Security Policy

3rd Party Management

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.

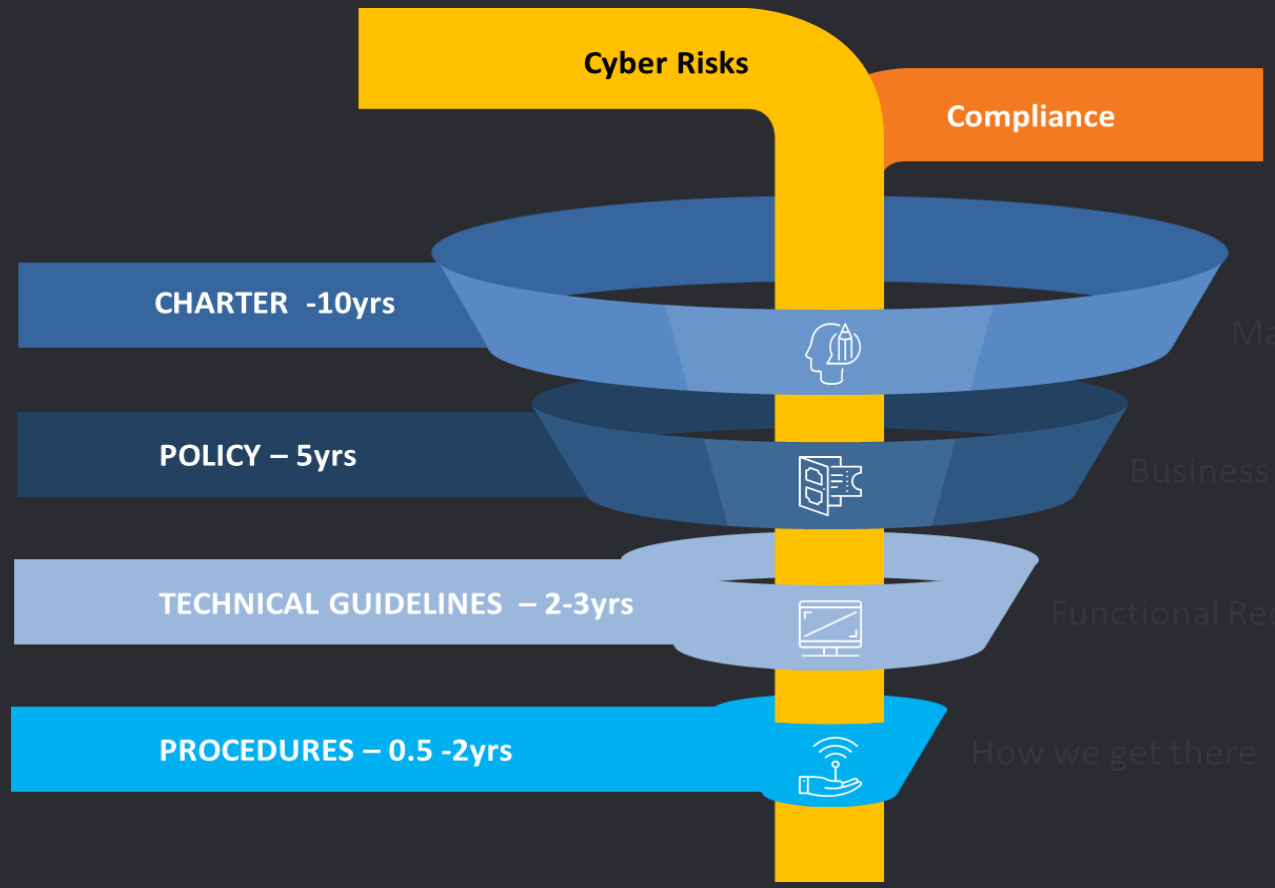
Inside a Policy

- 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: 3rd Party Management

Policy Objective

Scope
This policy shall apply to all The Company Users partnering with 3rd party to provide a service for The company

Roles and Responsibility
The Company Management are responsible to ensure vendor management procedures are followed. Company Users are to follow the 3rd party management policy guidelines

Enforcement / Compliance
Vendor mgmt. procedures and 3rd party audit reviews

Policy Owner
Business Owners, Vendor Mgmt.

Effective date: Last Reviewed: By:

Policy: 3rd Party Management

Policy Statement

- Third parties comprise of any external supplier (including entities performing outsourcing functions, like managed security service providers – MSSPs) who:

    - has access to company networks
    - holds copies of data, e.g. off-site backup storage
    - is responsible for maintaining hardware, infrastructure or applications that support company information assets
    - is responsible for hosting any company information system assets in their own network, cloud or data centre
    - in some other way has access to confidential or sensitive data owned or used by the company

- Access by third parties to the above functions shall occur only where it is strictly necessary. The full security implications of providing third party access to company information will need to be assessed as far as practically possible.

Policy: 3rd Party Management

Policy Statement

- All contracts clearly state the information and/or systems to be accessed by the third party and how security incidents will be dealt with.
- All contracts contain appropriate clauses to protect the company's information
- The third party is responsible for informing the company immediately of any security incidents.
- Any company employee who is aware of security violations by a third party will report them in accordance with company incident reporting.
- Third parties must sign a confidentiality agreement to protect The Company's sensitive information.
- Where the third party has access to cardholder data, or a cardholder data environment, the following requirements apply:
    - The company will add the third party's information to a list of "service providers" that interact with cardholder data
    - The agreement between the company and the third party will include an acknowledgement from both parties showing the extent to which the third party has responsibility for the security of cardholder data, which PCI DSS version is being used, and which PCI DSS requirements are partly or wholly the responsibility of the third party

Policy: 3rd Party Management

Policy Statement

- The contract with the third party includes the right for the company to audit their environment for security controls protecting the company's data and systems, documentation of physical and logical controls employed by the third party, determination of all legal requirements including privacy and data protection and the approach or standard that the third party will use to maintain and test system security on an ongoing basis.
- Detailed documentation of third parties with access to company networks is maintained and re-assessed at regular intervals to ensure that the requirement is still valid.
- Where the third party is unable to comply with the company security standards, senior business management is be made aware of the areas of non-compliance and of any potential security issues that could result from a failure to comply.
- Operating units shall maintain the right to monitor and terminate any connection to or from a third party that is deemed to be in breach of any security measures or requirements, or causing disruption to other users.
- For physical access to the company's systems, the third party must be escorted.