Security Policy

Policy Organisation

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.

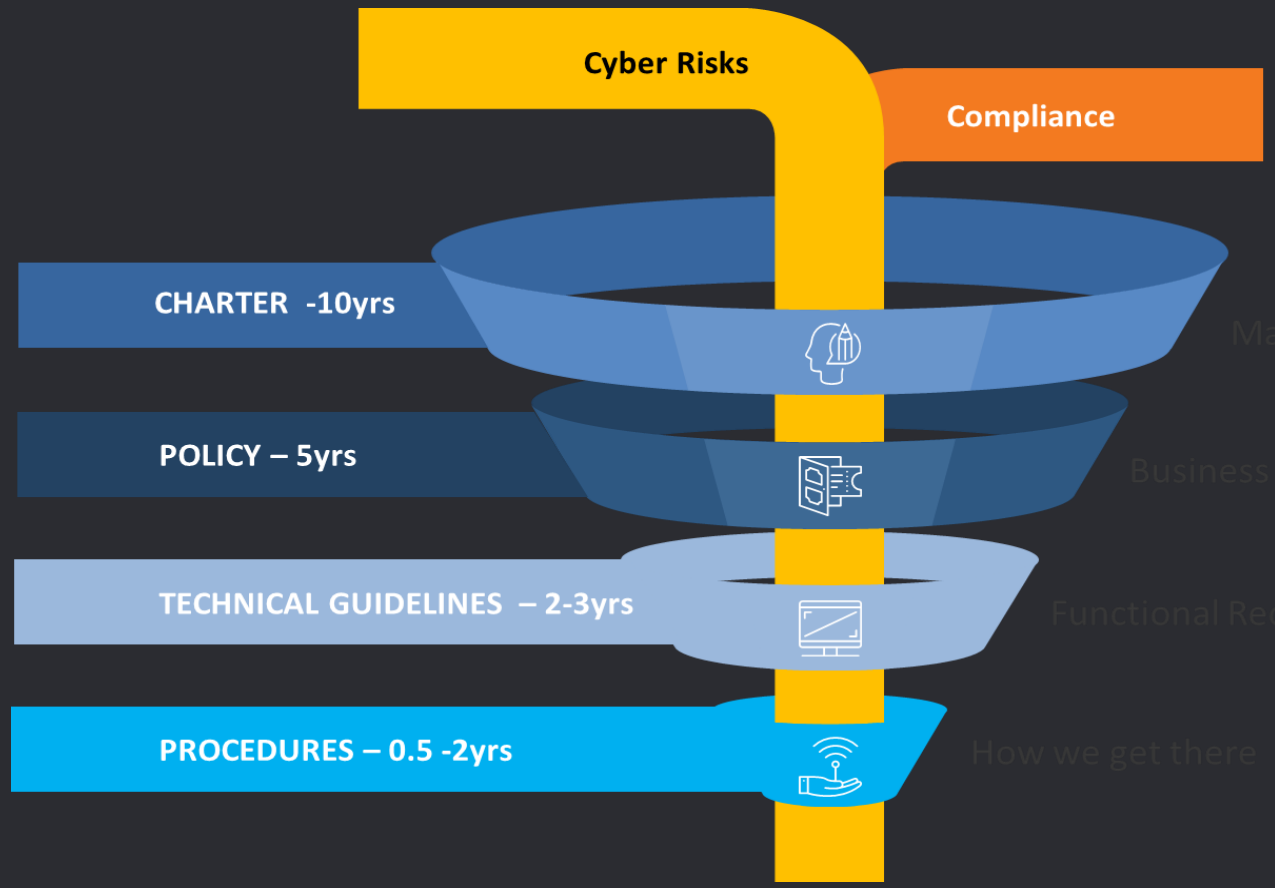
Inside a Policy

- 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



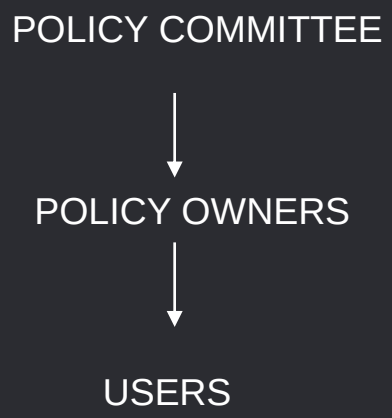
As the diagram suggests, the average lifetime expectancy of an IT policy is 5 years. However new policies are being developed continually within this period to address new risks and technology. Therefore, a process to create new Company policies are important.

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: Policy Organisation

Policy Organisational Structure

Information security is addressed as necessary through a series of structures. The structure of these committees is shown below and the members and responsibilities of each area.



Policy: Policy Organisation

Policy Committee

Information security is addressed as necessary at the Policy Meetings to ensure that there is clear direction and visible management support for security initiatives.

Committee security responsibilities:

- minimising company information asset exposure
- embedding information security within the company information planning process
- approving the information security policy
- coordinating policy implementation across the company
- promoting information security awareness
- reviewing serious information security incidents and enhancing policies and procedures as necessary
- approving major initiatives to enhance information security

Policy Owner

The owners of the policy are responsible for:

- ensuring the information under their control is secured as effectively as practically possible
- classifying information under their care
- authorizing access to those who have a business need for the information
- removing access (or modifying it) from those who no longer have a business need for the information
- communicating access control requirements to IT management and the information users
- monitoring policy compliance with their scope of authority
- responding to any detected security incident and ensuring it is reported

Policy: Policy Organisation

Users

All staff members have responsibilities for safeguarding the company's information and computing assets and for ensuring that third parties (such as consultants and contractors) do the same. This involves complying with the information security policy, acceptable use policies, and all practices and supporting procedures designed in accordance with the policies.

Specific user responsibilities are addressed and communicated by company on security requirement statements. Where practicable, users should acknowledge acceptance of responsibilities by signing a document to show statements have been received and understood.

Team members (including staff and third parties) are accountable for their actions. Any unauthorised deviations from the information security policy may result in disciplinary action, including termination of employment.