REFERENCE SHEET

MANAGING ACCESS AND PASSWORDS

Purpose of the document

Manage accesses and passwords securely.

A stolen password or improper use of access codes can enable an ill-intentioned person to consult or steal confidential information and even carry out unauthorized transactions on a company's system.

This document will help you ensure better access management and strengthen your password security.

Document recipient: Person responsible for information systems security

Last updated: 2017-06

Access management

Creating, modifying, removing and reviewing access rights

- Notify the person responsibility for managing access rights when an employee arrives, changes position, leaves, or takes an extended leave. The manager must be sure to indicate the employee's position, the access rights to be granted, and the effective date of the change.
- Make sure that an employee who requests additional access actually needs it for their work before granting it.
- Check employees' accounts and accesses to applications annually so that managers can make sure that employees' accesses are still warranted by a business need.
- Make sure that access codes are personal, i.e. each employee is assigned a code and is responsible and accountable for using the one they are assigned.
- Deactivate access rights for any leave exceeding 2 weeks, excluding vacation.
- Deactivate access codes and remove access rights to applications or projects within 10 days of an employee's departure. Foster employee awareness - Cybersecurity kit
- Foster awareness among internal employees as well as external employees (e.g. consultants) about access code use and password protection as soon as they are hired.

Fostering employee awareness

- Foster awareness among internal employees as well as external employees (e.g. consultants) about access code use and password protection as soon as they are hired.

Passwords

The initial password must be disclosed securely to the employee (e.g. sealed envelope delivered in person). All initial passwords must be changed the first time they are used. It is important to create secure passwords because passwords that do not meet security requirements can be found by hackers in a few minutes.

Use complex passwords (at least 10 characters) in keeping with either of these two options:

Option 1: password containing random letters or numbers
- o Tip: Use the first letter of each word in a sentence
- o E.g. The sentence "My dog Fido is a white purebred poodle that barks" becomes "mdfiapptb"

Option 2: password made up of at least 3 words, excluding words to be avoided
- o E.g. tablesheetmountain
- o Avoid words associated with your immediate environment or personal or professional life. E.g. name of your spouse, child or pet, or the brand name of your computer or mouse

Do not:

- Use the passwords shown on this page as examples.
- Copy passwords in an Excel file, write them down on post-its, other than in password management software (e.g.: 1Password, KeePass).
- Share your passwords with anyone, not even a colleague, manager, assistant or any other employee, friend or family members, even if:
  - the technical assistance centre asks you for it. You must always enter your password yourself and not disclose it to a technical assistance centre employee
  - you're away on vacation or taking a leave
  - you're being replaced temporarily
  - you're asked for your password by email.