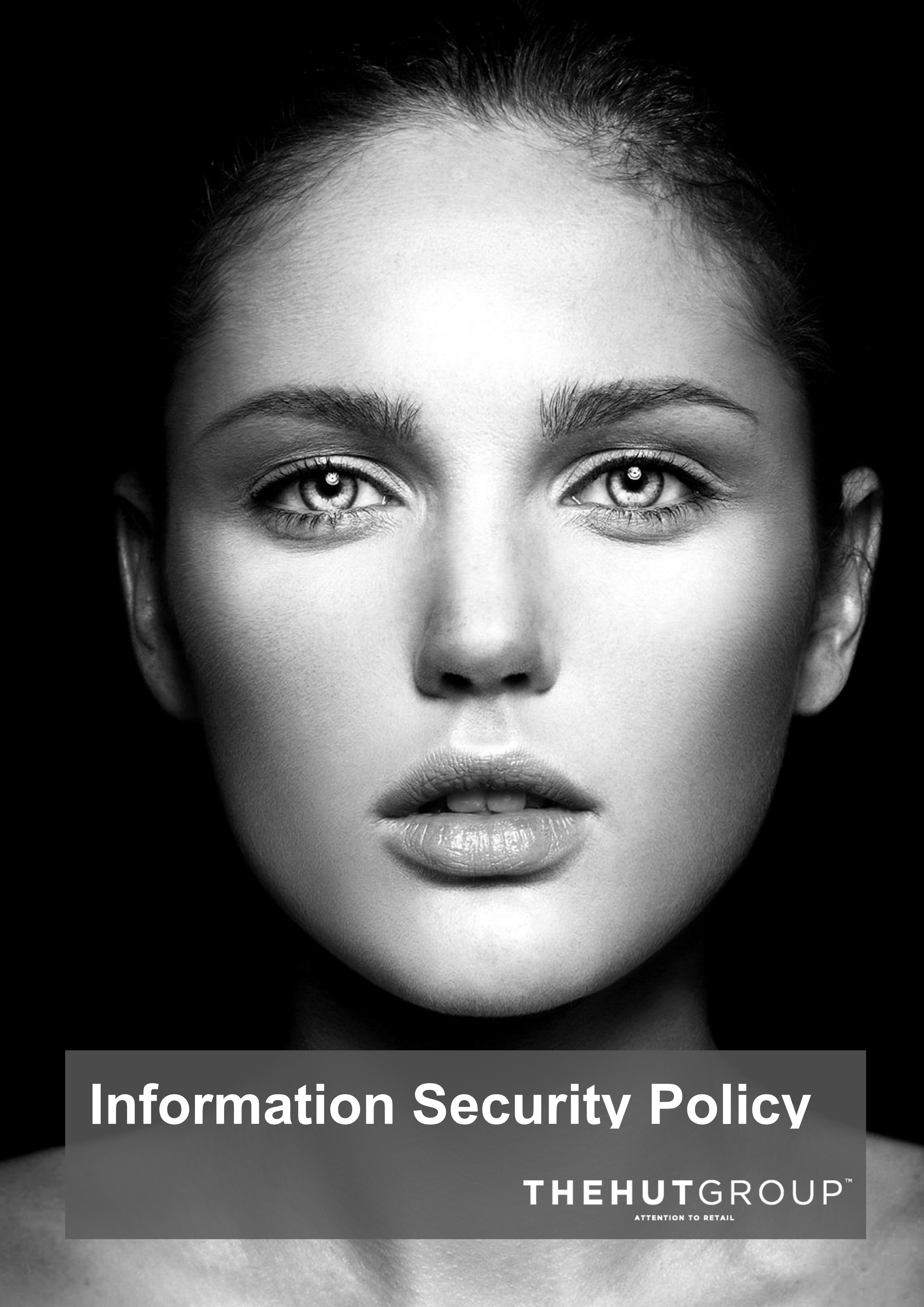

# Information Security Policy

THEHUTGROUP™

ATTENTION TO RETAIL

# INFORMATION SECURITY POLICY

**Version:** 1.0
**Effective:** 01 February 2016
**Policy owner:** Graham Thomson, Chief Information Security Officer
**Policy sponsor:** Schalk vd Merwe, Chief Technology Officer

**Version History:**

| Version | Author | Description | Reason for Amendment | Date | Next review |
|---|---|---|---|---|---|
| 1.0 | Graham Thomson CISO | New policy | n/a | Feb 2016 | Feb 2017 |
| | | | | | |
| | | | | | |

**Approvals**

| Name | Title |
|---|---|
| John Gallemore | Chief Finance Officer |
| Schalk vd Merwe | Chief Technology Officer |
| Graham Thomson | Chief Information Security Officer |
| James Pochin / Gareth Hill | Legal |
| Ben McKenzie | HR |

**Distribution**

| Name | Method |
|---|---|
| All staff | Staff handbook and Wiki |

## Contents

# 1. Introduction

## 1.1. Scope of the policy

The Information Security Policy (the Policy) applies to all The Hut Group staff, including permanent, temporary employees and third party personnel (such as temps, contractors and consultants), who have access to, process, or store The Hut Group's information, herein referred to as Staff.

The Policy applies to all forms of The Hut Group's information, including but not limited to:

- Paper information (whether printed or written)
- Digital information and communications
- Technology assets (such as servers, PCs, laptops, and mobiles)
- Removable storage media such as CDs, DVDs, tape, and USB memory sticks

**All Staff must read sections 1 to 5 of this Policy**.

Section 2 describes the roles and responsibilities that all Staff need to know about and follow.

Section 6 (the minimum security controls) is for the Information Security team and those who are in specialist roles with additional security duties. This lists the key security risks and the measures to mitigate them. The Information Security team will work with the relevant stakeholders to implement and run the measures that are appropriate to their functions.

Technical policies are provided in the form of separate Information Security 'standards' and 'guidance' documents and once completed will be made available to all Staff for reference at:

- https://wiki.gbb.thehut.local/index.php/Company_Documents

## 1.2. What are the threats?

Information is gold these days, a commodity that is bought, sold and stolen. Whether it's in paper or electronic format, information like customer and personal data, payment card details, trade secrets, intellectual property, and even just usernames and passwords, is often worth something to someone, somewhere.

Cybercrime continues to increase and evolve globally, and the UK is reported to be the most cyber-attacked country in Europe and the second-most in the world. Cybercrime is so lucrative that law enforcement agencies believe that international criminals are abandoning traditional high risk crimes for cybercrime, netting them billions in profit and with a lower risk of getting caught.

Information Security incidents, such as data losses & theft, virus attacks and other types of malicious software (aka malware), hacking attacks, and denial of service attacks, can be profoundly damaging. The types of business impact that can occur as a result of an incident are categorised as:

- **Reputational** damage: such as loss of customer confidence in the business and brand
- **Operational** damage: such as a server or website outage, or staff being unable to work
- **Financial** damage: such as regulatory fines, legal fees, or lost business

In the UK, the Information Commissioner can fine companies up to £500,000 for a breach of personal data, but the true cost to businesses who suffer a cyber-attack or a data breach is often measured in the millions. In 2015 the average cost of a UK data breach was between £1.46million and £3.14millon.

In some cases a breach can be so serious that it puts the company out of business.

## 1.3. Where do the threats come from?

The 'threat actors' are the people who are behind these threats, and they are generally put into three categories:

- **1/ Criminals:** such as hackers, fraudsters, phishers, scammers, activists and amateur enthusiasts. Their main aim is to make money or cause damage. Cyber-crime costs the UK £billions each year.
- **2/ Nation-states:** such as China's Unit 61486, Russia's FSB, the USA's NSA, and the UK's GCHQ. These are spies who steal secrets and cause sabotage to further their own countries' economies and achieve military or political goals.
- **3/ Insiders:** such as staff and contractors who legitimately work for a company. Typically, the threat from insiders is from theft or accidental loss of confidential company information.

Cyber-attackers typically use three main methods of attack to achieve their objectives:

- **1/ Malware** (an abbreviation of 'malicious software'), such as viruses, worms and Trojans, that can be silently downloaded onto computers and mobiles. Threat actors hide malware in websites, pirated software & apps, and in email attachments. Once installed on a victim computer, it allows the attacker to control it to commit other crimes, and steal passwords and other data.
- **2/ Phishing** with emails, websites, social media connections, calls and text messages. Threat actors try to trick people into giving away information or activating hidden malware. Phishers want private or personal information so that they can exploit it further or sell it on to other criminals. In particular they want people's passwords, because they know that many people (wrongly) use the same password for most things online – steal one and they have access to all.
- **3/ Hacking** into our technology systems or websites to make fraudulent orders, steal customer data, or take our systems offline. Typically, hackers take advantage of technical weaknesses (aka vulnerabilities) such as software weaknesses or by guessing weak passwords.

Threat actors try to exploit security weaknesses in company assets to achieve their objectives. Such assets include our Staff, paper and digital information, software, hardware, and our buildings.

### 1.4. Information Security: countering the threat

The goal of Information Security is to reduce the risk posed to the business from these threats, by protecting our assets, and by detecting and responding to threats and incidents.

Even though we use modern security technologies like antivirus and firewalls, our people are the first and most important line of defence. It only takes one person to open a malicious email attachment, visit a website with hidden malware, or respond to phishing, to potentially compromise the whole business.

A business with a strong security culture is much better protected, which is why all employees must be aware of the threats, and know how they can play their part in defending against them.

Security is a team effort, and every employee has a responsibility to work securely. The requirements for this are detailed in the Roles and Responsibilities section.

### 1.5. Purpose of the policy

The Policy is a risk management policy that sets out The Hut Group's minimum requirements for managing Information Security throughout the business. It's comprised of high level risks and risk treatment measures (called 'controls') that when implemented will reduce the risk to an acceptable level. The format is designed to be accessible to all Staff to improve awareness of information security issues.

The Policy has been reviewed, approved, and is sponsored by senior management. It will be reviewed at least annually to ensure that it meets business requirements and any new laws or regulations.

The objectives of the Policy are to:

- Promote and sustain a culture of strong security throughout The Hut Group
- Enable the business to grow and operate securely
- Proactively detect and mitigate the threats
- Protect the confidentiality, integrity and availability of information and technology
- Secure the business through defence in breadth

The high level risk areas addressed by this Policy are:

- **Information security**

  Inappropriate or ineffective information security arrangements leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact to the business.
- **Physical security**

  Failure to protect staff, buildings and physical assets against the threats affects the safety of staff or the integrity of physical assets, and results in an operational, financial or reputational impact to the business.
- **Business continuity**

  Failure to run and recover the business and technology systems effectively following an incident affects the operational effectiveness, agility and growth of the business, and results in an operational, financial or reputational impact to the business.

## 2. Roles and Responsibilities

**All staff must be aware of their general security responsibilities, which are detailed below:**

- Staff must read and abide by the **Acceptable Use Policy** (available on the wiki). Acceptable Use refers to the use of our communications systems that must be legal, reasonable and appropriate. Specific examples of what is deemed 'unacceptable use' are detailed in the standard.
- Staff must read and abide by the **Information Classification and Protection Standard** (available on the wiki). A classification is a grading that indicates how sensitive a piece of information is and from this the appropriate protective measures can be identified. All of The Hut Group's information will fall into one of the following three classifications:

  - **CONFIDENTIAL** (very sensitive, special security requirements apply)
  - **INTERNAL** (mildly sensitive, basic protection required)
  - **PUBLIC** (non-sensitive, anyone can access it)

- Follow good security hygiene practises, including:
  - Beware of suspicious looking external emails that may be phishing or malware (e.g. typos, bad spelling/grammar, attachments you didn't expect). Do not click on links within them, and don't open attachments from someone you don't know or don't have a business relationship with.
  - Don't install software that has not been authorised by Service Desk.

- Protect passwords and other authentication credentials by following the guidance detailed in the **Secure Password Guide** (available on the wiki).
  Choose strong passwords and don't share them with anyone. The primary password format is:
  - Comprised with a minimum of eight characters constructed from at least three of the four categories: (i) UPPERcase, (ii) lowercase, (iii) numerals, or (iv) special characters.
  - Use un-guessable, complex, and a few different passwords for all your important work related websites and applications.

- Complete any Information Security Awareness training that is issued.
- Report actual or potential security breaches (e.g. Policy breaches, loss or theft of information or Technology assets, suspicious activity) to the Information Security team as soon as possible.
- Help physically secure our offices to keep staff and property safe by following these rules:

  - ID passes (aka swipe cards) are used to ensure that only staff and authorised third parties can access our buildings, and must be worn at all times when in the office.
  - Do not let anyone who is not showing a company ID pass tailgate them through the doors (i.e. when someone follows you through without 'swiping' themselves).
  - Report suspicious activity, such as unescorted people in the office who are not displaying an ID pass and are acting suspiciously.
  - Lost or stolen ID passes must be reported to Payroll so they can be cancelled to prevent anyone else from using them to enter our offices.
  - Keep a 'clear desk' by ensuring that any confidential information is secured away when left unattended for long periods of time, and when working at home, in hotels, or when travelling.
  - Physically secure mobile assets (such as phones, laptops, USB storage, Cds, etc) to protect from theft when left unattended for long periods of time, and when working at home, in hotels, or when travelling.
  - When left unattended all laptops must be secured to a fixed point with a cable lock.

**Senior management:**

- Responsible for ensuring that the business manages information security risks.

**Line managers:**

- Must ensure that direct reports, including relevant third parties, are aware of this Policy, and that new starters complete the induction training.
- Must, when requested, approve/deny their employees' access rights to technology systems and applications (e.g. after access audits, and new access requests by their direct reports).

- Must inform HR if their staff are leaving the business, so that their access can be revoked by the Service Desk, any company assets can be returned, and Payroll can process them as a leaver.

**Information Security team:**

- Responsible for the development, management, update, communication, implementation and governance of this Policy and associated standards.
- Responsible for the identification of information security risks, and that mitigating plans are produced and tracked to completion.
- Responsible for working with the relevant business stakeholders to ensure that they understand any specific security responsibilities that they are required to maintain for their function.

**System owners:**

- Technology systems must have a defined owner who is responsible for ensuring the ongoing development, maintenance and security of their systems.
- System owners must define which users/groups/roles are allowed access to their system.

**System administrators:**

- Technology systems must have a defined administrator (includes database administrators, and network administrators).
- System administrators are responsible for ensuring the availability, performance, and security of their systems, including applying updates, patches, configuration changes, adding, removing and updating accounts, and resetting passwords.

## 3. Exceptions to the Policy

Where a control cannot be applied, it is the responsibility of the control owner to raise the matter with the Information Security team, and the Chief Information Security Officer will take a risk based decision on whether to permit or deny exceptions for a maximum of one year before review. Where justified and necessary (e.g. in urgent circumstances), temporary exceptions are allowable, but these must be formalised as soon as possible thereafter.

Where an exception is permitted, the control owner will assume accountability for any incidents that arise as a direct result of the exception. The control owner will maintain appropriate compensating controls where feasible.

## 4. Breaches of the Policy

A breach of this Policy is defined as:

- Any non-compliance with this Policy where there is no approved exception; or
- Failure or inadequacy of any minimum security control that has been implemented, whether or not it has resulted in an incident.

Non-compliance with this Policy (where there is no approved exception) may be treated as a disciplinary matter.

All breaches must be reported to the Information Security team in a timely manner.

## 5. Further help and information

This Policy and the supporting security standards and guidelines are owned by the Chief Information Security Officer and all questions or queries regarding them should be directed to the Information Security team.

- Information.Security@thehutgroup.com

## 6. Minimum security controls

**Format and explanation**

The minimum security controls serve to document the key security risks that the business faces and the set of 'controls' that aim to mitigate the risk. The risk is the 'inherent risk', i.e. the raw risk faced if the business did not have any controls to mitigate it. The 'controls' are the measures that use a mix of people, process and technology, that will tackle the risk.

The controls must be implemented and maintained by the relevant control owners. The Information Security team will work with the control owners to help them understand what their controls are and how to implement and run them. It is the control owners' responsibility to ensure that their controls are implemented and operating effectively in their function.

Compliance with the controls is mandatory and they may be subject to audits and assurance testing. Where a control cannot be met an exception for risk acceptance must be made to the Information Security team.

**Format and structure**

The Policy is based on the international standard ISO:27001 (2013) and also incorporates requirements and guidance from legal and regulatory sources and other international security standards. It covers the following risk domains:

1. **INFORMATION SECURITY POLICIES**
2. **ORGANISATION OF INFORMATION SECURITY**
3. **HUMAN RESOURCE SECURITY**
4. **ASSET MANAGEMENT**
5. **ACCESS CONTROL**
6. **CRYPTOGRAPHY**
7. **PHYSICAL AND ENVIRONMENTAL SECURITY**
8. **OPERATIONS AND COMMUNICATIONS SECURITY**
9. **APPLICATION DEVELOPMENT SECURITY**
10. **CHANGE MANAGEMENT**
11. **INFORMATION SECURITY INCIDENT MANAGEMENT**
12. **RISK MANAGEMENT**
13. **BUSINESS CONTINUITY AND TECHNOLOGY DISASTER RECOVERY**
14. **INFORMATION ASSURANCE AND COMPLIANCE**

An explanation of the structure is as follows:

1. **Policy domain name** (*the high level category for the associated inherent risk*)

1.1. **Subdomain title** *(the sub-category of the risk area)*

**Risk description:** *(a description of the risk and its impact to the business)*

**Risk treatment objective:** *(the objective of the risk treatment plan)*

1.1.1. **Control reference and title:** *(the control name and its description, i.e. the risk treatment plan)*

# The controls

## 1. Information security policies

### 1.1. Management direction for information security

**Risk description**: Lack of management direction and support for information security, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Provide management direction and support for information security in accordance with risk based business requirements, relevant best practices, laws and regulations.

1.1.1. **Policies for information security:** An **Information Security Policy** and a set of standards and guidelines must be created, approved by management, communicated to Staff, and reviewed at least annually.

## 2. Organisation of information security

### 2.1. Internal organisation

**Risk description**: Lack of information security management within the organisation, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Establish a management framework to implement, run and govern information security within the organisation.

2.1.1. **Information security roles and responsibilities**: Information security responsibilities must be defined in the Information Security Policy and communicated to Staff.

2.1.2. **Contact with authorities:** Procedures must be in place that specify when and by whom authorities (e.g. law enforcement, regulatory bodies) should be contacted in relation to incidents.

2.1.3. **Contact with special interest groups:** The Information Security team must keep contact with special interest groups, forums and associations to keep up to date with best practices and threat information.

2.1.4. **Information security in project management:** Information Security Risk Assessments must be undertaken for all new projects that involve storing or processing confidential information or new technology systems to ensure compliance to the Information Security Policy and standards.

2.1.5. **Information security for suppliers**: Third parties that access, process or store The Hut Group's confidential information, or access its technology systems, must be risk assessed by the Information Security team to ensure they meet minimum security requirements (e.g. using the Information Security team’s Third Party Security Governance Questionnaire), and contracts must consider privacy and security clauses, audit rights, exit and termination clauses, and business continuity clauses, where relevant.

### 2.2. Mobile devices and remote working

**Risk description:** Lack of security of staff working remotely and the use of mobile devices, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure appropriate security measures for remote workers and mobile devices.

2.2.1. **Remote workers policy:** Staff working remotely must be authorised to so, and must be made aware of their security responsibilities (e.g. via the Remote Access User Agreement).

2.2.2. **Mobile device users policy:** Staff must be authorised to use mobile devices, and must be made aware of their security responsibilities and the security settings (e.g. via an appropriate Mobile Device User Agreement).

2.2.3. **Mobile device technical security:** Appropriate technical security configurations must be defined in the **Endpoint Security Standard**, and implemented on mobile devices, to reduce the risk from unauthorised access if lost or stolen.

2.2.4. **Remote email:** Appropriate technical security configurations must be defined in the **Remote Email Standard**, and implemented, to reduce the risk from unauthorised access.

## 3. Human resource security

### 3.1. Prior to employment

**Risk description:** Failure to ensure that new Staff understand their security responsibilities, and failure to screen Staff for their roles, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure that staff understand their security responsibilities and are vetted where appropriate.

3.1.1. **Screening (vetting):** Background checks on all new Staff, and for movers into high risk roles, must be carried out on a risk basis.

3.1.2. **Terms and conditions of employment:** Staff contracts must state the responsibilities for information security during and after employment, specifically covering: information classification and protection, acceptable use of company assets, and confidentiality.

### 3.2. During employment

**Risk description:** Failure to ensure Staff fulfil their information security responsibilities, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure Staff are aware of their information security responsibilities and the consequences of not fulfilling them.

3.2.1. **Information security awareness and training:** All Staff must receive initial and ongoing general security awareness training to ensure they are aware of their security responsibilities in line with the **Security Awareness Training Standard**.

3.2.2. **Disciplinary process:** A formal disciplinary process must be in place to take appropriate action against Staff who breach the information security policy, whether accidentally or through negligence.

## 4. Asset management

### 4.1. Responsibility for assets

**Risk description:** Failure to identify organisational assets and define appropriate protection responsibilities, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Identify company assets and define appropriate protective measures.

4.1.1. **Acceptable use**: Rules for the acceptable use of information and Technology assets must be set out in the **Acceptable Use Policy** and communicated to Staff.

4.1.2. **Secure desk checks**: Regular out of hours desk checks for unsecured laptops, assets, and any confidential material must be carried out.

4.1.3. **Inventory of assets:** An inventory of Technology assets, both virtual and physical, connected to the network must be continually maintained.

4.1.4. **Unauthorised devices**: Unauthorised devices that attempt to access the network must be automatically detected (e.g. via asset discovery, and/or Network Access Control).

4.1.5. **Inventory of data**: An inventory of critical data must be maintained (e.g. databases with customer data).

4.1.6. **Hardened images**: Standardised and hardened images (builds) of technology systems must be maintained in line with the requirements of the **Endpoint Security Standard**, and should include the removal of unnecessary accounts and services, applying patches, closing unnecessary ports, and installing endpoint security software. Images should be refreshed regularly to update software.

4.1.7. **Returning assets:** Staff must return company assets upon termination of their employment.

### 4.2. Information classification

**Risk description:** Failure to ensure that information receives an appropriate level of protection in accordance with its importance to the organisation, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure information is protected appropriately in accordance with its importance.

4.2.1. **Information classification**: Staff must be made aware of the information classifications in line with the requirements of the **Information Classification and Protection Standard**.

4.2.2. **Information handling and protection**: Staff must be made aware of how to protect information when created, stored, used and disposed of in line with the **Information Classification and Protection Standard**.

### 4.3. Mobile device handling

**Risk description:** Failure to prevent unauthorised access, modification, or destruction of information stored on mobile devices, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Prevent unauthorised access, modification, and destruction of information stored on removable media.

4.3.1. **Mobile device encryption**: Encryption must be used to protect information stored on mobile devices (e.g. laptops, mobile phones, tablets and USB storage) from unauthorised access as detailed in the **Endpoint Security Standard**.

4.3.2. **Control of removable media**: Removable media ports (e.g. USB ports) must be blocked by default, and only permitted via user requests (e.g. to Service Desk), and data transfers to USB storage must be logged in line with the **Endpoint Security Standard**.

## 5. Access control

### 5.1. Business requirement of access control

**Risk description:** Failure to limit access to information, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Control logical access to information.

5.1.1. **Access control policy**: Requirements for access control must be set out in the **Access Control Standard**.

5.1.2. **Management of secret authentication information**: There must be documented password allocation, reset, and account unlocking processes for access to the network, systems and applications.

5.1.3. **Remote network access**: All remote access into the internal network must require two-factor authentication (i.e. requires two of: i) something only the user knows, e.g. password, PIN; ii) something only the user possesses, e.g. token, mobile phone; iii) something the user is, e.g. biometric. These elements must be independent so that the breach of one does not compromise the other, and at least one should be non-reusable and not capable of being surreptitiously stolen).

5.1.4. **Least privilege access restriction**: Access must be restricted to ensure that users only obtain the minimum access they require for their role.

5.1.5. **Secure log-on**: Access to technology systems and applications must be controlled by an authentication mechanism which permits authorised users and denies unauthorised users.

5.1.6. **Passwords**: Systems must implement a secure, standardised password format in line with the **Password and Authentication Standard** (the primary password format is a minimum of eight characters using three of uppercase, lowercase, numerals, or, special characters, and changed at least every 90 days).

### 5.2. User access management

**Risk description:** Failure to ensure authorised user access and to prevent unauthorised access to systems and services, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure access is authorised and prevent unauthorised access to systems and services

5.2.1. **User account creation**: The user account creation process must ensure that:
- Unique IDs are used for each user and redundant user IDs are not be re-issued to other users.
- Shared IDs where more than one person uses the account are only permitted for specific operational reasons and must be approved.

5.2.2. **Joiner, mover, leaver access**: Access to the network, systems and applications must be approved, with access granted by roles (where possible) and based on least privilege:
- For joiners, there must be a request and approval process for granting new access.
- For leavers, there must be a process to disable or remove access within 24 hours.
- For movers (job role changes), there must be a process to revoke old access and add new access.
- For existing staff there must be a process to authorise requests to add, change or revoke access rights.

5.2.3. **Account housekeeping**: Processes must be in place to:
- Periodically identify and remove or disable redundant user IDs.
- Ensure all accounts, including service accounts, have a nominated owner.
- Ensure all 3rd party accounts (i.e. contractors) have a pre-set expiry date.

5.2.4. **Review of access**: A process to review access permissions on critical technology systems, critical applications and critical databases must be in place that ensures that:
- High risk end user access is reviewed and recertified at least annually.

• Privileged / administrative access is reviewed and recertified at least twice annually.

5.2.5. **Privileged access**: Privileged / administrative access rights must be controlled, ensuring that:
• Privileged access rights are assigned to an ID different from those used for regular business activities (e.g. end user email and internet access).
• Users of privileged / administrative accounts are informed of their security responsibilities.

5.2.6. **Segregation of duties**: Security duties must be segregated to reduce opportunities for fraud and misuse (e.g. security administrators of key applications are separate from the users).

### 5.3. User Responsibilities

**Risk description:** Failure to make users accountable for safeguarding their authentication information, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure users are accountable for safeguarding their authentication information.

5.3.1. **Secret authentication information**: Staff must be informed of their duty to protect their passwords and other authentication credentials by following the guidance detailed in the **Secure Password Guide**.

## 6. Cryptography

### 6.1. Cryptographic controls

**Risk description:** Failure to ensure proper and effective use of cryptography, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

6.1.1. **Cryptographic policy**: All cryptographic algorithms and controls for asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms must be in line with the **Encryption Standard**.

6.1.2. **Key management**: There must be a procedure to describe how cryptographic keys are to be protected and managed.

## 7. Physical and environmental security

### 7.1. Secure areas

**Risk description:** Failure to prevent unauthorised physical access, damage and interference to the organisation’s information and Technology facilities, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Prevent unauthorised physical access, damage and interference to the organisation’s information and Technology facilities.

7.1.1. **Physical security policy**: The requirements for physical security must be set out in the **Physical Security Standard**.

7.1.2. **Physical entry**: Secure areas, office work areas and delivery areas must be protected by entry controls to ensure that only authorised people are allowed access, in line with the **Physical Security Standard**.

7.1.3. **Physical access to Technology facilities**: Physical access to critical Technology rooms and data centres must be controlled:
• An access list of authorised users is maintained.
• Designated Technology managers are appointed to manage and approve physical access to critical Technology rooms and data centres.
• Access events to critical Technology rooms and data centres are recorded.

7.1.4. **Security perimeter**: Secure areas must be protected by security perimeters with appropriate security measures in place (e.g. barriers, entry controls and/or CCTV surveillance) in line with the **Physical Security Standard**.

7.1.5. **Management of CCTV**: CCTV systems must be installed, managed and maintained in line with the **CCTV Standard**.

### 7.2. Equipment

**Risk description:** Failure to prevent loss, damage, theft or compromise of physical assets, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Prevent loss, damage, theft or compromise of physical assets.

7.2.1. **Technology communications rooms**: Communications rooms must have physical access controls to prevent unauthorised access.

7.2.2. **Secure disposal or re-use of Technology equipment**: Technology assets, hardcopy and electronic media must be recycled or disposed of securely (e.g. by overwriting data and hard drives).

## 8. Operations and communications security

### 8.1. Protection from malware

**Risk description:** Failure to ensure that information and technology systems are protected against malware, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure that appropriate protective and detective security architecture is in place so that information and technology systems are protected against malware.

8.1.1. **Technical security architecture policy**: The minimum technical security requirements must be set out in the **Technical Security Architecture Standard**.

8.1.2. **Controls against malware (endpoints):** Defensive and detective technical controls to protect against malware must be implemented, including:
• Anti-malware software is installed and kept updated on all technology systems.
• Anti-malware scheduled scans are automated at least monthly.
• Automatic anti-malware scanning of files transferred from removable storage (e.g. USB media).
• Limit the number of users with local administrator permissions to those who need it.

8.1.3. **Controls against malware (email):** Defensive and detective technical controls to protect against malware must be implemented, including:
• Anti-malware scanning of incoming and outgoing emails and attachments at the email gateway.
• To prevent email spoofing implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.

8.1.4. **Controls against malware (internet):** Defensive and detective technical controls to protect against malware must be implemented, including:
• Anti-malware scanning of web pages before code reaches the endpoint (i.e. at the web proxy/gateway).
• Restrict undesirable internet web content via category filtering.

8.1.5. **Controls against malware (network):** Defensive and detective technical controls to protect against malware must be implemented, including scanning inbound and outbound network traffic for anomalies, malware, known malicious command and control domains, and known compromised systems (e.g. via regularly updated IDS, IPS).

### 8.2. Logging and monitoring

**Risk description:** Failure to record events and retain evidence, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Record system events and retain evidence.

8.2.1. **Event logging policy**: Event logs recording user, administrator and system activities, faults and security events on critical technology systems and applications must be kept for at least 12 months, analysed and reviewed in line with the **Security Information and Event Management (SIEM) Standard**.

8.2.2. **Protection of log information**: Logging systems and their logs must be protected against tampering and unauthorised access.

8.2.3. **Clock synchronisation**: Clocks of all technology systems must be synchronised to an appropriate central time source via Network Time Protocol (NTP) to ensure good continuity of evidence.

### 8.3. Cyber threat intelligence

**Risk description:** Failure to detect and anticipate threats to the business, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Detect and anticipate threats to the business.

8.3.1. **Cyber threat intelligence**: Processes must be in place to proactively detect and mitigate specific internal and external threats to the business, such as: cyber-squatting; phishing; breaches involving company accounts/email domains; network & endpoint breach detection; employee misuse; and keeping track of new cyber-threats.

8.3.2. **Honeypots**: Appropriate technology systems should be maintained that are specifically designed to be the target of malicious attacks for the purpose of detecting, and analysing attacks.

### 8.4. Technical vulnerability management

**Risk description:** Failure to prevent exploitation of technical vulnerabilities, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Prevent the exploitation of technical vulnerabilities.

8.4.1. **Patching and vulnerability management policy**: Regular assessments of missing patches and other vulnerabilities must be performed in line with the **Patching and Vulnerability Management Standard**.

8.4.2. **External vulnerability scanning**: Vulnerability scanning must be conducted on critical internet facing technology systems and applications at least quarterly.

8.4.3. **Patching**: Critical and security patches must be applied within a reasonable timescale.

8.4.4. **Penetration testing**: Penetration testing must be conducted on critical internet facing technology systems and applications at least annually and after major changes with issues prioritised according to risk, in line with the **Penetration Testing Standard**.

### 8.5. Network security management

**Risk description:** Failure to protect the network, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure the protection of the networks.

8.5.1. **The network is securely designed**: Multiple layers of security defences must be deployed to protect the network from the threats as set out in the **Technical Security Architecture Standard**.

8.5.2. **Firewall management policy**: Firewalls rules must be periodically reviewed in line with the **Firewall Management Standard**.

8.5.3. **Internet Protocol Version 6**: Use of IPv6 must be controlled, ensuring that network devices have IPv6 disabled by default.

8.5.4. **Network controls**: Data must be encrypted when travelling across public networks, and wireless networks, in line with the **Information Classification and Protection Standard**.

8.5.5. **Segregation in networks**: To limit access by an insider, external attacker, or malware spreading, appropriate internal network segmentation must be employed (e.g. DMZs, VLANs and data stores).

8.5.6. **IP video and telephony**: IP video and telephony systems must use secure protocols, and have their traffic separated from data traffic (e.g. VLAN).

8.5.7. **Wireless network policy**: Wireless networks must be deployed securely in line with the **Wireless Network Standard**.

### 8.6. Information transfer

**Risk description:** Failure to maintain the security of information transferred within an organisation and with any external entity, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Maintain the security of information transferred internally and externally.

8.6.1. **Information transfer policy**: Staff must be made aware that the transfer of information internally and externally must be protected in line with the **Information Classification and Protection Standard**.

8.6.2. **Emails to customers**: Emails to existing customers should reassure the recipient of the authenticity, and reduce the phishing risk, by greeting the customer by their name.

8.6.3. **Email data loss prevention**: Outgoing emails and attachments must be scanned for data loss prevention based keywords and data loss indicators (including: payment card numbers; large numbers of post codes) and be blocked and logged accordingly.

8.6.4. **Web data loss prevention**: Access to known file transfer and email websites must be restricted based on staff roles.

## 9. Application development security

### 9.1. Security in development

**Risk description:** Failure to ensure that information security is designed and implemented within the development lifecycle of applications, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure that security is embedded within the application development lifecycle.

9.1.1. **Secure development policy**: A **Secure Application Development Standard** that details OWASP based secure application development principles, must be communicated to Developers and followed.

9.1.2. **Secure development environment**: Secure development environments must be maintained by ensuring that the production environment is separated from the development and test environment, and access to the production/development/test environments is limited to only those who require it.

9.1.3. **Outsourced development**: Third parties used for outsourced development must be risk assessed by the Information Security team, and have appropriate contracts in place (e.g. non-disclosure agreements and escrow agreements for source code – if this is considered appropriate by the system owner).

9.1.4. **Application security testing**: Security code reviews must be carried out and identified issues prioritised according to risk, in line with the **Secure Application Development Standard**.

9.1.5. **Application security risks**: Identified information security risks must be logged in a risk register, assessed, and have the appropriate mitigating actions tracked to completion.

9.1.6. **Bug bounty programmes**: Bug bounty programmes must be run in accordance with the **Bug Bounty Standard**.

9.1.7. **Protection of test data**: Test data must be managed in line with the **Management of Test Data Standard**.

## 10. Change management

### 10.1. Change management

**Risk description:** Failure to ensure that only authorised and tested Technology changes are made to the live environment, impacts the operational effectiveness, agility and growth of the business, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure that only authorised and tested technology changes are made.

10.1.1. **Change management procedure**: There is a formal change management procedure in place.

10.1.2. **Change testing and sign off**: All changes to technology systems and applications undergo appropriate and structured testing and sign off before go-live.

10.1.3. **Change documentation**: Technical changes to technology systems result in updates to system documentation where relevant.

10.1.4. **Emergency changes**: Emergency changes are logged and retrospectively authorised.

10.1.5. **Audit trail**: There is a full audit trail of changes.

## 11. Information security incident management

### 11.1. Management of Information Security Incidents

**Risk description:** Failure to ensure a consistent and effective approach to the management of information security incidents, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

11.1.1. **Incident management and investigations policy**: Information security incidents must be managed in line with the **Security Incident Management and Investigations Standard**.

11.1.2. **Reporting information security events**: Staff must be informed to report actual or suspected security events as quickly as possible to the Information Security team.

11.1.3. **Red team exercises**: Red Team exercises should be performed periodically to test incident detection capabilities and to improve the team's ability to respond to incidents and conduct digital forensics.

## 12. Risk management

### 12.1. Risk management

**Risk description:** Failure to ensure that security risks are identified, assessed and mitigated, impacts the operational effectiveness, agility and growth of the business, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure that security risks are identified, assessed and mitigated appropriately.

12.1.1. **Risk assessment methodology**: A process for assessing risk based on likelihood and impact must be set out (e.g. in a Security Risk Management Guide).

12.1.2. **Risk register**: Identified security risks must be logged in a risk register, assessed, and have mitigating actions tracked to completion.

## 13. Business continuity and Technology disaster recovery

### 13.1. Business continuity

**Risk description:** Failure to run and recover the business effectively following an incident impacts the operational effectiveness, agility and growth of the business, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure that the business can be recovered effectively following an incident.

13.1.1. **Business continuity policy**: A Business Continuity policy must be defined and updated at least annually.

13.1.2. **Business continuity plans**: Business Continuity plans must be maintained and updated at least annually.

13.1.3. **Business impact analysis**: Business Impact Analysis (BIA) for key business areas must be maintained and updated at least annually.

13.1.4. **Awareness and training**: Staff with a responsibility for Business Continuity must receive awareness training to make them aware of their responsibilities.

### 13.2. Technology disaster recovery

**Risk description:** Failure to ensure that Technology infrastructure and applications are resilient and be recovered effectively following an incident, impacts the operational effectiveness, agility and growth of the business, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure that critical Technology infrastructure and applications are resilient and can be recovered effectively following an incident.

13.2.1. **Technology disaster recovery plan**: A Technology Disaster Recovery plan must be maintained and updated at least annually.

13.2.2. **Technology system criticality**: Technology systems must be categorised into priority classes linked to criticality.

13.2.3. **Backups**: Data on critical systems must be backed up at an appropriate frequency.

13.2.4. **Backups**: Back-up media must be stored securely (i.e. via encrypted back-up media).

13.2.5. **Backups**: Backed up data must be periodically tested to ensure it can be relied upon for emergency use.

## 14. Information assurance and compliance

### 14.1. Compliance with legal and regulatory requirements

**Risk description:** Failure to avoid breaches of legal, regulatory or contractual obligations related to information security and of any security requirements, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Avoid breaches of legal, regulatory or contractual obligations.

14.1.1. **Identification of requirements**: The Information Security team must keep up to date with security related legal and regulatory requirements (e.g. maintain a Technology Related Laws and Regulations Guide).

14.1.2. **PCI DSS**: Compliance with the Payment Card Industry Data Security Standard (PCI DSS) must be assessed annually, in line with the **PCI DSS Standard**.

14.1.3. **Privacy**: A Data Protection Officer must be appointed to provide guidance and to ensure a data retention policy and schedule is maintained.

14.1.4. **Banned shipping items and countries**: Processes must be in place to detect unauthorised changes to the lists of banned shipping items and countries.

### 14.2. Information assurance

**Risk description:** Failure to ensure that information security is implemented and operated in accordance with policies and procedures, leads to a compromise of confidentiality, integrity, or availability of information or technology systems, and results in an operational, financial or reputational impact.

**Risk treatment objective:** Ensure that information security is implemented and operated in accordance with this Policy.

14.2.1. **Compliance with security policies and standards**: Compliance with the Information Security Policy must be assessed, tracked and reported.

14.2.2. **Security risks are managed**: Identified information security risks must be logged in a risk register, assessed, and have the appropriate mitigating actions tracked to completion.

14.2.3. **Technical compliance and metrics**: Technology systems and applications must be reviewed for technical information security compliance (e.g. via penetration testing, vulnerability scanning, and configuration audits). Metrics and configuration audits should be carried out in line with the **Security Configuration Audit Standard**.

## Key Definitions

| | |
|---|---|
| **Asset** | Anything tangible or intangible that is capable of being owned or controlled to produce value and that is held to have positive economic value.<br>Assets include our Staff, paper and digital information, software and hardware, our buildings and other physical assets. |
| **Control** | A means of managing risk involving people, processes and technologies.<br><br>**Types of Controls:**<br>**Preventative** = e.g. firewalls, passwords, IPS<br>**Detective** = e.g. IDS, SIEM alerts, audits<br>**Corrective** = e.g. backups, mirror sites<br>**Deterrent** = e.g. policy, standards, vetting |
| **Information Security** | The term that describes protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction. The risk to information relates to breaches of confidentiality, integrity and availability (CIA), which are defined as:<br><br>**Confidentiality**: The need to protect sensitive or proprietary information from accidental or deliberate unauthorised access or disclosure.<br>**Integrity**: The need to maintain consistent, accurate and complete information.<br>**Availability**: The need to have information, technology systems and applications available when required. |
| **Malware** | Short for malicious software, malware is defined by its deliberate malicious intent to gain unauthorised access, or cause disruption, modification, or destruction. It includes viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware. |
| **Policy** | Overall intention and direction as formally expressed by management. |
| **Risk** | A combination of the probability of an event occurring and its impact to the business.<br><br>**Risk** = **threat** x **vulnerability** x **asset**<br>If there is no **threat** or **vulnerability** or **asset** then there is no risk.<br><br>**Risk Mitigation Actions:**<br>**Treat/Tackle** (Risk Mitigation): build additional controls<br>**Transfer** (Risk Transference): transfer the risk to someone else, i.e. insurer / 3rd party<br>**Tolerate** (Risk Acceptance): do nothing, accept the risk<br>**Terminate** (Risk Avoidance): stop the activity if it's too risky |
| **Security Incident / Security Breach** | An event that compromises the confidentiality, integrity, or availability of information or technology systems (such as hacking, data loss, data theft, denial of service attack, malware attack). |
| **Technology** | The hardware and software used to store and process information (aka technology systems and applications). |
| **Third Parties** | Suppliers and service providers engaged under contract, and includes contractors operating as businesses or through an agency. |
| **Threat** | Potential cause of a security incident that may result in harm to the business.<br><br>**Threat level** = **vulnerability** (*method*) x **capability** (*means*) x **intent** (*motive*)<br>If there is no **vulnerability** or **capability** or **intent** then there is no threat.<br><br>**Vulnerability**: a security weakness that can be exploited by a threat actor.<br>**Capability**: the ability of the threat actor to carry out a malicious action.<br>**Intent**: the threat actor's decision to take malicious action. |