Information Security Policy

Document Type: Policy (Internal)

Version: 1.3

Issue Date: 11th March 2019

Author: Lee Thompson

Contents

1. Context and Overview

Policy prepared by: Lee Thompson
Approved by: Lee Gregson
Policy became operational on: 1st April 2019
Next review date: 30th March 2020

Introduction

This policy is concerned with the management and security of the company's information assets (an information asset is defined to be an item or body of information, an information storage system or an information processing system) and the use made of these assets by its staff and others who may legitimately process data on behalf of the company.

Why this policy exists

An effective Information Security Policy is the basis for defining and regulating the management of our systems and information assets. This is necessary to ensure that information is appropriately secured against failures in confidentiality, integrity, availability and compliance that may otherwise occur.

Scope

The Information Security Policy applies to all information assets which are owned or used by the company and all members of staff who may process information on behalf of the company.

Information security principles

The company has adopted the following principles as the foundations of this policy:

1. Information will be protected in line with all relevant company policies and legislation, notably those relating to data protection, human rights and freedom of information.
2. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
3. Information will be made available solely to those who have a legitimate need for access
4. All information will be classified according to an appropriate level of security.
5. The integrity of information will be maintained.
6. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
7. Information will be protected against unauthorised access.
8. Compliance with the Information Security policy will be enforced.

2. Outsourcing and Third Party Compliance

This policy applies to any staff who are considering engaging a third party to supply a service where that service may involve third party access to the company's information assets. This third-party access could occur in a number of situations including:

1. Cloud computing services
2. Software or middleware development
3. Disaster recovery and business continuity facilities

Managing outsourcing risk

Prior to outsourcing or allowing a third-party access to the company's non-public information or systems, a decision must be taken by staff of appropriate seniority that the risks involved are clearly identified and acceptable to the company. The level of staff seniority will depend on the nature and scale of the outsourcing.

Formal outsourcing

Where a service is formally outsourced by the company, the process must be managed by the relevant staff and a contract must be in place that covers standards and expectations relating to information security.

Due diligence

The process of selecting a third-party service provider must include due diligence of the third party in question, a risk assessment and a review of any proposed terms and conditions to ensure that the company is not exposed to undue risk. This process may involve advice from members of the company's board of directors with expertise in contract law, IT, information security, data protection and human resources. This process must also include the consideration of any information security policies or similar information available from the third party and whether they are acceptable to the company.

Legal

All third parties who are given access to the company's information or systems must agree to follow the information security policies of the company.

3. Human Resources

For roles involving handling of strictly confidential information or accessing sensitive information systems, Human Resources may use a pre-employment or change of role screening process to help ensure that employees selected are suited to the demands of the position.

Employment contracts

All Employees are to sign a contract binding them to comply with the Rules of Conduct for members of staff and the Terms and Conditions of Employment which stipulates adherence to the company's Data Management and Information Security policies.

Employee termination

Upon termination, suspension or change of appointment, Human Resources will revise the staff record accordingly. This will trigger appropriate account management processes on centrally managed IT systems. Managers, however, should be aware that access to many sensitive systems is not yet automatically controlled and should make

appropriate requests for access, change of permissions or denial of access to the relevant system managers. Upon termination, all employees, contractors and third parties must return all information assets and equipment held which belong to the company.

Third party compliance

Precautions, in the form of a contract, should be taken to protect the information security interests of the company where external organisations or individuals are employed to work on company information systems or provided with or given access to confidential information.

4. Information Handling

Information assets must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation which would otherwise occur.

Ownership of information assets

An inventory of the company's main information assets will be developed and maintained with the ownership of each asset clearly stated. Each asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset. Each information asset will be assigned a security classification by the asset owner which reflects the sensitivity of the asset.

Disposal of information

Attention needs to be given to ensure that information assets are disposed of securely. Confidential paper waste must be disposed of in accordance with formal company procedures. Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the company, unless the disposal is undertaken under contract by an approved contractor. In cases where a storage system (for example a computer disc) is required to be returned to a supplier it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. If this is not possible, then the storage system should not be returned to the supplier and should remain in the possession of the company until it is disposed of securely.

Information on desks, screens and printers

Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times. Care should also be taken when printing confidential documents to prevent unauthorised disclosure. Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended.

Backups

Information owners must ensure that appropriate backup and system recovery measures are in place. Where backups are stored off site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.

Information exchange

Whenever significant amounts of personal data or other confidential information are exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by a formal written agreement with the third party. Information classified as strictly confidential may only be exchanged electronically both within the company and in exchanges with third parties if the information is strongly encrypted prior to exchange. Information classified as secret may not be transmitted electronically except with the explicit written permission of the information owner.

When exchanging information by email or fax, recipient addresses should be checked carefully prior to transmission. Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

Members of staff must not disclose nor copy any information classified as confidential or above unless they are authorised to do so.

Facilities

The company is obliged to maintain appropriate physical and logical site processes to ensure data, equipment and third-party stocks are secured. Only those staff and authorised contractors shall be granted access to the facility to deliver contracted services and whose role requires them to have such access, provided on the principles of minimum privilege and demarcation. Physical controls shall include, but not be limited to:

1. Fob-based electronic access control systems on all external and relevant internal entranceways
2. Logging of access requests
3. HD CCTV surveillance of all relevant areas of site, with recordings retained for a maximum of 14 days
4. Redcare monitored intrusion alarm systems
5. Security measures including: locked gates and compound, 360-degree lighting, ram posts.

5. User Accounts

Management of user accounts is essential in order to ensure that access to the company's information and information systems is restricted to authorised users

Privileges

Accounts will only be issued to those who are eligible for an account and whose identity has been verified. When an account is created, a unique identifier (userID) will be assigned to the individual user for his or her individual use. This userID may not be assigned to any

other person at any time except with written permission of the information owner. Such examples may be grouped accounts, designed for collaborative working.

On issue of account credentials, users must be informed of the requirement to comply with the company's Information Security policy. Access rights granted to users will be restricted to the minimum required in order for them to fulfil their roles.

Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately and in a timely manner to reflect any changes in a user's circumstances (e.g. when a member of staff changes their role or leaves the company).

Admin accounts are used for the management of information systems and are distinct from user accounts. These accounts may be used by system administrators when undertaking normal or specific tasks which require special privileges.

Password management

As part of the account provisioning process, the user will be informed of an initial, temporary password. This password must be communicated to the user in a secure way and must be changed by the user immediately. This change should be enforced automatically wherever possible.

6. Acceptable Use

Company information and communication facilities, including email addresses and computers, are provided for administrative purposes related to work or personal research at the company. Personal use is permitted provided that it does not interfere with the member of staff's work or contravene any company policies.

User identification

Each member will be assigned a unique identifier (userID) for his or her individual use. This userID may not be used by anyone other than the individual user to whom it has been issued. Each member will be assigned an associated account password which must not be divulged to anyone, for any reason. This company password should not be used as the password for any other service. Individual members are expected to remember their password and to change it if there is any suspicion that it may have been compromised. Each member will also be assigned a unique email address for his or her individual use and some members may also be given authorisation to use one or more generic (role based) email addresses. Members of staff must not assign their company email address to anyone else without explicit permission.

Connecting devices

In order to reduce risks of malware infection and propagation, risks of network disruption and to ensure compliance with security policies, it is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose. It is permissible to connect personally owned equipment to the company's wireless networks.

To further reduce risk of data loss, members of staff should not connect any personally owned peripheral device which is capable of storing data (for example, a personally owned USB stick) to any company-owned equipment, irrespective of where the equipment is located.

Any device connected to the company network must be managed effectively. Unauthorised devices are liable to physical or logical disconnection from the network without notice.

Equipment

Computers and other equipment used to access company facilities must not be left unattended and unlocked if logged in. Members must ensure that their computers are locked before being left unattended. Care should be taken to ensure that no restricted information is left on display on the computer when it is left unattended.

Particular care should be taken to ensure the physical security of company-supplied equipment when in transit.

Unacceptable use

In addition to the foregoing, the following are also considered to be unacceptable uses of company facilities.

1. Any illegal activity or activity which breaches any company policy.
2. Any attempt to undermine the security of company facilities. (For the avoidance of doubt, this includes undertaking any unauthorised penetration testing or vulnerability scanning of any company systems).
3. Providing access to facilities or information to those who are not entitled to access.
4. Any irresponsible or reckless handling of company data.
5. Any use which brings the company into disrepute.
6. Any use of company facilities to bully, harass, intimidate or otherwise cause alarm or distress to others.
7. Sending unsolicited and unauthorised bulk email (spam) which is unrelated to the legitimate business of the company.
8. Creating, storing or transmitting any material which infringes copyright.
9. Creating, storing or transmitting defamatory or obscene material. (In the unlikely event that there is a genuine business need to access obscene material, the company must be made aware of this in advance and prior permission to access must be obtained from the Research and Development Director.)
10. Creating, accessing, storing, relaying or transmitting any material which promotes terrorism or violent extremism or which seeks to radicalise individuals to such causes.
11. Using software which is only licensed for limited purposes for any other purpose or otherwise breaching software licensing agreements.
12. Failing to comply with a request from an authorised person to desist from any activity which has been deemed detrimental to the operation of the company's facilities.
13. Failing to report any breach, or suspected breach of information security to person or persons in authority.
14. Failing to comply with a request from an authorised person to change your password.

Penalties for misuse

Minor breaches of policy will be dealt with by heads of department and the board of directors may be informed of the fact that a breach of policy has taken place. More serious breaches of policy (or repeated minor breaches) will be dealt with under the company's disciplinary procedures Where appropriate, breaches of the law will be reported to the

police. Where the breach has occurred in a jurisdiction outside the UK, the breach may be reported to the relevant authorities within that jurisdiction.

7. System Management

The company's computer systems are managed by suitably skilled staff who oversee their day-to-day running and ensure on-going security, confidentiality, integrity and availability. These system managers will undertake their duties in collaboration with individual technical service managers whose services are running on these computer systems. This policy applies to all members of staff who use administrator (or elevated) privileges on any company multi-user computer system (server) to administer the system or the services running on the system.

Duties and responsibilities

System managers play a key role in ensuring the security of the company's systems and services. They are expected to be aware of the company's Information Security policy in its entirety and must always abide by the policy. System managers should assign a business criticality level to their systems and depending on the level of criticality, they are responsible for ensuring appropriate business continuity measures are in place to protect against events which might otherwise result in loss of service. They should also assign (and record) a confidentiality level to their systems which indicates the suitability, or otherwise, of using any individual system for the storage or processing of different categories of data. This is in order to allow data owners to make informed decisions as to whether the system meets their security requirements.

System managers are also responsible for ensuring the on-going security of their systems and must apply software patches in a timely manner (depending on the criticality rating of the vulnerabilities addressed by the patches and the level of exposure to the vulnerabilities). High priority patches must be applied in accordance with software suppliers' recommendations (or requirements) or within 30 working days of release, whichever is the shorter. If it is not possible to patch within this time period, other compensatory control measures must be taken to mitigate risk.

Change control

All changes to computer systems are subject to the company's change management processes and procedures.

Access control

Access to all computer systems must be via a secure authentication process, with the exception of read-only access to publicly available information. Wherever possible, authentication should be either via the company's domain and authentication service. Locally administered accounts should be avoided wherever possible. Access must only be granted in strict accordance with the User Management guidelines.

Administrator accounts and accounts with elevated privileges must only be used when necessary in order to undertake specific tasks which require the use of these accounts. At all other times, the principle of "minimum privilege" should be followed. Access to administrator accounts (whether direct or indirect) from untrusted networks (e.g. home) or when using personally owned devices should be protected by two-factor authentication wherever possible.

Monitoring and logging

The use and attempted use of all computer systems should be logged. The data logged should be sufficient to support the security, compliance and capacity planning requirements of the system but should not be unnecessarily intrusive. Users of systems should be given clear information of what information is recorded, the purposes of the recordings and the retention schedule of the data collected. This information should be made available to users in the form of a system specific privacy policy. Data protection legislation requires that any personal data collected is collected for specific purposes and that it should be deleted when it is no longer needed. It is recommended that log files are recorded on a different system from the system being monitored. Audit logs should be configured to record any actions undertaken using administrator or elevated privileges. Audit logs should be secured to protect them from unauthorised modification.

8. The Network

The network must be designed and configured to deliver high levels of performance, availability and reliability, appropriate to the company's business needs, whilst providing a high degree of control over access.

Security and Integrity

Networking and communications facilities, including wiring cabinets and computer rooms must be adequately protected against accidental damage (fire or flood, for example), theft, or other malicious acts. The network should, where appropriate and possible, be resilient to help mitigate the impact of the failure of network components.

Connecting devices

It is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose. It is permissible to connect personally owned equipment to the company's wireless networks. Any device connected to the network must be managed effectively. Devices which are not are liable to physical or logical disconnection from the network without notice. All devices connected to the network, irrespective of ownership, are subject to monitoring and security testing, in accordance with normal operational practices.

Address management

The allocation of network addresses (IPv4 and IPv6) used on the company network shall be managed by the network and infrastructure team, which may delegate the management of subsets of these address spaces to other teams within the company. Network addresses (IPv4 or IPv6) assigned to end-user systems will, wherever possible, be assigned dynamically (and will therefore be subject to change).

Access controls

Access to network resources must be strictly controlled to prevent unauthorised access. Access control procedures must provide adequate safeguards through robust identification and authentication techniques. The network and infrastructure team are responsible for the management of the gateways which link the company's network to the Internet. Controls will be enforced at these gateways to limit the exposure of systems to the Internet in order to reduce the risks of hacking, denial of service attacks, malware infection and propagation and unauthorised access to information. Controls will be applied to both incoming and outgoing traffic.

9. Software

All software, including operating systems and applications must be actively managed.

Installation

Checks should always be made that there is a valid licence before installing software and users advised of any special conditions regarding its usage. Automated installs should be used wherever possible in line with current procedures. Appropriate licence management procedures must be followed.

Regulation

Use or installation of unlicensed software and using software for illegal activities could be construed to be a disciplinary offence. Use of software which tests or attempts to compromise system or network security is prohibited unless authorised by the Research and Development Director. Use of software which causes operational problems that inconvenience others, or which makes demands on resources which are excessive or cannot be justified, may be prohibited or regulated. Software found on systems which incorporates malware of any type is liable to automated or manual removal or deactivation.

Maintenance

All changes to computer systems are subject to established change management processes and procedures. Software must be actively maintained to ensure that all fixes and patches, needed to avoid significant emerging security risks, are applied as promptly as possible - commensurate with the risk. High priority patches should either be applied within 30 working days of release or other compensatory control measures taken to mitigate risk. Systems running software, including the operating system, which are clearly not being maintained adequately and which may be presenting a wider risk to security are liable to have their network connectivity withdrawn.

Removal

Software that is not licence compliant must be brought into compliance promptly or uninstalled. Software that is known to be causing a serious security problem, which cannot be adequately mitigated, should be removed from service. Change control processes and procedures must be used, commensurate with the risk When decommissioning a computer system, for disposal or re-use, appropriate measures must be taken in relation to any software stored on it. Software must be removed, where not doing so could lead to breaking the terms of its licence.

10. Remote and Mobile Working

While recognising the benefits of permitting the use of mobile devices and staff working away from the office, the company also needs to consider the unique information security challenges and risks which will necessarily result from adopting these permissive approaches. In particular, the company must ensure that any processing of personal data remains compliant with data protection legislation.

Personal devices

A mobile computing device is defined to be a portable computing or telecommunications device which can be used to store or process information. Examples include laptops,

netbooks, smartphones, tablets, USB sticks, external or removable disc drives, flash/memory cards and wearable devices (such as iWatch).

Whilst the company does not require its staff to use personal devices for work purposes, it is recognised that this is often convenient and such use is permitted subject to users giving due consideration to the risks of using personal devices to access information and in particular, information classified as confidential.

The following requirements are mandatory in respect of personal devices and their use:

1. The device must run a current version of its operating system.
2. A current version is defined to be one for which security updates continue to be produced and made available to the device.
3. Mobile devices must be encrypted. (Some older devices are not capable of encryption and these should be replaced at the earliest opportunity.)
4. An appropriate passcode/password must be set for all accounts which give access to the device.
5. A password protected screen saver/screen lock must be configured.
6. The device must be configured to "autolock" after a period of inactivity (no more than 10 minutes).
7. Devices must remain up to date with security patches both for the device's operating system and its applications.
8. Devices which are at risk of malware infection must run anti-virus software.
9. All devices must be disposed of securely.
10. The loss or theft of a device must be reported to IT Services.
11. Any use of personal devices by others (family or friends) must be controlled in such a way as to ensure that these others do not have access to restricted company information assets.

Company devices

The company may provide computing devices to staff. When it does, it will supply devices which are appropriately configured to ensure they are as effectively managed as off-site and within the office environment. Devices supplied by the company must meet the minimum security requirements listed above for personally owned devices.

Loss

All members of staff have a duty to report the loss, suspected loss, unauthorised disclosure or suspected unauthorised disclosure of any company or relevant personal asset to any member of the network and infrastructure team immediately.

11. Investigation of use

The company respects the privacy of its staff and recognises that investigating the use of IT may be perceived as an invasion of that privacy. However, the company may carry out lawful monitoring of its IT systems when there is sufficient justification to do so and subject to authorisation at an appropriate, senior level.

Company powers to act

Authorised staff may access files and communications, including electronic mail files, stored on any IT facilities owned, managed or provided by the company and may examine

the content of these files and any relevant traffic data. The company may access files and communications for the following reasons:

1. ensure the operational effectiveness of its services (for example, the company may take measures to protect its systems from viruses and other threats).
2. establish the existence of facts relevant to the business of the institution (for example, where a case of suspected plagiarism is being investigated and there is sufficient evidence, the contents of an individual's communications and/or files may be examined without their consent with the authority of an authorised person).
3. investigate or detect unauthorised use of its systems.
4. ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the company's activity.
5. monitor whether or not communications are relevant to the business of the company (for example, checking email accounts when staff are absent, on holiday or on sick leave)
6. comply with information requests made under the relevant and applicable data protection legislation.

Agency powers to act

A number of other non-company bodies and persons may be allowed access to user communications under certain circumstances. Where the company is compelled to provide access to communications by virtue of a Court Order or other competent authority, the company will disclose information to these non-institutional bodies/persons when required as allowed under the Data Protection Act 1998. For example, under the Regulation of Investigatory Powers Act 2000 a warrant may be obtained by a number of law enforcement bodies regarding issues of national security, the prevention and detection of serious crime or the safeguarding of the economic well-being of the UK.

12. Changes to this Policy

We reserve the right to change this policy at any time without notice to you so please check regularly to obtain the latest copy.