
Security Policy
CEO Policy Statement

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.

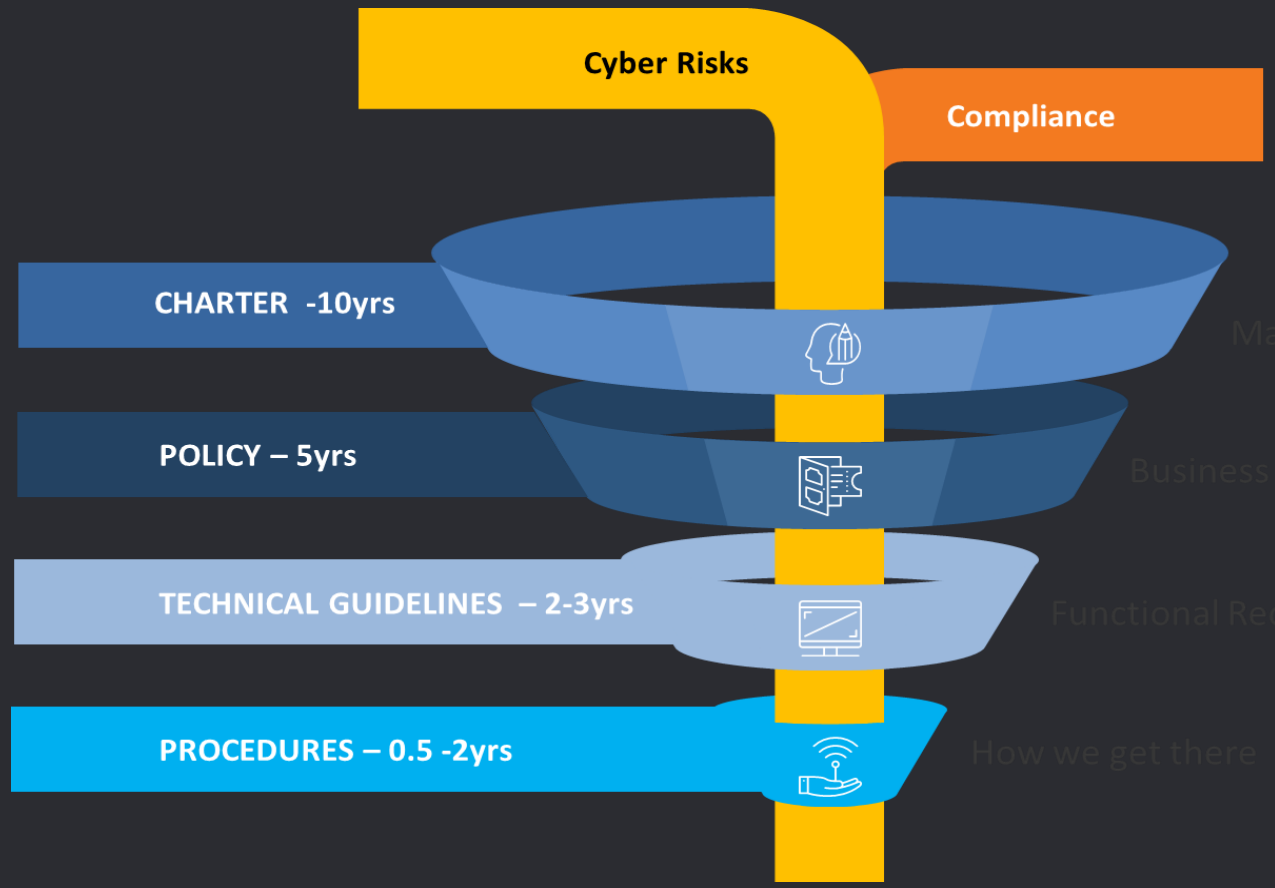
Inside a Policy

- 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: CEO Policy Statement

The Need for Information Security Policy
This information security policy statement is applicable to all existing and proposed systems within The Company and is effective from the date of issue of this policy. The manager responsible for each system must ensure that all risks are identified and reasonable measures are taken to protect the Company Assets.

Scope of Policy
These security policies apply to all Company Assets Owned, Rented, Hosted and all staff, users, permanent employees, contractors, consultants, agents and suppliers.

Advice and Assistance
The Company IT Manager or Business Owner is responsible for developing, monitoring and reviewing The Company's Information Security Policies

Management Responsibilities
All managers and supervisors have security as part of their normal duties. Senior managers are accountable for enforcing The Company Security Policies. The Company promotes an environment of openness that allows anyone to report security breaches without fear of reprisal. The security performance of all staff with management or supervisory responsibilities will be monitored and assessed in regular reviews. Managers are responsible for the prevention, investigation and reporting of incidents that infringe The Company Information Security Policies.

Policy: CEO Policy Statement

Employee Responsibilities
The Company expects all employees to safeguard company information and to use resources provided by The Company for information exchange in a professional manner. Breach of this policy by anyone in any way that impacts The Company may result in disciplinary action. All Staff are responsible for maintaining the Confidentiality of The Company 'and our Clients' data and information and safeguarding its security.

Risk Assessment
Regular information security audits will be undertaken at all locations where information is stored or processed. Tests to determine vulnerabilities will be undertaken at every location and management is responsible for acting upon the reports that are produced as a result of this preventative work. These tests may be undertaken without notice or involvement of local management

Training and Awareness
Training and advice will be provided at induction and regularly thereafter to ensure all our employees understand the security risks and the need for precautionary measures.

A copy of our Security Policies will be made available to every employee.

Signature

CEO