WRITTEN PLAN

For the Institution's Technical Infrastructure

Approved by Accreditation Steering Committee: August 26, 2025

Purpose of this plan

This plan details the processes used by the Information Technology and Telecommunications (IT) Department to support and safeguard the College's technical infrastructure. Providing a safe, secure, and reliable technical infrastructure is critical for the ongoing operation of services to students, employees, and the public. In the sections that follow, the plan will outline the scope of services provided by the IT Department, the budgetary resources allocated to maintain and enhance technical systems, the major activities involved in sustaining infrastructure operations, the methods used for evaluating the effectiveness of these efforts, and the stakeholders with whom the plan is shared to ensure transparency, collaboration, and accountability.

Information Technology and Telecommunications Department

The College's Information Technology and Telecommunications Department is responsible for the planning, installation, maintenance, security, and support of the institution's technical infrastructure. This includes a wide range of systems and services such as network infrastructure, email, desktop and mobile computing devices, internet access, Wi-Fi access points, data storage, security cameras, door access controls, telephony, emergency alert systems, printers, and peripheral devices. These services are provided across both the main campus and the Collette Mercier Campus at Business Depot Ogden (BDO).

A critical function of the IT Department is to establish and enforce security protocols that protect the privacy of sensitive information and safeguard College resources from internal and external threats. Maintaining a secure and reliable technical environment is essential to supporting the ongoing delivery of services to students, employees, and the public.

Adequacy, Improvements, and Protection of Technical Infrastructure

To ensure the adequacy and continuous improvement of the College's technical infrastructure, the IT Department relies heavily on customer communication and feedback. These insights help identify system needs, assess performance, and guide enhancements.

Customer Feedback Mechanisms

IT Work Order System and Surveys: A web-based work order system allows users to submit IT service requests. This system not only tracks requests but also collects user feedback through integrated surveys, providing valuable data for service evaluation and improvement.

Director's Feedback Channels: The IT Director receives ongoing feedback through regular meetings with division directors, one-on-one conversations, and email correspondence. These interactions offer direct insight into system performance and user needs, enabling the department to make informed decisions and implement continuous improvements.

Emergency Backups

The College employs robust backup systems to protect all technical services, including student and staff data. These systems include both onsite and offsite data backups, ensuring redundancy and resilience in the event of data loss or system failure.

Data Center Design

The College data center has redundant power to all major systems. The data center also has dual cooling units to allow continued operation in the event of a failure. These features remove single points of failure and provide more reliable redundancy.

Data Center Reliability

The College's data center is engineered for high reliability, featuring redundant power supplies and dual cooling units to eliminate single points of failure. To maintain system accessibility during power outages, the data center is equipped with backup batteries and an emergency generator that self-tests weekly. These systems ensure uninterrupted operation of critical services and allow for controlled shutdowns during extended outages. Emergency power also supports continued operation of telecommunications, surveillance, and network systems for a limited time after a power loss.

Uninterrupted Power Supplies

Each secure network closet across campus is equipped with battery backup systems that provide temporary power during outages and protect equipment from surges. These systems are monitored and notify the IT department of power disruptions or equipment failures, enabling proactive maintenance and ensuring system reliability.

Ongoing operation and maintenance of technical infrastructure

The IT Department is staffed by qualified professionals, including a director, two system engineers, senior technician, technician, and IT security analyst. Additional support is provided

by contracted IT professionals and installers. Together, they ensure the continuous operation and maintenance of the College's technical infrastructure.

Periodic Review and Replacement of Software and Equipment

To maintain optimal performance, the College reviews and replaces key systems on a regular cycle. Desktop computers, data center hardware, and networking equipment are evaluated for replacement approximately every five years. Reviews consider cost, manufacturer support, spare parts availability, and technological relevance. Software agreements are typically reviewed and renewed annually, allowing for adjustments to improve operations.

Standardized Hardware

The IT Department uses standardized equipment wherever possible, including computers, printers, and networking devices. This approach simplifies maintenance, improves efficiency, and ensures consistency across the College's technical environment.

Support Contracts and External Contractors

Support contracts are maintained for critical systems, providing access to replacement parts and technical assistance. In cases of equipment failure, these contracts are essential for timely troubleshooting and resolution. The IT Department also engages external contractors for specialized maintenance and complex technical issues beyond internal capabilities.

Equipment and Supplies

A stock of commonly used equipment, spare parts, and tools is maintained to support daily operations. The IT Department ensures that diagnostic tools, expendable materials, and miscellaneous items are readily available to address routine and emergency needs.

Privacy, safety, and security of data

The College enforces its Information Technology Acceptable Use Policy (540.19) to guide responsible use of IT resources, protect networks and systems, and maintain a safe learning and working environment.

Content Filtration

To ensure safe internet usage, the College employs URL and content filtering systems. All internet traffic is monitored and categorized, enabling accurate reporting and blocking unsafe or irrelevant content.

Malicious Content Prevention

The College utilizes a comprehensive security system that includes an Intrusion Prevention System (IPS) and application inspection tools. The IPS actively monitors and blocks unauthorized access attempts by identifying threats in real time. Application inspection enables the IT Department to analyze network traffic, identify application types, block unnecessary applications, and restrict risky applications to approved uses.

User Rights Restrictions

To minimize the risk of malicious software installations, all College desktop computers, laptops, and tablets are restricted from installing software without prior IT approval, unless an exception is granted by College Administration. This policy ensures tighter control over the software environment and enhances network security.

Antivirus and Endpoint Protection

The College deploys centrally managed antivirus and endpoint protection software across all computing devices. These tools are automatically updated and monitored to prevent the execution of potentially harmful programs, ensuring consistent protection against malware and other threats.

Network Security Zones

The College's network is segmented into distinct security zones, allowing for granular control and visibility of traffic flow between users, systems, and resources. This zoning strategy supports the enforcement of security policies and helps prevent unauthorized access across different parts of the network.

Password Security

Access to College systems is protected by user authentication protocols requiring unique passwords that meet complexity standards. These passwords are enforced by system policies.

Multifactor Authentication

To further enhance security, multifactor authentication (MFA) is implemented across many College systems. In addition to a username and password, users must verify their identity through an authentication app on a mobile device. This significantly reduces the risk of unauthorized access due to compromised credentials.

Centralized Configuration and Security Enforcement

All College computers are managed through centralized configuration software, which ensures consistent application of security policies and system settings across the institution's devices.

IT Security Controls Framework

The College is adopting a standardized IT security framework consisting of 150 controls designed to strengthen its cybersecurity posture. This framework provides a structured approach to managing risks and protecting institutional data and systems.

Data Privacy

Access to sensitive data is strictly controlled based on job responsibilities. By default, employees are granted the lowest level of access, with elevated permissions provided only to those whose roles require it. This role-based access control is enforced alongside other security measures to protect the privacy of institutional data.

Employee Orientation, Training, and Threat Testing

New employees receive orientation on College network systems, including password setup, MFA, and security best practices. Ongoing cybersecurity training is delivered through a third-party online platform, with employees periodically enrolled in courses and required to complete them by set deadlines. Completion certificates are provided for professional development documentation.

To assess awareness and preparedness, the IT Department conducts periodic phishing and threat simulation tests. These exercises help identify areas where additional training may be needed and reinforce safe computing practices.

Distance Education Infrastructure

In partnership with the Utah Education Network (UEN), the IT Department ensures continuous support for the College's distance education infrastructure. This includes 24/7 remote access to instructional content and availability of IT staff during evenings, weekends, and holidays to resolve technical issues.

Budgetary Resources

The College allocates annual funding to support the objectives outlined in this plan. Budgets are reviewed and approved by the College Board of Trustees to ensure adequate resources for maintaining and improving technical infrastructure.

Annual Evaluation and Distribution of the Plan

Feedback from students and employees is collected through the online help desk ticket system and post-service surveys. Annually, the plan is distributed to all College employees via email for review and input. The final version is approved by the College Accreditation Steering Committee to ensure alignment with current COE standards. Once approved, the plan is published on the College website under the "Policies and Plans" section for access by employees, students, and the public.