# CSEC-602 – Security Planning

## Assignment 2

(Acceptable Use of Office Computers Policy)

**Yuvraj Singh Gill**

**000560556**

**gill0680@saskpolytech.ca**

# CCU - Acceptable Use Policy for Office Computers

## Purpose

The purpose of this policy is to outline the acceptable use of office computers at Cyber Chaiwala University (CCU). These rules are in place to protect the authorized user and University's resources. It ensures the responsible, ethical, and secure use of university-owned computing resources by employees and authorized personnel.

## Scope

This policy applies to all faculty, staff, and other authorized users who have access to CCU's office computers and related systems.

## Definitions

- **Office Computer**: Any computing device provided by CCU for official work-related purposes, including desktops, laptops, and workstations.
- **Authorized User**: Any individual granted permission to access CCU's office computers and systems, including employees, faculty, and staff.
- **Sensitive Data**: Any information classified as confidential, proprietary, or personally identifiable that requires protection.
- **Unauthorized Access**: Any attempt to access files, systems, or networks without explicit permission.

## Acceptable Use

Users must:

- Use office computers strictly for work-related tasks such as academic research, administrative duties, communication, and university-sanctioned projects.
- Access only authorized systems, files, and networks as per their role and responsibilities.
- Maintain confidentiality and integrity of sensitive university data.
- Ensure compliance with all university policies, local laws, and regulations regarding digital communication and data protection.
- Use strong passwords and regularly update them to protect accounts.
- Report any security concerns, breaches, or suspected cyber threats to the IT department immediately.

### Unacceptable Use

Users must not:

- Use office computers for personal, commercial, or non-university-related activities.
- Download, install, or use unauthorized software or applications.
- Engage in activities that compromise the security, performance, or integrity of university networks and systems.
- Share login credentials, passwords, or sensitive university information with unauthorized individuals.
- Access, store, or distribute offensive, illegal, or inappropriate content, including hate speech, harassment, or discriminatory material.

### Monitoring and Compliance

- The university reserves the right to monitor computer usage to ensure compliance with this policy.
- Any violations of this policy may result in disciplinary action, including loss of access privileges, termination of employment, or legal action if applicable.

## Policy Acknowledgment

All employees and authorized users must read, understand, and acknowledge this policy before accessing office computers.

## Contact Information

For any questions or concerns regarding this policy, contact the IT Department at **it-support@ccu.edu**.

**Approved by:** Cyber Chaiwala University Administration

**Effective Date:** 23 February 2025

**Review Date:** 23 February 2025

# References


- Martins, A. (2025, January 29). Why you need an acceptable use policy and how to create one. business.com. https://www.business.com/articles/acceptable-use-policy/
- Firch, J. (2022, May 19). *Sample Acceptable Use Policy template*. PurpleSec. https://purplesec.us/resources/cyber-security-policy-templates/acceptable-use/
- Kirvan, P. (2024, November 18). What is acceptable use policy (AUP)? WhatIs. https://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP