Security Policy

Staff Acceptable Use Policy

Security Policy

Overview. The objective of the policy is to show how it meets with or supports a security control for the user to adapt as part of their policy framework.

This policy statement can also be applied to other security standards such as NIST, ISO, CIS and ISA, or adapted to meet with local regulatory and/or client security obligations.

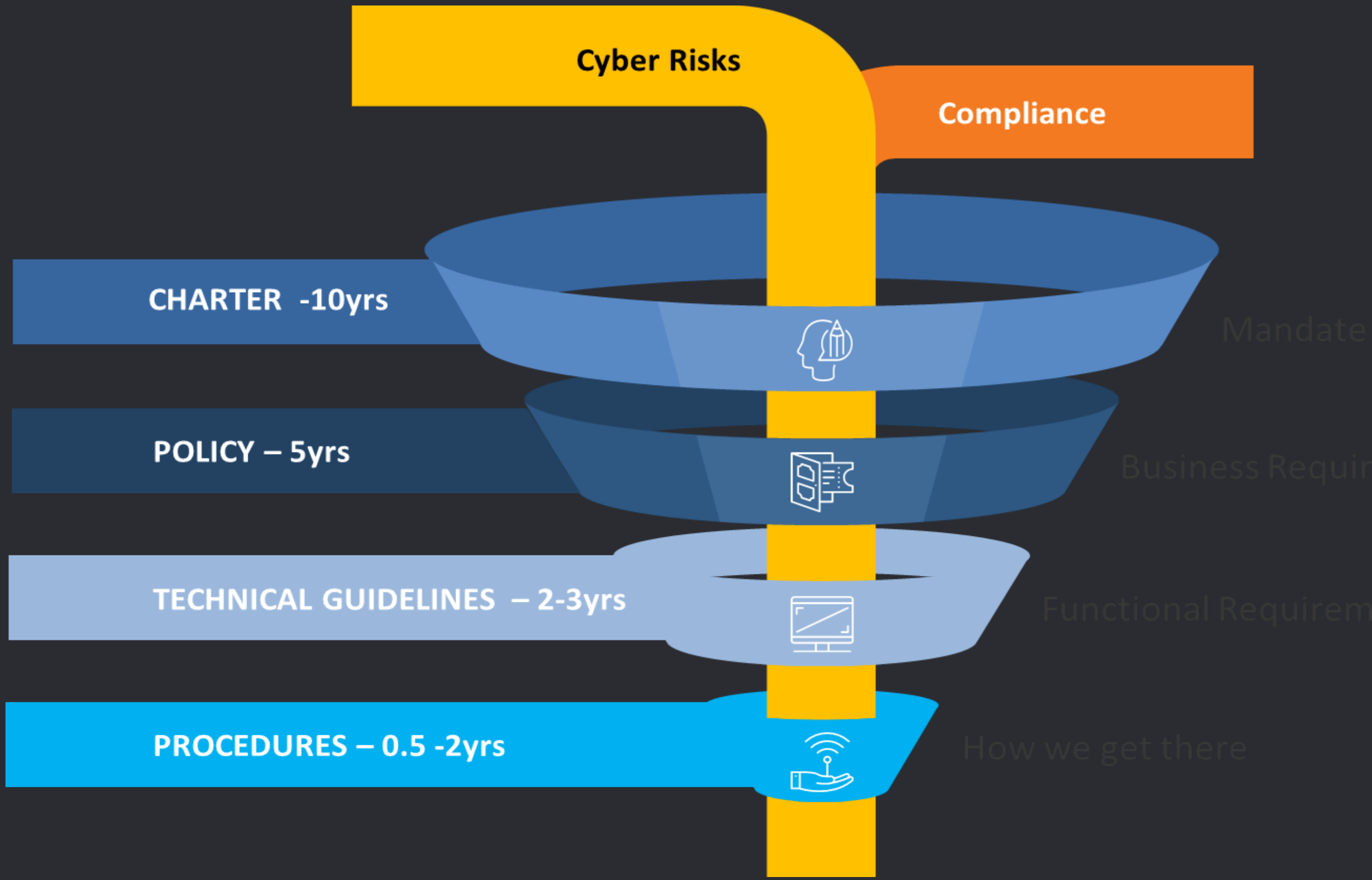
Inside a Policy

- Policy Title
- Policy Objective
- Scope
- Roles and Response
- Policy Statement
- Policy Owner
- Enforcement / Compliance
- Date / Expiry

Other Policies available

- CEO Policy Statement
- Acceptable Use Policy
- Security Awareness
- Data Classification
- Password Management
- Mobile Device Management
- Email Safety
- Social Media
- Vulnerability Management
- Policy Organization
- Remote Access
- Data Privacy

Policy Life Cycle



Cyber Risks

Compliance

CHARTER -10yrs

POLICY – 5yrs

TECHNICAL GUIDELINES – 2-3yrs

PROCEDURES – 0.5 -2yrs

Mandate

Business Requirement

Functional Requirement

How we get there

As the diagram suggests, the average lifetime expectancy of an IT policy is 5 years. However new policies are being developed continually within this period to address new risks and technology. Therefore, a process to create new Company policies are important.

Company policies are developed with a five (5) year lifetime in mind and are therefore high-level in design. The technical guides or standards supporting the policy are more regularly changed and are therefore designed in such a way to address the rapidly changing technology and the risk landscape or security ecosystem.

Policy Staff AUP

Objective

The purpose of this policy is to set out the requirements in relation to information security practices and the use of The Company systems, to enable the company to keep its employee, client, market and company information secure, and help minimise the risk of information loss, corruption, misuse, unauthorised disclosure, cyber risk e.g. virus attack, financial crime and business interruption. This Policy should be read in conjunction with local policy/procedures, which may set more stringent requirements, depending upon the type of information handled.

This Policy applies to The Company Staff which for the purpose of this Policy includes permanent employees, temporary employees, contractors, and consultants at The Company. This Policy applies to all equipment that is owned or leased by The Company, and personal devices, where permitted for business use.

Consequences

Individual(s) - failure to comply with this Policy will be considered a disciplinary offence which can result in termination of employment and/or legal action.

Policy Staff AUP

General Staff Policy Violations

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of software products that are not appropriately licensed for use.
- Unauthorised copying of copyrighted material including, but not limited to, distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the company or the end user does not have an active license.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws
- Deliberate Introduction of malicious programs (“malware”) into any information system (including but not limited to viruses, worms, Trojan horses, spyware, ransomware).
- Revealing account passwords to anyone, inside or outside of the company. The practical necessity of allowing colleagues or secretaries access to your account in certain circumstances needs to be weighed against the risks of misuse or disclosure at that point or in the future.

Policy Staff AUP

General Staff Policy Violations

- Using a company information system to engage in procuring or transmitting material that is in violation of local sexual harassment or hostile workplace laws.
- Making fraudulent offers of products, items, or services.
- Giving warranties, express or implied, unless this is a part of normal job duties.
- Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data the employee is not authorised to access or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, “disruption” includes any activity that adversely affects the availability of one or more hosts on a network, or the network itself, such as a denial of service attack or forged routing information.
- Port scanning or security scanning, unless prior authorization is obtained from the necessary senior management or this is within the scope of regular duties.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duties.

Policy Staff AUP

Company Email Usage

- The company e-mail system is not intended for personal use, but reasonable personal use may be permitted. Personal messages will be treated no differently from other messages. Accordingly, e-mail users are not entitled to privacy and personal e-mails sent via company information systems may be accessed, reviewed, copied, deleted or disclosed at the company's discretion.
- All e-mail remains the property of the company.
- Personal e-mail and web mail systems should not be used for any company business or to store or transmit business correspondence unless explicitly authorised. The use of personal web mail from office equipment should not be permitted.
- Users must not transmit or store e-mails containing material which is defamatory, pornographic, offensive, of a harassing nature (sexual, racial or other), breaches another's copyright, or contravenes the company's Code of Conduct. Reported incidents may result in disciplinary action being taken against involved parties up to and including termination of employment.

Policy Staff AUP

Company Email Usage

- Users must not attempt to unnecessarily view another’s e-mail. However, the company reserves the right to view a user’s e-mail in the following circumstances, when duly approved and authorised: …
- When the company has a business need to access the employee’s mail box (e.g. when a staff member is on long-term leave, and material needs to be retrieved from their e-mail)
- When the company receives a valid legal request to disclose e-mail messages from law enforcement officials or in ongoing legal proceedings
- When the company has reason to believe that the employee is using e-mail in violation of company policies
- Bulk distribution lists (“Everyone” e-mail groups, for example), should not be used except by authorised personnel.
- Users must not redistribute or forward any “chain” e-mails. Generally, the mere request in an e-mail that it be “forwarded to everyone on your list” is an indication that the contents are worthless. If the user is in any doubt, the e-mail must be forwarded to the IT Helpdesk.
- Large files (the precise size will be determined by the company’s IT department) should not be sent by e-mail without prior approval. If this cannot be avoided, the recipient should be warned beforehand.

Policy Staff AUP

Company Email Usage

- Users must not use their company e-mail address to subscribe to any mailing lists or newsgroups or register with any web site for their personal use.
- Users must give consideration to the volume of e-mails sent and received, and unnecessary copying and forwarding of e-mails (including by replying to another e-mail) should be reduced as much as possible.
- e-mails have the same legal status as written documents, and that they may inadvertently form contracts through e-mail correspondence and be held liable for representations or promises made via e-mail in order to secure a transaction. Users' authority in this regard must be strictly and expressly limited.
- e-mails, like any other document, may be used as evidence in a court. e-mail messages must remain on the company's systems even after they have been "deleted", so deleting may not avoid an obligation to disclose e-mails to a court. Likewise, important e-mails should be retained or archived (and/or a hard copy made). An e-mail may be protected from disclosure by "privilege" (e.g. when it is sent by a qualified lawyer when giving legal advice).
- Any legal sensitive, potentially litigious or prejudicial comments and should not be sent by e-mail (just like traditional forms of communication) as they may have to be disclosed; if such material must be sent, it must be sent by a lawyer.

Policy Staff AUP

Company Internet Usage

- Web access is provided at the company’s own expense for activities related to the company’s business. Limited personal use of web facilities, within reason, is permitted. Only employees with a legitimate corporate need to use the Internet should be granted access.
- Users must not deliberately use company information systems to access any web sites that contain material which is defamatory, pornographic, offensive, of a harassing nature (sexual, racial or other), breaches another’s copyright, or contravenes the company’s Code of Conduct. Nor should they do so on company premises using their personal mobile devices. If the user believes they have malicious software on their computer which is causing accesses to such sites, they must inform IT immediately.
- Employees should consider using their personal mobile devices for personal use of the web, rather than using company resources.
- Social networking: Sites such as Facebook, Twitter, Weibo, LinkedIn, etc. These sites can consume a lot of staff time, so The Company may restrict access so that only staff members with a business need to access the sites can do so.

Policy Staff AUP

Company Internet Usage

- Corporate web proxies will be used to control which staff are permitted to access the various different types of social networking and media web sites.
- The basic requirement for staff who participate in social networking and media activities, either for business purposes or for their own enjoyment, is that they will be held responsible for any facts or opinions about the business that they publish.
- Staff are reminded of the confidentiality obligations in their employment contract and must not breach those obligations when publishing material about the company in any form of social media.
- Before publishing anything online (text, pictures or video), staff must consider the implications: Who will see it? Who will share it, and how far could it get? How will it affect the company? How will it affect the staff member him/herself, and his/her colleagues?
- Any postings about the company or its staff should comply with the company's policy on racial, sexual and religious harassment. Sexual or racial slurs should be avoided, there should be no obscenity or insults, and sensitive topics like religion should be approached carefully. In all postings about the company, the poster is expected to be professional.
- Social network sites are not to be used for communication between co-workers about company-related issues (unless the site is a private social network hosted by the company).

Policy Staff AUP

Cloud Data Storage

- Staff must ensure the storage service is provided by a large, reputable organization.
- the storage service supports two-factor authentication and this is being used to protect the company information
- the account is dedicated for work use only and is considered to be owned by the company
- company information is not held in a “public” folder or accessible without authentication
- Use of cloud file storage, if permitted, must be registered so that when a member of staff who uses cloud file storage leaves the company, it is possible to verify that no company information remains in their cloud storage facility.
- Cloud-based password managers should be encouraged for personal use, since this reduces password re-use and therefore reduces the likelihood that a company password will be compromised through its re-use on a user’s personal account.
- Consumer-level cloud-based password managers should not be used to store passwords for any company systems or resources, or that protect stored company information. However, if the company has provided enterprise-grade password management tools, then the users should be required to use them.

Policy Staff AUP

Personal Devices- BYOD

- By using any personal device to access or store company information, you are consenting to the device being inspected or used in any manner at any time by the company, regardless of the ownership of the device. If the device has been used to access or store company information, the company has the right to demand deletion of all stored information and all user accounts created to access company information; the company also has the right to inspect the device to ensure this has been performed effectively and completely. The device shall be returned to its owner when the company is satisfied that the deletion is complete.
- Personal devices used to access company information systems will be held accountable for the security of these devices. These devices must not be left unattended at any time except if they have been deposited in a secure location such as a locked closet or a hotel safe. Devices containing confidential company information must not be lent to anyone.
- The loss of any device containing company information, whether owned by the company or by the employee, must be reported immediately to an appropriate management.
- information cannot be obtained by third parties, and that unauthorized individuals cannot access company information systems. Hence, personal device requires repair, that repair must be arranged through the company

Policy Staff AUP

Personal Devices – BYOD

- Users must back up devices containing company information by synchronizing with a workstation or laptop that belongs to the company or is approved by the company for business use at least once each week. Backups to the Internet (e.g. using proprietary online storage services like Dropbox) must not be made unless additional compensating controls exist to prevent information being accessed (e.g. backing up to iCloud).
- Users must not access company web mail servers by means of third-party gateways. This activity places the user’s login ID and password in the hands of untrusted third-parties.
- Employees who use personal devices for business purposes should receive regular awareness training to ensure that they remain aware of their obligations to report the loss/theft of such devices, to use strong device passwords, and to ensure that the authentication credentials for any company accounts (e-mail and otherwise) are not compromised.

Policy Staff AUP

Company Laptops and Desktops

- Desktop and laptop computers are issued to staff by the company, at its own expense, for business purposes only.
- Staff may not install (and should not be able to install) any software on company computers without the permission of an appropriate manager.
- It is forbidden for staff to attempt to escalate privileges on a company desktop or laptop above those granted by the company.
- Laptops must not be left unattended in public places, or in any part of a car. In hotel rooms, if possible, the laptop must be locked in the safe while the room is unoccupied. If the staff member is a visitor in an office, the laptop must not be left unattended for any period of time; the staff member must carry it, or lock it in a desk drawer. In the event that a laptop is lost or stolen, the staff member must inform his/her manager immediately.
- Company laptops must not be used by or lent to any other individuals, including the staff member’s own family.
- Security devices (including multi-factor authentication tokens) must not be kept in the same bag as the laptop.

Policy Staff AUP

Company Laptops and Desktops

- Users should not install or use instant messengers for discussing business-related information or exchanging files unless they (a) support encryption using a recognized standard protocol and (b) that encryption cannot be disabled, or a warning is given if the other party (or parties) do not support end-to-end encryption.
- This is applicable also to instant messengers on mobile devices (e.g. WhatsApp, WeChat, and a huge number of others). Apps like WhatsApp support end-to-end encryption and indicate when the other party cannot support it. Apps like WeChat do not support end-to-end encryption. QQ supports encryption but the protocol is proprietary and not documented.
- Users should not use instant messengers to send or receive company information.

Policy Staff AUP

Removable Storage Media

Removable storage is defined as:

- Drives (e.g. external hard disc drives, DVD writers)
- Flash memory (e.g. USB drives, memory cards connected via an internal or USB adaptor)
- Storage on portable devices (e.g. phones, tablets, MP3 players, digital cameras)

- Removable storage devices introduce an element of risk that data held on them may be lost or stolen, and that some devices may be used as a vector for introducing malicious software onto the company's systems.
- Users may not use their own personal removable storage devices without permission from a manager. That permission will be based on the capabilities of the device in terms of encryption of data, backup of data, and business case. Where the company issues its own equivalent devices, these will be used in preference to the user's personal device.
- Users must not use removable devices to take company information away from the office without a suitable business case and authorization from their manager. However, devices may be used to exchange information within the office, as long as they are scanned for viruses before use and information is securely deleted after use.

Policy Staff AUP

Removable Storage Media

- Users must not use removable devices to circumvent other security restrictions, e.g. bringing files into the company network that are not permitted to be downloaded using the company’s Internet connection.
- The loss or theft of a memory stick or removable storage device containing company information must be reported to the user’s manager immediately.