CONNECTICUT COLLEGE

College Owned Computer Use

Service Level Agreement

Revised July 21, 2017

Purpose

This agreement has been designed to inform employees of best practices to protect college-owned equipment and sensitive data stored on the equipment.

Connecticut College provides many computing tools to its employees to enhance their productivity and jobs. These tools include computers and their software, internal networks (e-mail, intranet, VPN etc.), external networks like the Internet, telephone systems, voice mail, fax, copiers, etc. Connecticut College requires that these systems be used in a responsible manner, ethically and in compliance with all legislation and other Connecticut College policies and contracts.

Individuals at Connecticut College are encouraged to use the college systems to further the educational and business goals and objectives of the college. The types of activities that are encouraged include:

- Communicating with fellow employees, students, colleagues, and businesses within the context of an individual's assigned responsibilities;
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.

Computer User's Responsibilities

It is the responsibility of every Connecticut College employee to make every reasonable effort to handle all college-issued equipment with care and to protect the college's data. You or your department will be responsible for damages from negligence, accidents or user abuse.

Physical Security

All computing devices must be used and stored in a safe and secure location.

Every computer must run a College-approved antivirus software and its auto-updating agent.

Every computer must run a current supported operating system that is updated at the regular vendor-defined cycle, except as otherwise directed by IS.

The removal or modification of college installed computer management, antivirus, network or security software is not allowed.

When travelling with any equipment, ensure the equipment is on your person, or if it does need to be stored in the vehicle, ensure the vehicle is locked and the equipment is stored out of sight before reaching your destination. Take precautions to deter theft of any equipment in your possession.

You are responsible for the physical care of the computer. If repairs need to be performed due to negligence, accidents or user abuse (i.e. liquid spilled on keyboard, dropped notebooks or intentional damage), the repair service charge will not be covered by the manufacturer's warranty. **You or your department will be responsible for the cost of repairs.**

CONNECTICUT COLLEGE

Data Security

Be aware of the sensitivity of data that may be stored on the college's computing devices. All computer users must take special precautions to prevent the loss or disclosure of sensitive information. These precautions include:

Never give out your password to another person.

Password protect access to the computer.

Do not change screensaver access settings without authorization.

Do not share a computer that contains FERPA protected, sensitive, or personally identifiable information with a person that is not authorized to view that information.

Do not install unauthorized software, screensavers, and toolbars.

Do not connect to gaming and file sharing web sites without authorization.

Data will be backed up with CrashPlan, do not turn off CrashPlan.

Your supervisor and the Information Security Officer must be notified immediately if your password is compromised or if your computing device is missing.

VPN and general access to the Internet

VPN and general access to the Internet for use by immediate household members through the Connecticut College network on college-owned computers is prohibited. The Connecticut College employee bears responsibility for the consequences should the access be misused.

Non Compliance

The ETS/Information Services will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, application tools reports, internal and external audits, and feedback.

Any exception to the policy must be approved by the Information Security Office in advance.

Non-compliance of this policy and procedures, may result in disciplinary action, following the usual disciplinary processes of the College for faculty and staff. The Vice President of the Administration Division will determine whether to initiate the disciplinary process.

CONNECTICUT COLLEGE

Employee Name:

Department:

Assigned Computer:

Description: _____

Connecticut College Bar Code # _____ Serial # _____

Date Issued _____

Additional assigned items:

Description: _____

Connecticut College Bar Code # _____ Serial # _____

Description: _____

Connecticut College Bar Code # _____ Serial # _____

Description: _____

Connecticut College Bar Code # _____ Serial # _____

I accept responsibility for the care and safekeeping of this equipment.

Employee Signature: _____ Date: _____

Installing Technician _____ Date: _____