Title	Policy ID:	
VSC Acceptable Use Policy	**600-1**	
	Version:	Date:
	2.0	**2018/12/04**

1. Purpose

1.1. The purpose of this policy is to define permissible behavior of those Vermont State Colleges ("VSC") faculty, staff, students and others using VSC computing and telecommunications resources ("VSC IT Resources") in order to preserve the confidentiality, integrity, and availability of VSC IT Resources and promote the goals and values of the VSC. These rules are in place to protect the user and the VSC. Inappropriate use exposes the VSC to risks including virus attacks, compromise of network systems and services, and legal issues. The Vermont State Colleges (VSC) owns and maintains computing and telecommunications technologies to support the education, research and daily work of its faculty, staff, and students.

1.2. By connecting thousands of computers at the Vermont State Colleges with each other and with national and international networks, VSC IT Resources provides a wide range of educational benefits. The VSC values freedom of expression, scholarly inquiry, and information sharing, provided they are consistent with VSC policies, state and federal laws, and constitutional provisions. Associated with these values is the personal and professional obligation of each member of our community to use computer and network resources responsibly, ethically, and in accordance with the laws and rights of others. The use of shared resources relies on a spirit of mutual respect and cooperation to create and maintain an open community of responsible users.

2. Scope

2.1. This policy applies to faculty, staff, students, contractors, consultants, temporaries, and other workers at Vermont State Colleges, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Vermont State Colleges, the employee, or a third party, as well as all information, electronic, and computing devices, and network resources used to conduct Vermont State Colleges business or interact with internal networks and business systems. This policy applies to any user of VSC IT Resources. The right to use VSC IT Resources and the Internet is dependent upon compliance with this policy.

2.2. VSC provided equipment, including but not limited to computing equipment, software, operating systems, storage media, network resources, email, web browsing, and FTP, are the property of Vermont State Colleges.

2.3. Nothing herein shall be construed to preclude authorized information technology staff from performing their work including diagnosis, compliance with law, maintenance tasks, and the support of investigations instituted pursuant to the procedures set forth in this Policy. The VSC will seek to maintain system security and privacy, but the VSC IT Resources exists for the furtherance of VSC business and users should not have an expectation that information in user accounts, or on VSC-owned or administered computers, is private.

2.4. All employees, contractors, consultants, temporary, and other workers at Vermont State Colleges and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Vermont State Colleges' policies and standards, and with local laws and regulation.

2.5. Network capacity is finite. Because of this, the VSC retains the right to manage the availability of network resources, in accordance with the following priorities:

HIGHEST: All education, research, and administrative purposes of Vermont State Colleges.
MEDIUM: Other uses indirectly related to Vermont State Colleges' purposes with education or research benefit, including personal communications.
LOWEST: Recreation and entertainment.
NOT PERMITTED: Any use that is a violation of this policy.

3. Policy

3.1. General Use and Ownership

3.1.1. Vermont State Colleges' proprietary information stored on electronic and computing devices, whether owned or leased by Vermont State Colleges, the employee or a third party, remains the sole property of Vermont State Colleges. Users have a responsibility to promptly report the theft, loss, or unauthorized disclosure of VSC proprietary information. Access, use, or sharing of VSC proprietary information is only authorized to the extent necessary to fulfill your assigned job duties.

3.1.2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of computing resources. In the absence of such policies, employees should be guided by departmental policies on personal use, and in the case of uncertainty, employees should consult their supervisor or manager.

3.1.3. For security and network maintenance purposes, authorized individuals within the VSC may monitor equipment, systems and network traffic at any time.

3.1.4. Vermont State Colleges reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2. Security and Proprietary Information

3.2.1. All mobile and computing devices that connect to internal network resources must comply with the 609-1_VSC_Mobile_Devices_Policy.

3.2.2. System level and user level passwords must comply with the 610-2_VSC_Password_and_Access_Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

3.2.3. All VSC-owned computing devices must be secured with a password-protected screensaver. VSC faculty, staff, and lab computers and mobile devices will lock after ten minutes of inactivity. VSC-owned classroom devices used for presentation will lock after no more than 45 minutes of inactivity. Users must lock the screen or log off when the device is unattended.

3.2.4. Postings by employees from a Vermont State Colleges email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Vermont State Colleges, unless posting is in the course of business duties.

3.2.5. Employees receiving unexpected email attachments should verify with the sender before opening to reduce the risk of compromising VSC resources.

3.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of Vermont State Colleges authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Vermont State Colleges-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

3.3.1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Vermont State Colleges.

3.3.2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Vermont State Colleges or the end user does not have an active license is strictly prohibited.

3.3.3. Accessing data, a server, or an account for any purpose other than conducting Vermont State Colleges business, even if you have authorized access.

3.3.4. Unauthorized access to any information or data on VSC IT Resources.

3.3.5. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

3.3.6. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail malware, etc.) or sending unsolicited advertising, to propagate computer worms and viruses or for computer hacking.

3.3.7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home or using a password other than one’s own.

3.3.8. Using a Vermont State Colleges computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction or any other threatening, obscene, harassing and or libelous conduct.

3.3.9. Making fraudulent offers of products, items, or services originating from any Vermont State Colleges account.

3.3.10. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

3.3.11. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized

to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

3.3.12. Port scanning or security scanning is expressly prohibited unless prior notification to the Chief Information Officer is made.

3.3.13. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty. This includes originating or attempting to originate email from someone else.

3.3.14. Circumventing user authentication or security of any host, network or account.

3.3.15. Introducing honeypots, honeynets, or similar technology on the Vermont State Colleges network.

3.3.16. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

3.3.17. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet.

3.3.18. Providing information about, or lists of, Vermont State Colleges' employees to parties outside Vermont State Colleges without VSC consent.

3.3.19. Any illegal purposes under local, state or federal law including copyright violation, libel, criminal threatening, fraud, etc.

3.3.20. Tampering with the physical network (cables, hubs, computers and peripherals etc.).

3.3.21. Logging on or attempting to log on to any piece of VSC computer equipment without an account.

3.3.22. 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.

3.3.23. VSC IT Resources may not be used for profit-making activities.

3.3.24. Selling network access.

3.3.25. Unreasonable or inappropriate use of VSC IT Resources and computing resources for personal business as is using more than a fair share of such resources.

3.3.26. Granting access to VSC IT Resources (for example, computers, services, or data) to persons not associated with the Vermont State Colleges or to persons associated with the Vermont State Colleges who have been denied network access.

3.3.27. The installation and/or removal of any software on a VSC- or college-owned machine without the specific written permission of the Chief Information Officer (CIO) or school Chief Technology Officer (CTO), unless authorized by college policy or procedures.

3.3.28. 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 CIO or a school CTO, unless authorized by college policy or procedure.

3.3.29. Operating a server of any kind on VSC IT Resources without specific written permission of the CIO or school CTO. Operators of approved servers must provide server passwords to the CIO or school CTO upon request.

3.3.30. Registering a domain name associated with the VSC without specific written permission of the CIO.

3.3.31. Other use of VSC IT Resources for purposes inconsistent with the mission of the VSC and the purposes set forth above.

3.4. Email and Communication Activities

When using company resources to access and use the Internet, users represent the VSC. Whenever employees state an affiliation to the VSC, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the VSC". Questions may be addressed to the local IT Department.

Prohibited uses of email include:

3.4.1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

3.4.2. Sending any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3.4.3. Unauthorized use, or forging, of email header information.

3.4.4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

3.5. Social Media

3.5.1. Vermont State Colleges' Confidential Information policy also applies to social media. As such, Employees are prohibited from revealing any VSC confidential or proprietary information, trade secrets or any other material covered by VSC's Confidential Information policy when engaged in social media.

3.6. Authorized Access Without Notice To The User

3.6.1. VSC staff shall have access to a VSC IT Resources user's resources to perform the following tasks without notice to the user:

3.6.2. Diagnosis – tasks necessary to identify or diagnose and correct systems problems.

3.6.3. Maintenance – tasks necessary to the health of VSC IT Resources, including backups, scans, and other essential business functions of the VSC.

3.6.4. Compliance with state or federal law including a lawfully issued subpoena, court order or other compulsory legal process.

3.6.5. To address a health or safety emergency. Suspected violations of any VSC policy discovered during the performance of these tasks will be reported to the Chief Information Officer. All other information accessed during such tasks will be treated as confidential, except as otherwise permitted or required by VSC policy or law.

3.6.6. Only the Chancellor, President, or designee may authorize any other tracking, monitoring, or accessing of VSC IT Resources without notice to the user. Authorization for these activities shall be based on a reasonable belief that one or more of the Rules for the Use of Computing and Telecommunications Technology has been or is being violated, or is necessary to conduct college or system business.

3.7. Policy Compliance Measurement

3.7.1. The VSC will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback.

3.7.2. Any exception to the policy must be approved by the VSC in advance.

3.8. Non-Compliance

3.8.1. Students - Violations of this Policy by students may lead to loss of VSC IT Resources privileges and/or discipline up to and including dismissal.

3.8.2. Employees - Violations of this Policy by employees may lead to loss of VSC IT Resources privileges and/or discipline up to and including termination. Any employee disciplinary action considered in association with this policy shall follow procedures set forth in the relevant employee collective bargaining agreement or, in the case of employees not covered by a collective bargaining agreement, the VSC Personnel Handbook.

3.8.3. Students and employees who engage in activity related to copyright infringement may be liable for civil and/or criminal penalties.

3.8.4. The VSC shall maintain a plan, approved by the Chancellor, to effectively combat the unauthorized distribution of copyrighted material.

3.9. Related Standards, Policies and Processes

3.9.1. 600-1 VSC_Acceptable Use Policy

4. Definitions

4.1. Honeypot - A computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

4.2. Honeynet - Two or more honeypots on a network form a *honeynet.*

4.3. Proprietary Information - Also known as a trade secret, is information a company wishes to keep confidential.

4.4. Spam - Irrelevant or inappropriate messages sent on the Internet to a large number of recipients.

4.5. Network Resources - Shared resources, also known as network resources, refer to computer data, information, or hardware devices that can be easily accessed from a remote computer through a local area network (LAN) or enterprise intranet.

5. Revisions

Date	Revision	Approval	Signature
2018/02/08	Merged with old policy	M. Knapp	
2018/02/02	Formatting Update	Donny Bazluke	
2018/04/03	Edits	G. Malinowski	
2018/12/04	Approval	Kevin Conroy	Kevin Conroy