application Name and Description	**Security Measures**
Phoenix Solutions Platform (PSP) Online Procurement Portal for existing Phoenix customers	• SSL encryption • user registration required • Users must set the own password which meets complexity rules (at least one uppercase, one lowercase, and one-digit, minimum length of 8 characters) • Passwords are stored in a hashed form using RFC 2898 PBKDF2 with 10,000 iterations • Logins are disabled after 3 incorrect attempts • Common passwords are blacklisted and cannot be used
GDPR Website for opting in for marketing communications	• SSL encryption • User identifies with email address • Authentication is completed when user send email using same address (double opt in) • User is temporarily tracked using a GUID in store in a SQL database before the information is updated in Oasis
SWGFL (Sophos) Website for ordering Sophos products for the South West Grid For Learning	• SSL encryption • During checkout user enters contact details including name, address, email, and school • For authentication user must also enter a DFE number for this school, which is validated against government education database
SWGFL (BitDefender) Website for ordering BitDefender products for the South West Grid For Learning	• SSL encryption • User registers with SWGFL who capture all the contact details (this is a website maintained and hosted by SWGFL) • User authenticates at SWGFL who pass all contact details to out portal in HTTP POST • Contact details are validated using a shared secret and has of all details including time of authentication.
License Dashboard Portal	• HTTPS/TLS 1.2 • User accounts created by admin role(s)

	• Users must set their own password which meets configurable complexity rules (length, number of lower/upper/numeric/special chars) • Passwords are stored in a hashed form using ASP.NET Identity PBKDF2 (Password-Based Key Derivation Function 2) with HMAC-SHA1, 128-bit salt, 256-bit subkey, 1000 iterations • Configurable password expiry • Configurable prevention of reusing previous passwords • Configurable lockout on a number of unsuccessful login attempts • Sessions timeout after a configurable period of inactivity • All customer asset data is isolated and read-only • Depending on customer requirements, sensitive information

11.3 Protecting application services transactions

Information involved in application service transactions should be protected to prevent incomplete transmission, miss-routing, unauthorized message alteration, unauthorised disclosure, unauthorized message duplication or replay. This takes into consideration:

- the use of electronic signatures by each of the parties involved in the transaction – covered by the use of SSL certificates
- all aspects of the transaction, i.e. ensuring that:
- user's secret authentication information of all parties is valid and verified
- the transaction remains confidential - covered by the use of SSL certificates
- privacy associated with all parties involved is retained – Privacy policy is available on the company website
- communications path between all involved parties is encrypted - covered by the use of SSL certificates
- protocols used to communicate between all involved parties are secured - covered by the use of SSL certificates
- ensuring that the storage of the transaction details is located outside of any publicly accessible environment, e.g. on a storage platform existing on the organisational intranet, and not retained and exposed on a storage medium directly accessible from the Internet – All external facing servers are web application servers with data stored on a SQL server that is not accessible from the internet
- where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process

11.4 Secure development

Phoenix developers adhere to and verify that their code is in compliance with the Phoenix Secure Coding Guideline documents.

LD developers adhere to and verify that their code is in compliance with the LD Secure Development Guidelines documents.

All developers are responsible for maintaining the required knowledge to develop code that follows the secure coding guidelines. Online training is available to developers to help keep their secure development knowledge up to date and its use monitored.

It is paramount that security requirements are identified through the development lifecycle as outlined below.

Requirements

- security and privacy risk assessment – review the proposed solution and identify security and privacy risks
- define Quality Gates – define the minimum acceptable levels of security and privacy
- team peer review of requirements for potential security issues

Design

- Attack Surface Analysis – analyse the surface area of the application that is potentially open for attack
- Threat Analysis – based on the attack surface and known vulnerability types determine risks and establish appropriate mitigations
- team peer review of design for potential security issues

Development

- use Approved Software and Libraries – only use software and libraries that have been approved for use and keep software up to date
- where possible use a vulnerability analyser which notifies if any vulnerabilities are discovered in libraries used
- deprecate Unsafe Functions – analyse functions and API's, banning those determined to be unsafe
- use Static Analysis Tools – use source code analysis tools that can identify potential security vulnerabilities
- document security requirements / configuration – make sure any specific requirements or
- configuration that is needed to provide secure operation of the software is documented

11.5 System change control procedures

OASIS / PSP / Procurement Portal:

New functionality or changes to systems are raised as a request for development, as documented in the Phoenix Secure Coding Guideline document. Azure DevOps is used to track all defects and feature requests for all development projects. Changes are deployed to production once it they have passed the following test phases: Systems Testing, Critical Path Testing, and User acceptance testing. The Change Advisory Board have to authorise the change before it is deployed to production

Phoenix uses Windows Update Services to deliver Windows critical updates, security updates, service packs and updates.

Each day a list of new updates is sent via e-mail to a monitored mailbox. This mail is used on a weekly basis by a Service Desk team member to approve updates for company production servers. A change control document is then raised, and the production server is logged on to install the updates outside business hours on a Thursday.

Additionally, the Service Desk department team member will also monitor a summary report for each server operating system against update classifications that have failed. These are checked on a daily basis. They will further investigate which machines still need updates and then recommend further action to the Service Desk Manager.

License Dashboard:

Software is only released from Azure DevOps release pipelines which ensures versioning and traceability of a release through the whole software development lifecycle. Releases can only be made from builds of the software which are built on the clean build server and all automated tests (functional and security) have run and passed. Released software is stored in Azure DevOps and on an internal fileserver from a software release distribution point.

For the License Manager product all components are signed with our code-signing certificate which verifies the components have not been modified or tampered with after the build.
Before being deployed to the production environment releases are deployed to a "UAT" environment which is separate from the production and development environments. Releases are tested in this environment against copies of production data.

Additionally, for the License Manager product (which can be installed on customers premises) a cycle of internal live occurs before the general release. Internal live involves deploying the release to our internal SAM auditors for use in the managed service production environment and typically lasts for 2 weeks. This allows the release to be verified in a production environment before being made generally available.

11.6 Technical review of applications after operating platform changes

Operating platforms include operating systems, databases, and middleware platforms. The control is applied for changes of applications.

When operating platforms are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on organisational operations or security.

Prior to changing the operating platform the following must be performed:

- installation of the operating platform in the test environment – no changes are made to production environments before being fully tested
- review of application control and integrity procedures to ensure that they have not been compromised by the operating platform changes

- ensuring that notification of operating platform changes is provided in time to allow appropriate tests and reviews to take place before implementation
- testing of all business applications that have the potential to be affected by the change
- ensuring that appropriate changes are made to the business continuity plans
- approval is granted from the Directors

11.7 Restrictions on changes to software packages

Phoenix does not modify vendor supplied software, all software in use is based on the code released from the vendor or code developed in-house.

11.8 Secure system engineering principles

Server builds are implemented based on vendor and security industry best practice, which include:

- Installation of security updates (important, critical, and moderate level updates)
- schedule security update installation on a weekly basis
- minimising local administrators to service owners and Service Desk employees
- renaming the local administrator account
- installation of Anti-virus and scheduled weekly full scans with alerting on infections

Further documentation on secure development guidelines can be found in

- PHX041 Secure Coding Guideline
- PHX055 LD Secure Development Guidelines

11.9 Secure development environment

A secure development environment includes the people, processes and technology associated with system development and integration.

Azure DevOps

The Phoenix and License Dashboard development teams both use Azure DevOps to manage their requirements / bugs, source control and build pipelines. In addition, the License Dashboard team use the release pipelines in Azure DevOps to create and, where applicable, deploy releases into test environments.

Please see Azure DevOps ISO/IEC 27001:2013 certificate for the DevOps certificate of registration.

Phoenix and License Dashboard teams operate separate DevOps organizations and are isolated from each other.

Access to the License Dashboard and Phoenix Azure DevOps organizations are restricted to members of the development team and certain key internal stakeholders. Access is further restricted via Azure DevOps group membership to project administrators, project team members, external developers, stakeholders, and readers.

Who has access and their level of access is periodically re-evaluated.

11.10 Outsourced development

Where appropriate Phoenix Software may look to Outsource Development.

When this is required, due diligence is made to ensure the correct outsourcer is engaged. This involves, at minimum, the Phoenix Project Owner, and Technical Lead.

Projects vary in their documented requirements, but the following should be considered for inclusion:

- Signed Non-Disclosure Agreement
- Statement of Works
- Proof of Concept
- Functional Specification
- Deliverables and Timetables
- Acceptance and adherence of Phoenix secure coding practice
- Project Team – Internal and External
- Warranty and Support
- Costing and Timetables
- Director Sign Off

11.11 System security testing

In line with Phoenix coding standards and guidelines, where applicable, security testing is carried out within the development lifecycle.

Phoenix Development Team

Testing is executed by the System Test team using pre-determined test scripts which detail all the steps required along with the expected results for each step. Defects are logged in Azure DevOps (SDLC system used by the development teams) detailing the step(s) executed, the expected results and the actual results.

For internal systems the scripts include user access privacy and security testing as part of the test cycles.

For external systems the scripts include a check to ensure all client to server traffic is secure.

Static code analysis at compile time is performed by Microsoft Roslyn analysers which are added to the project being built. The analysers check the project for various design, naming, performance, maintainability, reliability, and security issues.

Automated testing is performed to ensure existing functionality has not changed (outside of the scope of the new development) or produces unexpected results.

License Dashboard Development Team

Security testing occurs at the following points in the development lifecycle

Code check-in

When code is added/updated/deleted from source control a build pipeline is triggered. The build pipeline performs the following actions:

- Compiles the source code
- Performs static code analysis (see below)
- Executes automated tests (see below)
- Packages the distribution

Static code analysis

Static code analysis at compile time is performed by Microsoft Roslyn analysers which are added to the project being built. The analysers check the project for various design, naming, performance, maintainability, reliability, and security issues. All our projects use a common analyser configuration file which sets all security issues to cause a build error which prevents the build pipeline progressing further. This configuration file is under source control so changes can be audited and monitored.

Automated tests

The automated test suites include both functional and security tests. The security tests are designed to ensure any security aspects e.g. authentication, role-based access controls are correctly implemented and haven't regressed. A failure of any automated test causes a build error which prevents the build pipeline progressing further.

Static vulnerability scanning

We use Snyk to perform vulnerability scanning of all 3rd party libraries used by our solutions and alerts if any vulnerability is discovered in a library we are using. Snyk also performs security static analysis of the codebase.

11.12 System acceptance testing

System Acceptance testing programs and related criteria are established for new information systems, upgrades, and new versions.

System Acceptance testing is defined as end-to-end testing where the testing environment is similar to the production environment.

As part of System Acceptance testing, navigation is performed through all the features of the software. Testing takes place to ensure all features function as intended, this is also known as end-to-end testing.

System Acceptance testing is performed as part of the development lifecycle and conducted by the testers as part of the project.

Automated acceptance testing is used in addition to manual testing in the License Dashboard team. Automated tests are written in Specflow which is a Behaviour Driven Development tool. Tests are written in a natural language which creates a shared understanding of how the system should behave based on real usage scenarios. A critical subset of these tests are run on every code modification and the full set run overnight. Any failures will halt the build pipeline and prevent the build from being released.

12. Supplier Relationships

12.1 Information security policy for supplier relationships

Third Parties access to Phoenix information assets are controlled to ensure that the third parties Information Security policies are compliant with the Information Security Management System of Phoenix.

This is determined by either addressing the issue within supplier agreements – see 13.2 - or should access be required by an ad hoc supplier for them to provide confirmation of their compliance.

12.2 Addressing security within supplier agreements

Supplier agreements are established and where applicable documentation is requested to support their Information Security status.

Vendor or distributors are not allowed to access Phoenix systems.

12.3 Information and communication technology supply chain

Supplier agreements are established and where applicable documentation is requested to support their Information Security status. Where a supplier is involved in a further supply chain, where applicable, documentation is requested for the supply chain Information Security status.

The company has long standing supplier relationships and also suppliers where one-off purchases will take place.

The request for the Information Security status on the one-off suppliers is unlikely as it will slow the purchasing process down to an unacceptable level outside of the majority of our customer's service level expectations.

Our long-standing suppliers are often global enterprise organisations such as Microsoft, VMware and Adobe where they do not issue this information easily and the company accepts the risk of trading with them without their Information Security status.

12.4 Monitoring and review of supplier services

Monitoring and review of supplier services ensures that the information security terms and conditions within the agreements are being adhered to.

The responsibilities of managing the relationship with the supplier falls to the Operations Department, this involves a service management relationship process between the organisation and the supplier to:

- monitor service performance levels to verify adherence to the agreements
- review service reports produced by the supplier and arrange regular progress meetings as required by the agreements
- provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures
- resolve and manage any identified problems
- review information security aspects of the supplier's relationships with its own suppliers
- ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

12.5 Managing changes to supplier services

All technology systems are undergoing continuous upgrade, change or repair.

Phoenix determines how to manage the changes within the technology systems. Items considered include:

- service enhancements
- bug fixes
- use of new technology
- new development tools
- enhanced security measures

13. Information Security Incident Management

To ensure that Phoenix minimises the damage from information security incidents and learns from them, it ensures that all information security incidents are reported, recorded, and investigated.

All employees are required to report any observed or suspected incident promptly to allow the issue to be fully investigated in order to reduce the risk of it re-occurring.

This is documented in the Information Security Incident Management Procedure.

14. Information Security Aspects of Business Continuity Management

14.1 Planning information security continuity

In the event of a crisis or disaster all Information Security controls and policies still apply. For example:

- in the event the file server needs restoring the security on the directories is maintained
- changes to infrastructure due to a DR situation is still governed by change control
- classifications rules still apply

14.2 Implementing information security continuity

Phoenix ensures that:

- an adequate management structure and competent personnel are in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence
- documented plans, response and recovery procedures are developed and approved, detailing how Phoenix manages a disruptive event and maintains its information security to a predetermined level, based on management-approved information security continuity objectives

According to the information security continuity requirements, Phoenix establishes, documents, implements, and maintains:

- information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools
- processes, procedures, and implementation changes to maintain existing information security controls during an adverse situation
- compensating controls for information security controls that cannot be maintained during an adverse situation

These are documented in the Business Continuity and Disaster Recovery Plan.

14.3 Verify, review, and evaluate information security continuity

Organisational, technical, procedural and process changes are reviewed in line with Phoenix Information Security Management Systems.

The Business Continuity Plan is reviewed at least annually or when significant changes to a system, processes or the organisation has taken place.

14.4 Availability of information processing facilities

Systems at Phoenix have an adequate level of redundancy based on the availability / criticality of the relevant system.

Redundancy measures in place:

- RAID used on all production storage
- UPS's are used on all production servers/hosts
- spare thin clients and laptops
- redundant power supplies for all production servers/hosts
- clustering is used for all production databases

15. Compliance

15.1 Identification of applicable legislation and contractual requirements

Compliance requirements comprise of:

- identification of applicable legal (statutory and/or regulatory) and contractual requirements that Phoenix complies with
- complying with Intellectual Property Rights
- complying with Phoenix Security Policy and other related ISMS policies/supporting processes (procedures)
- aspects such as safeguarding of organisational records, data protection and privacy

The Information Security Committee and other relevant staff e.g. HR, Senior Management are responsible for ensuring compliance based on their awareness and also seeking external advice when required.

Legislative/Contractual Requirement	Relevance
Data Protection Act 2018 General Data Protection Regulation (GDPR)	Under the GDPR, the data protection principles set out the main responsibilities. Article 5 of the GDPR requires that personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to individuals; b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate,

	having regard to the purposes for which they are processed, are erased or rectified without delay; e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures." Phoenix adhere to the above policy points when dealing with any personal data. The company DPA certificate number is Z4809807
UK Electronic Communications Act 2000	• SSL Certificates • Laptop Encryption • TLS utilisation
Freedom Of Information Act 2000	• This does have a direct impact on Phoenix. It does have an effect in relation to Government framework agreements where our Public Sector transactions may become transparent to the public when requested. The FOI has been a discussion point in the tendering process for Government procurement.
The Telecommunications (lawful Business Practice and Interception of Communications) Regulations 2000	• Understand usage trends • Facilities being misused and time wasted • Being in line with the company's Acceptable Use Policy, Monitoring section
Computer Misuse Act 1990	• The Company Handbook and Acceptable Use Policy both cover areas of misuse that are relevant to Phoenix Software
The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016	• A list of electronic signatures are kept within the marketing department. Each time an electronic signature is used, the signatory is asked for permission. The Electronics Signatures Regulations 2002 revoked and replaced by new act. December 2016
The Privacy and Electronic Communications Regulations 2003/Amendment 2011	• We do not use automated call facilities • Direct Marketing Communications are sent to subscribed customers who also have a choice to unsubscribe • Websites utilise Cookies
The Consumer Contracts Regulations June 2014	• Understand requirements of the regulations and ensure our online sites adhere • Our order confirmations from telephone orders contain the correct information as required • IT software is mainly delivered electronically and immediately via licence keys. This often negates the ability to return goods • Services contracts state customer cancellation rights of 28 days' notice
Civil Contingencies Act (2004) (UK Government)	• This Act is acknowledged and has been added to our risk register • Invoking of our Business Continuity Policy

Copyright and Rights in Database 1997 Regulations.	• The company holds customer data within an internally coded system called Oasis.
Business Continuity Practice Guide: 2006 (UK Tripartite Authorities: Financial Services Authority (FSA), HM Treasury, Bank of England)	• The company has a Business Continuity Plan • The company does not offer Financial Services products
Companies Act 2006 contains a number of provisions concerning records and communications	• The company complies with the Act pertaining to records and communications.
Regulations Investigatory Powers Act 2000 (RIPA)	• The company refers to this Act in the Acceptable Use Policy to investigate misuse or monitor standards.
The Human Rights Act 1998 (HRA)	• The Company is aware of the Human Rights Act 1988 • Protection against discrimination is dealt with in the Company Handbook
Supplier / Vendor Contract Agreements	• Adobe • Citrix • Microsoft • Oracle • VMWare • Arrow ECS • Other supplier/vendor agreements are in place, but the numbers are extensive so are not listed here. Operations, Accounts and Vendor Management departments handle these agreements between them.
Customer Contract Agreements	• Crown Commercial Services RM3733 Technology Products • Crown Commercial Services RM1058 Technology Services • Crown Commercial Services G-Cloud • KCS –incorporating CBC • Individual smaller customer agreements • License Dashboard Managed Service Customers

15.2 Intellectual property rights

Relevant employee's contracts of employment document the employee's obligations regarding Intellectual property rights.

License Dashboard Ltd, part of the Blenheim Group own code relating to the License Manager portfolio of products. Copyright for each product is held within each product. Relevant trademarks are held for License Manager and License Dashboard.

Internal use systems, such as Oasis, Purchasing and Holiday systems are wholly owned by Blenheim Group and covered by the limitations within the contract of employment.

15.3 Protection of records

Some records need to be securely retained to meet statutory, regulatory, or contractual requirements, as well as to support essential business activities. Examples include records that may be required as evidence that an organisation operates within statutory or regulatory rules, national law or regulation may set the time period and data content for information retention.

This is documented in the Data Retention Policy.

15.4 Privacy and protection of personally identifiable information

Processing of personal data must comply with the seven principles of the General Data Protection Regulation (GDPR) act which ensures:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

To determine what data is personal refer to the following document from the Information Commissioners Office, https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf

It is the responsibility of the HR Department to ensure the processing of personal data complies with the GDPR.

15.5 Regulation of cryptographic controls

Phoenix complies with all cryptographic controls where necessary, including the GDPR.

15.6 Independent review of information security

The internal auditor is responsible for reviewing the Information Security Management Systems and making recommendations for improvements to the Information Security Committee.

These recommendations should be documented and agreed as part of the Management Review process

15.7 Compliance with security policies and standards

The Information Security Committee identify how to review that information security requirements defined in policies, standards and other applicable regulations are met.

If any non-compliance is found as a result of the review the Information Security Committee will:

- log the non-compliance
- identify the causes of the non-compliance
- evaluate the need for actions to achieve compliance
- implement appropriate corrective action
- review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses

Results of reviews and corrective actions carried out by the Information Security Committee are recorded.

15.8 Technical compliance review

Technical compliance is reviewed with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist. This is alongside manual reviews (supported by appropriate software tools, if necessary) carried out by members of Service Desk

Version Control

Author	Version	Date	Description
ISC	1.0	01/07/2015	Original
ISC	10.0	12/10/2020	Full Review
ISC	11.0	30/09/2021	Full Review
ISC	12.0	03/08/2022	Amendments following annual review
ISC	12.1	25/04/2023	Update of Governance Manager & CCTV

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	01/07/2015	Managing Director
Sam Mudd	10.0	12/10/2020	Managing Director
Sam Mudd	11.0	30/09/2021	Managing Director
Clare Metcalfe	12.0	30/09/2022	Operations Director
Clare Metcalfe	12.1	25/04/2023	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 25/04/2023