Password Policy - Sample

Policy Brief and Purpose

Rampant re-use of passwords is one of the largest issues within organizations. [Organization] believes that our people are truly the best defenders against cybercrime. According to recent research from the National Institute of Science and Technology, password length is the best defence.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any facility, has access to the network, or stores any non-public information.

Policy Elements

• 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).
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential information.
• Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.
• 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 [Organization] 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. There are several password managers that are approved by yourIT team including iCloud Keychain, LastPass, Dashlane, RoboForm, etc.