Password Standard

1.1 Overview

Passwords constitute a critical underpinning of computer security. They are the front line of protection for user accounts. Poorly constructed passwords may weaken the security of CPAC's information and information technology assets.

To ensure that CPAC's information and information technology assets remain secured appropriately, effective password controls are defined in this document. CPAC may impose more direction at its discretion.

1.2 Purpose

The purpose of this document is to provide a set of minimum privacy and security standards (hereinafter called 'the Standard') to be implemented in the context of securing CPAC's information and information technology assets through the use of passwords.

1.3 Scope

This standard applies to all CPAC employees, consultants and contractors who use CPAC's information technology assets. **This standard does not apply to CPAC's Cisco telephone system or the Ricoh multifunctional printers.**

1.4 Standards

i. All user passwords will expire every 90 days.
ii. Users will not be able to use the previous 10 passwords associated with their user account.
iii. User accounts that have system level privileges granted to CPAC's information and information technology assets must use CPAC's Administrator Password Software to securely store all administrative passwords.
iv. Passwords should not be inserted into email messages or other forms of electronic communication.
v. All passwords must be a minimum length of 8 characters and conform to the guidelines described below.

vi. The use of passwords that are difficult to guess are a critical underpinning of system security. Strong passwords are best created from passphrases that exceed 15 characters in length and are a sequence of words. All passwords or passphrases must contain the following characteristics:
   - Contain characters from each of the following four categories:
     - Uppercase characters (e.g. A-Z)
     - Lowercase characters (e.g. a-z)
     - Base 10 digits (.g. 1-9)
     - Non alphabetic characters (e.g. #$^%!+??/)
   - Are not based on personal information, such as names of family members.
   - Are not written down or stored on-line, unless other measures are in place to protect the password from unauthorised access.

vii. All passwords are to be treated with the strictest of confidence.

viii. Passwords are not to be given to any other person with the exception of the CPAC IT Service Desk for issue resolution or maintenance.

ix. If a password has become known to another person, it must be reset immediately.

x. Authentication is required in some cases for off-premises access to CPAC's information and information technology. The circumstances under which authentication is required, and the type of authentication that is required for each circumstance, is described in the Information and Information Technology (I&IT) Security Policy.

1.5 Enforcement

Failure to comply with this standard may result in actions which include but are not limited to the following:

i. Denial of access to CPAC's information and information technology assets.

ii. Contractual remedies, as may be appropriate for third party suppliers, consultants and/or contractors, such as provisions for breach or termination of contract.

iii. Disciplinary action for employees, including, but not limited to, written warnings, suspensions with or without pay, and/or immediate termination of employment for cause without notice or other obligations.

1.6 Definitions

Term	Definition
Information and Information Technology Assets	Computer equipment (including laptop and desktop computers), software, operating systems, storage media, network accounts, electronic mail, internet access, portals, gateways, network devices, mobile devices, servers, telephones and telephone systems, multifunction printers, personal/home computers while they are connected to the CPAC network either directly or over a VPN connection, information assets (whatever the media or format type) such as business or personal information, and any other thing that may be considered by CPAC to be an information and information technology asset.
User	Any person who accesses and uses CPAC's information and information technology assets.

1.7 Related Documents

- Information and Information Technology (I&IT) Security Policy
- Acceptable Use Policy
- Mobile Devices Policy
- Bring Your Own Device (BYOD) Policy
- Electronic Mail Standard

End of Document