



Title VSC Policy Mobile Devices	Policy ID:	Page:
	609-1	1 of 3
	Version:	Date:
	1.0	2/13/2018

1. Purpose

1.1. The Vermont State College System (VSCS) values its resources and the security and integrity of its student and employee nonpublic data. Mobile devices are a key resource for the VSCS because they enable communication and connectivity in areas or situations where conventional access to computer networks or telephones is not possible. This policy is intended to enable efficient and secure use of mobile devices and protect VSCS private data and data systems.

2. Scope

- 2.1. This policy applies to all mobile devices that access nonpublic VSCS network resources or synchronize with VSCS nonpublic data, both VSCS-provided mobile devices and personal mobile devices, whether operated by VSCS employees or students. For the purposes of this policy, "mobile device" includes, smartphones, PDAs, tablets and similar devices.
- 2.2. This policy incorporates VSC-Data-Security-Practices_620-1, VSC-Information-Sensitivity-Policy_627-1 and the VSC_Policy_Password_and_Access_Management_610-1. Where the two are inconsistent, it supersedes the VSC-MobileDevice-Best-Practices_631-1.

3. Policy

3.1. PROCUREMENT

3.1.1. VSCS-Issued Mobile Devices

- 3.1.1.1. Employees who are required to have a mobile device as part of their job-related duties should request a VSCS-issued mobile device from their manager.
- 3.1.1.2. Following established procurement procedures, managers can request a VSCS-issued mobile device from the school CTO.
- 3.1.1.3. VSCS will determine the appropriate contract terms for the device, including wireless provider and usage amounts.
- 3.1.1.4. Upon receipt of the device, the user will execute a VSCS-Issued Mobile Device Agreement Form.

3.1.2. Personal Mobile Device

- 3.1.2.1. Any employee who seeks to access nonpublic VSCS data or add a VSCS email account must execute the VSCS Personal Mobile Device Access Form.
- 3.1.2.2. Any employee who receives a stipend or other payment assistance related to their use of a personal mobile device for business use must follow the Data Access Security Policy, the Information Sensitivity Policy and the Password and Access Management Policy.

3.2. TERMS AND CONDITIONS FOR USING MOBILE DEVICES ACCESSING VSC NONPUBLIC INFORMATION OR VSC EMAIL SERVERS

3.2.1. All Mobile Devices

- 3.2.1.1. Password: All mobile devices must be secured using a PIN or other secure password protection meeting the requirements of the Password and Access Management Policy. This PIN or password must be required each time the user accesses the device after a lockout. VSCS staff will not store device PIN information. Forgotten PINs may require a factory reset of the device which may delete all data stored on the device.
- 3.2.1.2. Encryption: All mobile devices accessing nonpublic data must be set to encrypt data stored on the device. Where possible, all data sent from a mobile device to any other device or recipient must be encrypted.
- 3.2.1.3. Device Lockout: All mobile devices must be configured to lock after no more than ten (10) minutes of inactivity. When the device is being used to make a presentation, the lock time should be no longer than 45 minutes of inactivity.
- 3.2.1.4. Data Storage: Consistent with the Data Access Security Policy and the Information Sensitivity Policy, no nonpublic VSCS data should be stored on the storage media of any mobile device.

3.2.2. VSCS-Issued Mobile Devices

- 3.2.2.1. Acceptable Use: All VSCS-issued mobile device users shall comply with the VSC_Policy_Acceptable_Use_600-1.

- 3.2.2.2. Device Security: All VSCS-issued mobile device users must keep their devices in their possession or otherwise take steps to ensure they are secured at all times.
- 3.2.2.3. Remote Disabling: All VSCS-issued mobile devices must permit authorized VSCS personnel to remotely disable any applications and erase all data from the device.
- 3.2.2.4. Unsuccessful Log-in: All VSCS-issued mobile devices must be configured to revert to factory settings and delete all data after ten (10) unsuccessful login attempts.
- 3.2.2.5. Lost/Stolen: If a VSCS-issued mobile device is lost, stolen or otherwise compromised, the User must immediately change their VSC password and then report the situation to Local IT Department. The IT Department will take steps necessary to locate the device and/or erase all data from the device. The User is responsible for reporting the lost/stolen device to their manager or the issuing department.
- 3.2.2.6. Personal Use: Though the primary purpose of VSCS-issued mobile devices is for business use, they may be used for incidental personal, non-business purposes, provided:
 - 3.2.2.6.1. Any personal use of the device cannot interfere with the intended business use of the device;
 - 3.2.2.6.2. Any personal use of the device that incurs usage charges (e.g., data, voice, text), beyond the charges related to the business use of the device are the responsibility of the user, and VSCS may seek reimbursement for such charges;
 - 3.2.2.6.3. The User is responsible for any charges related to non-business use applications or other unauthorized purchases, and VSCS may seek reimbursement for such charges; and
 - 3.2.2.6.4. The device cannot be used for personal financial gain.
- 3.2.2.7. Ownership: All VSCS-issued devices remain the sole property of VSCS. Additionally, VSCS retains exclusive ownership over all data stored on such devices.
- 3.2.3. Replacement: VSCS retains discretion over when and how to replace lost, stolen, otherwise compromised or outdated VSCS-issued devices. Under certain circumstances, the user may be responsible for the cost of replacing the device.
- 3.3. Personal Mobile Devices
 - 3.3.1. Limited Authorization: Unless expressly required to do so by their supervisor, hourly employees are not permitted to access nonpublic VSCS data (including VSCS email) when they are not at work.
 - 3.3.2. Remote Access: All Users of personal mobile devices authorize appropriate VSCS personnel to remotely erase all data on a personal device that accesses VSCS email and/or data, at the User's request.
 - 3.3.3. Lost/Stolen: If a personal mobile device is lost, stolen or otherwise compromised, the User must change their VSC password immediately. It is strongly encouraged that the user report the situation to their local IT Department.

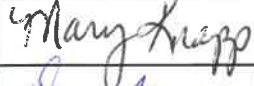
4. References

- 4.1. NIST Special Publication 800-124, "Guidelines for Managing the Security of Mobile Devices in the Enterprise" (June 2013), available at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf>
- 4.2. VSC Computing and Telecommunications Technology Conditions of Use Policy (3/18/10)
- 4.3. Patch Application Policy (1/24/07)
- 4.4. Data Access Security Policy (4/17/12)
- 4.5. Definition of Secure (9/1/06; reviewed 9/5/13)
- 4.6. Data Security Incident Response (11/13/13)
- 4.7. Information Sensitivity Policy (4/17/12)
- 4.8. Password and Access Management Policy (4/17/12)

5. Definitions

- 5.1. VSC – Vermont State Colleges
- 5.2. Business Use: Job-related tasks (including, without limitation, email, any form of mobile messaging, any resources connected to the Internet, video and audio communications) specific to academic instruction, research, business operations, recruiting, public safety or other activities directly related to the function of the VSCS and its member institutions.
- 5.3. Nonpublic data: All VSCS information that is protected from public disclosure by federal or state statute or regulation, including without limitation FERPA, HIPPA, GLBA, or by VSCS Policy, or information that may be excluded from disclosure under the Vermont Public Records Act.

6. Revisions

Date	Revision	Approval	Signature
12/5/2017	First Draft	Todd Daloz	
2/13/18	Formatted and referenced policy numbers added	M. Knapp	
10/29/19	Signed Off	ITC – Gayle Malinowski	
10/29/19	Signed Off	M. Knapp	
10/29/19	Signed Off	D. Bazluke	