VSC INFORMATION TECHNOLOGY SERVICES

VSC Data Access Security Policy

This document is intended to provide employees with information related to safeguarding and working with VSC data and resources. It applies to VSC-owned devices that use secured VSC resources. For additional information on accessing VSC resources on personal devices, please see the VSC Mobile Security Best Practices Guide.

Data practices for desktop and mobile devices that connect to select VSC resources:

- Data defined as "private" by the VSC Information Sensitivity Policy should only be stored in an approved location, defined by that policy. Any data saved to storage other than on a server or IT-administered backup device may be lost.
- To ensure confidentiality, integrity, and availability, all VSC data must be stored in an approved area as per the definition of the data in the VSC Data Sensitivity Policy.
- VSC data, public and private, must be backed-up according to the VSC data center backup practices and/or local college data backup practices.
- 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.
- When not in a locked VSC office, desktop and mobile devices must be either in the physical possession of the authorized user, or physically secured. Regardless of location, when leaving a device unattended, all users will lock device or log out of the device.
- Devices will require a unique username and password for access to data defined as "private" by the VSC Information Security Policy.
- Public computers will have the original image restored daily if used.
- At public computers and lab computers, users of administrative data should adhere to the data practices for remote access (below).
- At lab computers used for training, IT must be consulted in the installation and cleanup of applications and data. Mobile devices must be configured to be as secure as possible if they connect to secure VSC resources, up to and including encryption, passcode, and remote wipe. Please consult the VSC Mobile Security Best Practices Guide.

Additional data practices for remote access:

- Access to private data must be through an approved remote connection. Access to these connections must be approved by the President/Chancellor and the CTO. Access approvals will have an expiration date.
- Private information should never be stored on non-VSC owned device. E-mail is never used to transfer private data for remote work.

Data practices for other VSC-owned removable media:
Removable media include but are not limited to: USB, thumb, or flash drives, and CD-ROM disks.

- Private data will not be stored on removable media.
- In order to further protect VSC-owned removable media, when not in a locked VSC offices, removable media must be either in the physical possession of the authorized user, or physically secured.

Exceptions:

- IT will create and retain back-ups and archives of private data; this data must be physically removed from the premises following the VSC Data Center Disaster Recovery Plan and/or local college data backup practices.
- Grades for courses in progress may be stored by the instructor on a desktop or mobile device, either VSC-owned or personally owned, by the VSC Unique Identifier (Colleague record number) or name but never by Social Security Number or a redaction of the Social Security Number. As soon as practically possible, they should be moved to a secure location, as recommended by IT, and removed from the original desktop or mobile device.

References:
VSC Information Sensitivity Policy
VSC Encryption Policy
VSC Mobile device best practices guide

Definitions:
Public computer: no unique login required; these are generally located in our libraries
Physically secured: user has taken reasonable precautions to safeguard the device, including the use of a locking cable, securing it in a locked room or locked vehicle. Cables will be available to all laptop users.
Approved storage area: network drive, the content collection, enterprise servers.
Approved remote connection: Citrix; Terminal Services through an approved Virtual Private Network (VPN).
Select VSC resources: These resources have potential to provide wide access to storable sensitive data. This includes, but is not limited to Email, Network Drives, and Remote machine connections.
Mobile devices: Included are laptops, PDA's, smart phones, USB flash drives, external hard drives, and any other device that connects to a secured VSC resource.

Approved by/on: Council of Presidents, 01/17/06
Amended: IT Council, March 3, 2011
Reviewed: July 27, 2010