Purpose:

The purpose of this policy is to specify protection of end-user computing devices in university workplaces to prevent unauthorized access to Restricted Data or damage to computing devices.

Scope:

This policy applies to all university facilities where computing devices are used in the conduct of university business.

Policy:

1. Workplaces must be appropriately secured to prevent theft or damage of end-user computing devices.
2. Access to workplaces should be limited to only authorized persons.
3. Access to output devices (such as displays and printers) must be controlled to prevent unauthorized users from viewing or obtaining output.
4. Computing devices must be positioned to minimize damages from physical and environmental hazards.

Responsibilities:

1. All members of the University Constituency are responsible for maintaining the security of their workplaces. Violations of workplace security must be promptly reported, following unit procedures.
2. Information Security Administrators (ISAs) are responsible for unit procedures for the protection of workplaces and computing devices.
Deleted: The Vice President and Chief Information Officer (CIO) is responsible for implementing systems and specifications to facilitate unit compliance with this policy.