
Technical Guide
Password Standards

Technology Guide

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

This Technical Guide 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.

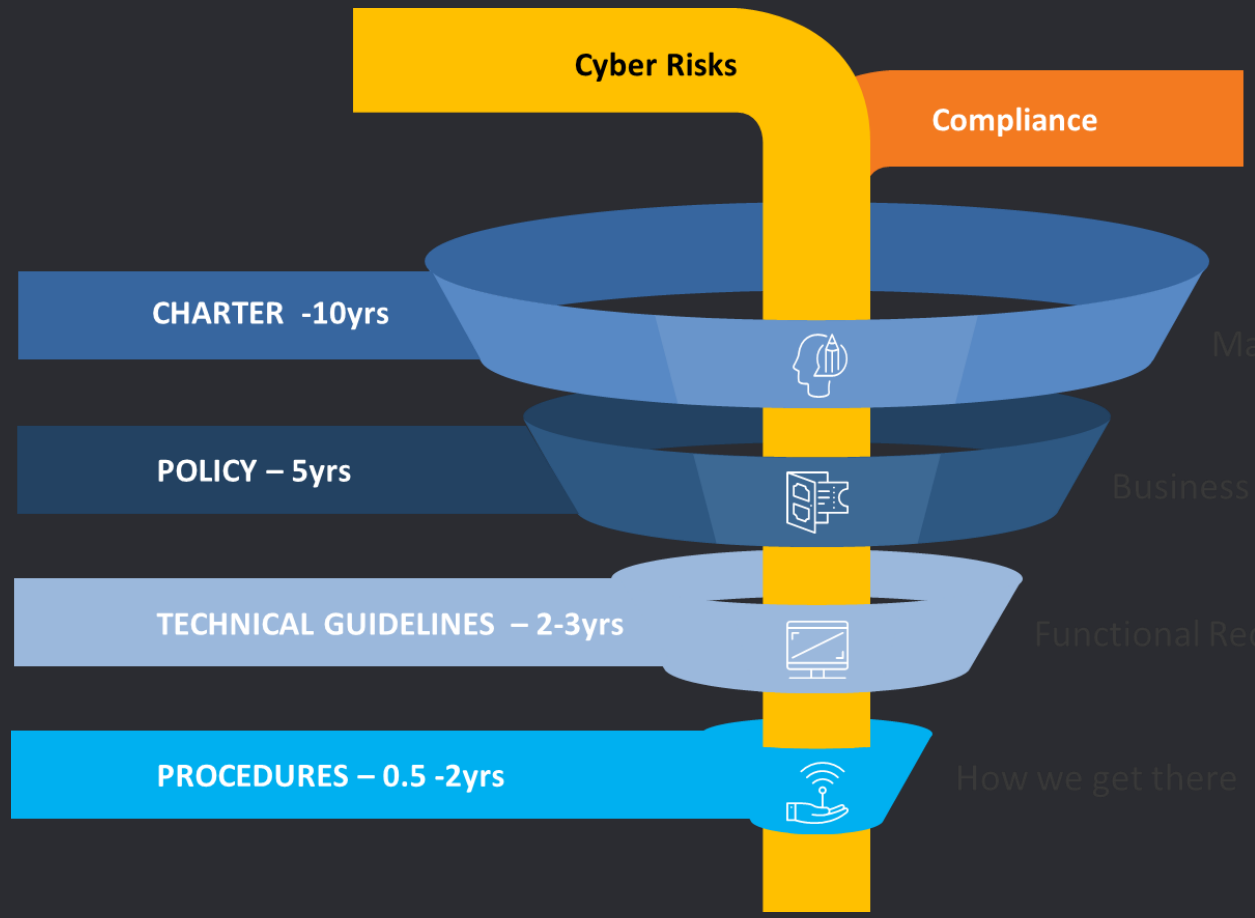
Inside a Technology Guide

- **Technology Scope**
- **Technology Configuration**

Other Technology Guides

- **Encryption**
- **Password Standards**
- **Email Secure**
- **Operating System Security**
- **Network Monitoring SNMP**
- **Wireless Security**
- **Vulnerability Management**
- **Privilege Accounts**
- **Anti Virus Settings**
- **Remote Access**
- **Patch Management**

Technology Guide Life Cycle



As the diagram suggests the average lifetime expectancy of a Technology Guideline is 2-3 years. However new technologies are being developed to address new risks and therefore a process to create new Technology Guides are important.

Technology Guides are developed with a two (2) year lifetime in mind and are therefore tactical in design. Your technology operational procedures 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.

Technology: Password Standards

Password Configuration

- Password minimum length must be 8 alphanumeric characters
- Expiry of all passwords shall be set at 90 days minimally
- Password history, where it can be set via the system, should be set at minimally user's last three passwords
- Account will be lockout after no more than five failed login attempts
- A lock-out duration of at least 30 minutes will be initiated after the above failed login attempts, or until an administrator intervenes

Passwords supporting business application or system access must be complex and adhere to the following format rules.
Passwords must adhere to the following content rules. The chosen password should:

- Not be a name (e.g. individual, place, location etc.)
- Not be a telephone number (e.g. Office number, Home number)
- Not be a date (e.g. birthday)
- Not be a car registration (or your Global Link Id)
- Not be a post code / zip code
- Not be the same as any password used on any home computing equipment
- Not be easily identifiable with the person, such as through social media web sites

Where the host computer system does not support complex passwords, the chosen password must adhere to as many of the format rules as possible and must adhere to all of the content rules.

Technology: Password Standards

Password Creation

- Users must not use the same password for accounts as for other non-access (for example, personal ISP account, option trading, benefits, and so on).
- Where possible, users must not use the same password for various access needs.
- User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
- Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

Password Change

- All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
- All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.
- Password cracking or guessing may be performed on a periodic or random basis by the InfoSec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

Technology: Password Standards

Password Protection

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
- Passwords must not be revealed over the phone to anyone.
  - Do not reveal a password on questionnaires or security forms.
  - Do not hint at the format of a password (for example, "my family name").
  - Do not share passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
  - Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
  - Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Application Development Passwords

- Application developers must ensure that their programs contain the following security precautions:
- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management; such that one user can take over the functions of another without having to know the other's password.

Technology: Password Standards

Use of Passwords and Passphrases

- Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.
- Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."
- A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

“Maythe4thBWithU"

All of the rules above that apply to passwords apply to passphrases.