

Information security policy

Table of Contents

1.	OBJECTIVE	ERROR! BOOKMARK NOT DEFINED.
2.	SCOPE	1
2.1	Policy Statement.....	1
2.2	Responsibilities	1
2.3	Enforcement	2
2.4	Standard	2
2.5	Compliance.....	2
3.	INFORMATION CLASSIFICATION	2
4.	NETWORK SECURITY POLICY	2
5.	SECURITY AWARENESS AND BEHAVIOR	8
5.1	Need to know.....	8
5.2	User identification and authentication	8
5.3	Physical security to control information access	8
5.4	Clear desk policy.....	9
5.5	Third party access	9
5.6	Granting access rights	9
5.7	Revocation of access rights.....	10
5.8	Review of access rights	10
5.9	Privilege management	10
5.10	System Utilities	10
5.11	Email usage	10
5.12	Mobile use	11
5.13	Personal Cloud Storage.....	11
6.	INFORMATION SECURITY TRAINING	12
6.1	Training requirements.....	12
6.2	Simulated Social Engineering Exercises	13
6.3	Remedial Training Exercises	13
6.4	Compliance and Non-Compliance with the training programme.....	13
6.5	Non-Compliance Actions.....	13
6.6	Responsibilities and Accountabilities.....	14
6.7	Failure Penalties	14

INFORMATION SECURITY POLICY

1. Scope

This policy applies to all information in the company's possession, whether held on computer systems or otherwise. The policy is applicable to all personnel employed or working with the Company, regardless of their position, location or relationship with the Company.

1.1 Policy Statement

It is the Company's policy to ensure that:

- Information will be safeguarded against unauthorised access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Availability of information when needed will be accessible by authorised individuals;
- Regulatory and legislative requirements will be met;
- Continuity plans will be produced, tested and maintained;
- Information security awareness amongst all staff will be created;
- All breaches of information security, actual or suspected, will be reported to, and investigated by the person or persons responsible for security;
- Copyright of intellectual property will be respected; and
- Information will be protected against malicious code.

1.2 Responsibilities

The information security manager ('ISM') and or the Chief Technical Officer ('CTO') has direct responsibility for maintaining the policy and providing advice on information security and guidance on its implementation. The ISM must ascertain that appropriate training is provided to data owners, data custodians, network and system administrators and users.

Management is responsible for implementing this policy within their business area and to ensure that all employees understand their obligation to protect the Company's assets and comply with security standards and related procedures.

- All employees have a responsibility to conduct themselves in an ethical manner.
- Data/information obtained inappropriately should not be used.
- Finding a system weakness is not a license to take advantage of it, albeit such system weaknesses should be reported immediately in accordance to the incident response policy.
- Every user has a responsibility to carry out his/her work diligently and will be held accountable for misuse of the Company's computer systems.
- When the confidentiality of information is unclear, its classification should be ascertained.
- Report any known violation or system weakness to the person or persons responsible for the Company's security or to the line manager.
- All intrusions should be reported, investigated and the Incident Response Policy should be adhered to.

1.3 Enforcement

Non-compliance with this Policy will be subject to Management review and action in conformance with the Company's disciplinary procedures.

1.4 Standard

Other related policies, all supporting standards, procedures, guidelines, operating instructions issued in support of this policy statement, will form an integral part of this Corporate Information Security Policy Statement and shall serve as a standard to be applied by the Management. It can also serve as a basis of compliance monitoring and review.

1.5 Compliance

All information held or processed by the Company, that is not publicly available should be kept internal and undisclosed. Consequently, any breach of secrecy is a definite breach of the Company's policy.

This policy will assist the Company's employees to comply with the applicable legislations, including REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2. Information Classification

Sort Services will classify its information as follows:

- **Confidential:** The information is considered very sensitive, and disclosure of the information is likely to cause severe damage. Access rights shall be restricted to named individuals.
- **Restricted:** The information is not classified as public or as Confidential. Unauthorized disclosure of the information may cause damage. Access rights may be assigned individuals with specified roles or group memberships on a need-to-know basis.
- **Public:** The intention is to spread the information to the public, or the information is already known outside of Sort Services. No specific access control is needed.

Sort Services' information shall be protected according to the results of the classification during the whole information life cycle, i.e. from creation /registration through destruction / disposal of the information.

Specific areas, like Intellectual Property Rights and Personally Identifiable Information, require special care when designing protective measures.

3. Network Security Policy

The use of networks is an essential part of the day-to-day business of Sort Services. Networks not only connect many of the components of business processes together internally, but they also link the organisation with its suppliers, customers, stakeholders and the outside world.

The company's networks have evolved over a period of time to become the circulatory system of the company, transporting information to where it needs to go and enabling business to be carried out effectively.

But the fact that so much information runs through our networks makes them a target for those who would try to steal that information and disrupt our business. Therefore, these networks need to be protected to ensure that the confidentiality, integrity and availability of our vital information is always assured.

The effective protection of our network requires that we adopt good practices in information security covering the design, implementation, operations and management of them and that we ensure that everyone involved follows these practices.

This policy sets out Sort Services' rules and standards for network protection and acts as a guide for those who create and maintain our IT infrastructure. Its intended audience is IT and information security management and support staff who will implement and maintain the organisation's defences.

As a cloud service provider (CSP), this policy also applies to the methods used to design and create the physical and virtual networks used to deliver service to our cloud customers.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Sort Services' systems,

3.1 Network security design

The design of networks is a complicated process requiring a good knowledge of network principles and technology. Each design is likely to be different, based on specific set of requirements that are established early in the process. This policy does not attempt to specify how individual networks should be designed and built but provides guidance for the standard building blocks that should be used.

3.1.1 Requirements

A network design must be based on a clear definition of requirements which should include the following security-relation factors:

- The classification of the information to be carried across the network and accessed through it
- A risk assessment of the potential threats to the network, taking into account any inherent vulnerabilities
- The level of trust between the different components or organisations that will be connected
- The hours of availability and degree of resilience required from the network
- The geographical spread of the network
- The security controls in place at locations from which the network will be accessed
- The security controls in place at locations from which the network will be accessed
- Security capabilities of existing computers or devices that will be used for access

Requirements must be documented and agreed before design work starts.

3.1.2 Defence in depth

A 'defence in depth' approach will be adopted to network security whereby multiple layers of controls are used to ensure that the failure of a single component does not compromise the network. For example, network firewalls may be supplemented by host-based software firewalls on server and clients in order to provide several levels of firewall protection.

At key points in the network a 'defence diversity' approach must also be taken so that vulnerabilities are minimised. For example, this may involve using firewalls from different subject to it. This may be extended to the use of more than one network virus scanner at the perimeter for the same reason.

3.1.3 Network segregation

The principle be adopted that, where appropriate, a network will consist of a set of smaller networks segregated from each other based on either trust levels or organisational boundaries (or both).

For a large network this may be achieved using separate domains, particularly where separate organisations' networks are being linked. An appropriate level of trust must be configured at the domain level and domain perimeters must be secured using a firewall where appropriate.

Within networks, Virtual Local Area Networks (VLANs) will be used to segregate organisational units.

In a cloud environment, it is important that requirements for segregating networks to achieve tenant isolation are defined and the cloud service provider's ability to meet these requirements is verified.

3.1.4 Perimeter Security

At all perimeters between the internal networks and an external network (such as the internet) effective measures must be put in place to ensure that only authorised network traffic is permitted. This will usually consist of at least one Stateful Inspection firewall and for major links with the Internet an Application (or Application Gateway) firewall must be used. For connections such as broadband at smaller locations a packet filtering firewall may suffice, depending on the results of a risk assessment.

Servers that are intended to be accessed from an external, insecure network (such as web servers) must be located in a Demilitarized Zone (DMZ) of the firewall in order to provide additional protection for the internal network.

3.1.5 Cloud networks

Where virtual infrastructure services are configured within a virtual private cloud, the same principles must be used as for the security of physical networks. These will include the use of network segmentation, firewall, access control lists and log monitoring.

3.1.6 Public networks

Where information is to be transferred over a public networks such as the internet, strong encryption via TLS must be used to ensure the confidentiality of the data transmitted.

Servers that will be accessed from devices on the public network will be located in the DMZ of the firewall.

3.1.7 Wireless networks

Wireless networks must be secured using WPA2 encryption. WEP and WPA must not be used.

Wireless networks must be treated as insecure even if WPA2 is used as the encryption method and a firewall installed between the wireless network and the main LAN.

A guest wireless network may be provided to visitors. This must be physically separate from all internal networks (including internal wireless networks) and secured using a firewall.

Wireless access points must be configured to not broadcast their SSID and to not allow secure connection using WPS (Wi-Fi Protected Setup) via physical access to the access point itself.

Wireless access point admin logon passwords must always be changed from the default.

3.1.8 Physical security

Remote network equipment will be housed in secure cabinets which will always be locked. Only support staff will have access to the key to each cabinet.

Backbone and centralised network equipment will be housed in appropriate lockable cabinets or racks in a secure server room to whom only authorised support staff will have access (except for local facilities staff for reasons of health and safety).

Wireless access points located in public areas must be hidden from view where possible and must be placed in positions where access by the public is difficult e.g. in or near the ceiling. A lockable protective casing must be installed here an access point is located in an unprotected public area e.g. a car park.

3.1.9 Remote access

Where there is a requirement for remote access to the internal network the following controls will be used:

- A Virtual Private Network (VPN) will be used providing session encryption using TLS
- Multifactor authentication at the client where appropriate
- Secure authentication using a RADIUS server
- Network access control (NAC) will be used to restrict access to remote clients that do not meet minimum requirements e.g. virus control

Remote access must be granted on an 'as required' basis rather than for all users by default.

3.1.10 Network intrusion detection

A Network-based Intrusion Detection System (NIDS) must be installed at the network perimeter and at all key points within the network e.g. on critical servers.

3.1.11 Network security standards

The following standards will be adopted with respect to network configuration and security.

3.1.11.1 Network hardware

Where possible a single supplier policy will be used for network hardware. An exception will be made where the use of multiple vendor hardware may increase the level of security provided e.g. in a dual network-based firewall configuration.

Network routing will be based on Cisco routers using OSPF. Cisco Gigabit switches will be used as standard for connectivity. Switch port, including diagnostic ports, will be configured to be administratively disabled until required. Hubs will not be used due to their inherent security weaknesses.

CAT 6 UTP will be used for network cabling unless specific circumstances (such as excessive interference) preclude its use. The network topography used will be Ethernet according to the IEEE 802.3 family of standards.

3.1.11.2 IP addressing

IPv4 will be used on internal networks. However new network devices purchased must support IPv6 in preparation for the future.

IP addresses and associated network information for desktop and laptop clients will be controlled using DHCP, internal DNS servers will be used.

3.1.11.3 Network protocols

The protocol used on all networks will be TCP/IP. UDP will be used where appropriate, but other OSI layer 4 network protocols should not be used.

Only protocols and ports required on a specific server will be enabled by default in order to reduce the attack surface. This is especially true for servers within the DMZ of the firewall(s).

3.2 Network Security management

Once networks have been designed and implemented based on a clear set of security requirements, there is an ongoing responsibility to manage and control the secure

networking environment to protect the organisation's information in systems and applications. This must be achieved via controls in the following areas.

3.2.1 Roles and responsibilities

Roles and Responsibilities for the management and control of networks must be clearly defined. In order to provide effective segregation of duties, the operation of networks is managed separately from the operations of the rest of the infrastructure such as servers and applications.

This segregation of duties is detailed in the following table.

Management role	Team	Main responsibilities
Network manager	Networks and Communications Management	- Design and implementation of new and changed networks - Installation and removal of networking equipment - Configuration of networking equipment - Third line incident management
Network operations manager	Network Operations	- Network availability monitoring - Network intrusion monitoring - Second line incident management - Configuration backups - Patching and updates - Setup and management of remote access users
Computer operations manager	Computer Operations	- Server and application backups - Job scheduling - Infrastructure monitoring - Sort Services line incident management

3.2.2 Logging and monitoring

Logging levels on network devices must be configured and logs monitored on a regular basis.

Firewall logs will be monitored for signs of excessive port scanning which may be a precursor to a remote attack. Where installed, a Network-based Intrusion Detection System must be configured to alert the Network Operations team of this activity.

Network monitoring for availability may be achieved using appropriate SNMP-based network management tool and recovery actions automated where possible.

Alerts from the Network Access Control (NAC) system must be addressed immediately to ensure that clients that do not meet minimum security requirements are only allowed access to a quarantined subset of systems on the network.

3.2.3 Network changes

All changes to network devices will be subject to the change management process and appropriate risk assessment, planning and back-out methods out in place. Configuration records must be updated whenever such changes are carried out so that a current and accurate picture of the network is always maintained.

3.2.4 Network security incidents

Network events which are deemed to be security incidents must be recorded and managed according to the company's incident response procedures.

4. Security awareness and behavior

4.1 Need to know

Access to information must be provided based on the need to know. Information must be disclosed only to people who have a legitimate business need for the information. At the same time, users must not withhold access to information when instructions were given for that information to be shared. To implement the need-to-know concept, the company has adopted an access request and approval process. Staff must not attempt to access sensitive information unless the appropriate access rights have been granted to them.

When a member of staff changes their job duties, including; termination, transfer, promotion and long periods of leave of absence, his or her supervisor must immediately notify the Information Security department so access is reviewed for that particular individual. The privileges granted to all users must be periodically reviewed to ensure that only those with a current need to know presently have access.

4.2 User identification and authentication

All users shall have unique personal accounts for personal use only. Shared accounts are not permitted. Logon procedures shall include user authentication with sufficient strength. Password management systems shall ensure that users choose passwords of high quality.

Initial passwords are distributed separately and securely by the Administrator to employees/contractors. The distribution method must ensure proper identification of the receiving user. Users shall immediately change passwords given by the Administrator.

4.3 Physical security to control information access

Access to every office, server room, or any other work area containing sensitive information must be physically restricted to those people with a need to know, based on the job designation and given only by few authorised personnel. When not in use, sensitive information must always be protected from unauthorised disclosure.

When an employee leaves a room unattended, they must ensure that sensitive information in paper form is locked away in appropriate containers or at least, they must ensure that all doors and windows to the unattended room are closed and locked.

During non-working hours, workers in areas containing sensitive information must lock-up all information. Employees must position their computer screens such that unauthorized people cannot look over their shoulder and see the sensitive information displayed.

4.4 Clear desk policy

Unless information is in active use by authorised people, desks must be clear and clean during non-working hours to prevent unauthorised access to information.

4.5 Third party access

Unless it has specifically been designated as necessary, all internal information and systems must be protected from access by third parties. Third parties may be given access to internal information and systems only when a demonstrable need to know exists, when a non-disclosure agreement has been signed, and when such a disclosure has been expressly authorised.

If there is suspicion of unauthorised access to the company's information systems, or if sensitive information is lost, disclosed to unauthorised parties, or is suspected of being lost or disclosed to unauthorised parties, the Information Security department must be notified immediately.

Unless an employee has been authorised to make public disclosures, all requests for information about the company and its business such as questionnaires, surveys, and newspaper interviews, must be referred to the person in charge of public relations. This does not apply to sales and marketing information about the company's products and services, nor does it pertain to customer technical support calls.

Access to the company's systems by third parties will only be allowed if they have a legitimate business need to be granted access and shall only be given for the duration of the assignment. Upon approval, access rights will be granted for the time period required to finish the approved tasks such as audits and maintenance.

4.6 Granting access rights

Any request for access must be made in writing (by email or hard copy) and must include the following information:

Start Date of Employment	Day/Month/Year
Name of Employee	Mr/Mrs/Ms. Xxxxx
Job title of the new employee	Ex. Customer Care Executive
Occupational group	Ex. Customer Support
Contact details	Ex. Work: 123-456 Ext. 54 Personal: 123-456
Additional Access required	Ex. Customer Management, Issuing of Reports (By default, new accounts have access to the Microsoft Office Suite and Internet.

Access to new employees shall be granted as follows:

- The request is sent to the IT department either by the new employee's manager or by Human Resources, with the required information.

- The IT Manager reviews the request and upon approval, the new employee's e-mail address and user account are created. Access is given as specified in the access request.
- A test email is sent to the new employee to ensure the account is working fine. This e-mail is also used to welcome the new employee and gives basic information on how to change the password as well as general guidelines.
- The new user account will not however be available until the employee's start date. On the Start Services day, the new employee will be advised of the user-id and password. The system will force them to change the password upon Start Services login.

4.7 Revocation of access rights

When an employee leaves the company, Human Resources inform the IT department of employee's new employment status promptly in writing (by email or hard copy). The IT department then deactivates the user's account and ensures that all privileges have been revoked.

4.8 Review of access rights

Access rights are re-evaluated regularly by management to ensure that no employees have more access rights than their need to know. Should an employee's role change, the IT department should be informed beforehand so they can make the necessary changes to that employee's access levels.

4.9 Privilege management

The allocation and use of privileged access rights, e.g. rights to invoke operating system level commands and to analyse system details and user behaviour, shall be restricted and controlled. Users with privileged access rights shall use a special personal account, without the privileges used for normal day-to-day work, for privileged access. All use of such special accounts shall be logged.

4.10 System Utilities

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

4.11 Email usage

All users must adhere to the following when using the company's email facilities:

- All employees using the Company's email facilities shall make themselves familiar with the content of this policy.
- Users are expected to act ethically and responsibly in their use of e-mails and to comply with the relevant national legislation, and Information Security Policy and regulations.
- Discrimination, victimisation or harassment on the grounds of gender, marital status, family status, sexual orientation, religious belief, age, disability, race, colour, nationality, ethnic or national origin is against company policy. Users must not bully, or harass other individuals via e-mail.
- Users shall not send messages that are likely to be considered abusive, offensive or inflammatory by the recipient/s.

- All users shall regard all e-mails sent from the facilities as Sort Services, representing the company and, secondly, representing the individual. Users shall be civil and courteous as e-mails can easily be misunderstood.

4.12 Mobile use

Users must familiarise themselves with their responsibilities regarding mobile devices (portable computers and media) responsibility including the following procedures:

- Information stored on portable devices shall be backed up regularly, if required.
- All company's files that are not considered trivial in regard to Confidentiality, Integrity, and Availability required protection must always have their primary copy stored on the company's Network.
- Information stored on portable devices that is 'Private & Confidential' shall be secured in line with the Information Classification Policy, Labelling and Handling Procedures.
- All portable devices not catalogued as for testing purposes must be protected in line with the Password Policy.
- Users must:
 - Make every attempt to ensure that portable devices are physically secure at all times. This applies to all portable devices including laptops, USB keys, and Mobiles.
 - Not attempt to bypass restrictions put in place.
 - Not install any non-standard software unless prior authorisation has been received from the ISM.
 - Notify the Information Security Officer as soon as possible if any portable device is lost or stolen in line with the Information Security Incident Management Policy.

4.13 Personal Cloud Storage

The personal use of Dropbox, Google Drive, One Drive and other similar products that synchronizes files and/or could make available files from the company's network on remote locations is allowed provided:

- The user is aware and acknowledges that installing these types of programs and synchronizing leave a copy of their personal data on company hardware, and as such it may be subject to audits and inspection according to company policy.
- No non Public company content shall be copied onto the synchronized folder. If the user requires work data to be available out of the Company's Premises then he shall request from his manager an approved secure solution.
- Enabling the One Drive Fetch feature on One Drive, or any other similar feature that could allow remote browsing files in the Company's Network (such as the user's workstation) is not allowed.
- As a result of audits or otherwise, files may be deleted without any notice for a variety of reasons and the Company is not responsible for any side effects on synchronization or data loss anywhere else.
- Reasons why personal content copied/synchronized and stored on a Company computer include but are not limited to the possibility of the information containing malware, possibility of it being unlicensed, possibility of containing software considered potentially harmful or being licensed for personal use but

used for commercial purposes, system administration routine maintenance. Although deletion is incontestable the user may enquire as to how avoid it in the future.

- Users shall not send e-mail, which portrays the company in an unprofessional light. Any e-mail involved in a legal dispute may have to be produced as evidence in court.
- Users must not create or forward chain letters or unsolicited e-mails e.g. SPAM.
- All users must be cautious when opening e-mails and attachments from unknown sources as they may be infected with viruses.
- All users shall ensure that up-to-date anti-virus software is installed and operational on the computer that they access their email on.

5. Information security training

5.1 Training requirements

All awareness training must fulfil the requirements for the security awareness program as listed below:

- The information security awareness program should ensure that all staff achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior.
- Additional training is appropriate for staff with specific obligations towards information security that are not satisfied by basic security awareness, for example Information Risk and Security Management, Security Administration, Site Security and IT/Network Operations personnel. Such training requirements must be identified in departmental/personal training plans and funded accordingly. The training requirements will reflect relevant prior experience, training and/or professional qualifications, as well as anticipated job requirements.
- Security awareness and training activities should commence as soon as practicable after staff joins the company, generally through attending information security induction/orientation as part of the on boarding process. The awareness activities should continue on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness.
- Where necessary and practicable, security awareness and training materials and exercises should suit their intended audiences in terms of styles, formats, complexity, technical content, etc. Everyone needs to know why information security is so important, but the motivators may be different for workers focused on their own personal situations or managers with broader responsibilities to the organization and their staff.
- The company will provide staff with information on the location of the security awareness training materials, along with security policies, standards, and guidance on a wide variety of information security matters.

The Company's IT department requires that each employee upon hire and at least annually thereafter successfully complete an information security awareness course/training. Certain staff may be required to complete additional training modules depending on their specific job requirements upon hire and at least annually. Staff will

be given a reasonable amount time to complete each course so as to not disrupt business operations.

5.2 Simulated Social Engineering Exercises

The Company's IT department will conduct periodic simulated social engineering exercises including but not limited to: phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. The IT department will conduct these tests at random throughout the year with no set schedule or frequency. They may conduct targeted exercises against specific departments or individuals based on a risk determination.

5.3 Remedial Training Exercises

From time-to-time the staff may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of the IT department as part of a risk-based assessment.

5.4 Compliance and Non-Compliance with the training programme

Compliance with this policy is mandatory for all staff, including contractors and executives. The IT department will monitor compliance and non-compliance with this policy and report to the executive team the results of training and social engineering exercises.

The penalties for non-compliance are described in the subsections below.

5.5 Non-Compliance Actions

Certain actions or non-actions by the company's personnel may result in a non-compliance event (Failure).

A Failure includes but is not limited to:

- Failure to complete required training within the time allotted
- Failure of a social engineering exercise

Failure of a social engineering exercise includes but is not limited to:

- Clicking on a URL within a phishing test
- Replying with any information to a phishing test
- Opening an attachment that is part of a phishing test
- Enabling macros that are within an attachment as part of a phishing test
- Allowing exploit code to run as part of a phishing test
- Entering any data within a landing page as part of a phishing test
- Transmitting any information as part of a vishing test
- Replying with any information to a smishing test
- Plugging in a USB stick or removable drive as part of a social engineering exercise
- Failing to follow company policies in the course of a physical social engineering exercise

Certain social engineering exercises can result in multiple Failures being counted in a single test. The maximum number of Failure events per social engineering exercise is two.

The company's IT department may also determine, on a case by case basis, that specific Failures are a false positive and should be removed from that staff member's total Failure count.

5.6 Responsibilities and Accountabilities

Listed below is an overview of the responsibilities and accountabilities for managing and complying with the training program.

The Chief Information Security Officer/Information Security Manager is accountable for running an effective information security awareness and training program that informs and motivates workers to help protect the organization's and the organization's customer's information assets.

Information Security Management is responsible for developing and maintaining a comprehensive suite of information security policies (including this one), standards, procedures and guidelines that are to be mandated and/or endorsed by management where applicable. Working in conjunction with other corporate functions, it is also responsible for conducting suitable awareness, training, and educational activities to raise awareness and aid understanding of staff's responsibilities identified in applicable policies, laws, regulations, contracts, etc.

All Managers are responsible for ensuring that their staff and other workers within their responsibility participate in the information security awareness, training, and educational activities where appropriate and required.

All Staff are personally accountable for completing the security awareness training activities, and complying with applicable policies, laws, and regulations at all times.

5.7 Failure Penalties

The following table outlines the penalty of non-compliance with this policy. Steps not listed here may be taken by the IT team to reduce the risk that an individual may pose to the company.

Failure Count	Resulting Level of Remediation Action
Sort Services Failure	Mandatory completion of the initial standard staff training upon new hire – no remedial action
Second Failure	Mandatory completion of the annual IS training – no remedial action
Third Failure	Mandatory completion of the specific IS course based on their job/ roles – no remedial action
Fourth Failure	Face to face meeting with their manager
Fifth Failure	Face to face meeting with their manager and Head of Human Resources
Sixth Failure	Face to face meeting with the CISO and the Head of Human Resources - Possibility that additional administrative and technical controls will be implemented to prevent further Failure

	events
Seventh Failure	Meeting with CISO, CEO and Head of Human Resources - Possibility that additional administrative and technical controls will be implemented to prevent further Failure events
Eighth Failure	Formal review of employment with Head of Human Resources - Possibility that additional administrative and technical controls will be implemented to prevent further Failure events
Ninth and Subsequent Failures	Potential for Termination of Employment or Employment Contract