Clean Desk Security Policy

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

Information Security Branch, Ministry of Central Services

This document outlines the Government of Saskatchewan security policy for Clean Desks.

Purpose

To ensure sensitive information in work spaces is safeguarded.

Scope

This policy applies to all users with access to GoS information assets.

Policy Statements

Users must safeguard sensitive information in their work space from unauthorized access, loss or damage by:

- clearing desktops and work areas;
- locking hard copy sensitive information in an appropriate cabinet;
- locking portable storage devices with sensitive information in an appropriate cabinet;
- activating a password-protected screen saver;
- safeguarding incoming and outgoing mail;
- retrieving documents from printers and fax machines; and
- ensuring that unneeded sensitive hard copies are placed in shredding bins, not recycle bins.

When visitors, cleaning staff or other personnel without a “need-to-know” are in the area, safeguard sensitive information by:

- covering up and maintaining control of hard copy files;
- blanking computer screens or activating the password-protected screen saver.

Sensitive information must not be discussed in public or other areas where there is a risk of being overheard by unauthorized personnel.

Compliance and disciplinary action

In cases where it is determined that a breach or violation of GoS policies has occurred, the Information Security Branch, under the direction of the Chief Information Officer and the respective Ministry, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, or in the case of contractors, vendors, or agents, the termination of a contract or agreement with the contractor, vendor, or agent.

Exceptions

In certain circumstances, exceptions to this policy may be allowed based on demonstrated business need. Exceptions to this policy must be formally documented and approved by the Chief Information Officer, under the guidance of the Information Security Office. Policy exceptions will be reviewed on a periodic basis for appropriateness.