CASTLETON UNIVERSITY
COMMUNITY COLLEGE OF VERMONT
NORTHERN VERMONT UNIVERSITY
VERMONT TECHNICAL COLLEGE

VERMONT
STATE COLLEGES SYSTEM

OFFICE OF THE CHANCELLOR
PO BOX 7
MONTPELIER, VT 05601
P (802) 224-3000

Policy 502 – Written Exception for Acceptable Use

The VSC Cybersecurity Team grants exceptions to VSC Policy 502 for the Vermont Technical College, CIS Department for educational purposes only for the following items in Article IV:

Article IV, Item 4: Sharing one’s password with others and allowing others to use one’s password or user identity or address are prohibited, unless specifically approved by the Chancellor, the appropriate college President, or designee.

Article IV, Item 7: Tampering with the physical network (cables, hubs, computers, and peripherals etc.) is prohibited.

Article IV, Item 8: Intercepting or attempting to intercept data is prohibited.

Article IV, Item 10: Logging on or attempting to log on to any piece of VSC computer equipment without an account is prohibited.

Article IV, Item 11: Using or attempting to use any network address or identity one has not be assigned by VSC or college authorities—even on a machine one may own—is prohibited.

Article IV, Item 18: The installation and/or removal of any software on a VSC- or college-owned machine without the specific written permission of the Chief Technology Officer (CTO), unless authorized by college policy or procedures, is prohibited.

Article IV, Item 19: The installation of any hardware device or component on a VSC or college-owned machine or the removal of such a device or component from a VSC or college owned machine without the specific written permission of the CTO, unless authorized by college policy or procedures, is prohibited.

Article IV, Item 20: Connecting a computer to VSCnet without specific written permission of the CTO, unless authorized by college policy or procedures, is prohibited

Article IV, Item 21: Operating a server of any kind on VSCnet without specific written permission of the CTO is prohibited. Operators of approved servers must provide server passwords to the CTO on demand.

These exceptions are granted under the condition that the VTSU Computer Science Department acknowledges and agrees to the following conditions of exception:

- Computer Science Network and Server environment is separate (logically or physically) from the VSC environment, including a Computer Science Department dedicated subnetwork.
- There shall be no VSC credentials shared among students or faculty.
- There shall be no storage of any non-educational institutional data.
- The Computer Science Department is responsible for maintaining their own server and network environment, with approval of new equipment from the VSC IT Department, along with any access to those systems by the VSC IT Department.
- There shall be no comprising or attempted compromising of any institutional system or external system not within the CIS contained environment.
- The CIS contained environment is subject to periodic review by the VSC Cybersecurity Department and/or the VSC IT Department.

The actions taken by the VSC IT Department with assistance from the Cybersecurity Team to ensure these conditions are met are as follows:

- Develop a strategy to work with the Computer Science Department to separate their environment from the main VSC Network
- Encourage use of OneDrive storage for any institutional data
- Assist with evaluation of equipment and its compatibility with current VSC technology
- Establish a review process and rubric to evaluate the Computer Science Department environment and operations each summer prior to a new academic year, with the VSC IT Department, and the Cybersecurity Team

The following parties hereby agree to the terms above

CIO Signature: KCampbell Date: 1/20/23

Computer Science Department Chair Signature: ______________

Date: 1/20/2023

ISO Signature: Tony Date: 1/23/2023

Approved: SEZdatny Date: January 18, 2023

Sophie Zdatny, Chancellor