Research Information Security Guideline

Introduction

This document provides general information security guidelines when working with research data. The items in this guideline are divided into two different sections, and depending on the types of data collected or used in the research project, one or both sections of the guideline may apply. School or departmental IT support should be consulted regarding the implementation of these security controls.

Definitions

Administrative Remote Access

Within the context of this document, administrative remote access refers to remote access to an IT system that allows the individual to directly manage the operating system of the IT system. Examples of such access include remote desktop protocol (RDP), Secure Shell Host (SSH), Telnet, and Virtual Network Computing protocol (VNC).

Administrative Rights

Administrative rights refer to the highest level of permission that is granted to a computer user. With administrative rights, a computer user is usually able to modify system configuration, install software and applications, and create or delete user accounts.

Annual Security Awareness Training

Within the context of this document, the annual security awareness training refers to the VCU information Security Awareness Training hosted on Blackboard, this training must be completed by University employees on an annual basis. More information about the training can be found at http://go.vcu.edu/securitytraining.

Authentication

Within the context of this document, authentication refers to the act of confirming the identity of an individual. Authentication of an individual can be accomplished in numerous ways, including the use of user name and password for electronic access, use of access cards or keys for physical access, or a combination of both.

Category I Information

Information protected under federal, state or industry regulations and / or other civil statutes, where if lost may require breach notification and cause potential regulatory sanctions, fines and damages to the institution's mission and reputation. More information on data and information classification can be found in the VCU Data Classification Standard.

Centrally Managed University File Server

Within the context of this document, a centrally managed University file server refers to a computer

server used to store data, in which the computer server is housed in the University Computer Center facilities and managed by professional University server administrators.

Local Computer
The local computer refers to a computer used by a department to conduct its day-to-day business, the local computer is typically located on-site at the department or is mobile. Examples of local computers include departmental desktop and laptop workstations.

Operating System
Operating System is the software that supports a computer's basic functions, such as authentication, executing applications, controlling peripherals, and scheduling tasks. Examples of Operating Systems include: Microsoft Windows, Apple Mac OSX, and Ubuntu Linux.

Patch Management System
Within the context of this document, a patch management system refers to a software application that can be used to detect, report, and deploy software and operating system patches to various computers that report to the system. Examples of patch management system include LANDesk, Kace, SCCM, and WSUS.

Strong Password / Passphrase
A password at least 10 characters long, with at least one upper character, one lower character, one number or one symbol (special character). Preferably, a passphrase that consists of multiple words that are easy to remember should be considered (e.g. I_L0ve_My_K1tten_Cuddl3s)

Strong Encryption Techniques
Strong encryption should utilize a strong password / passphrase and / or other techniques such as two factor authentication as the key to unlock the data, and utilize industry accepted encryption algorithms that are recommended and approved by Federal Information Processing Standard (FIPS). At the time of this writing, AES-128 is the minimum acceptable standard for symmetric encryption, and RSA or DSA / DSAEC should be used for asymmetric encryption. Readers of this guideline should check the latest FIPS encryption recommendations for the approved algorithms or ensure that the storage or transmission medium used is FIPS 140-2 compliant.

Two-Factor Authentication
Two-factor authentication refers to the approach to authentication which requires the presentation of two of the three authentication factors: Something you know (e.g. password), something you are (e.g. Finger print), something you have (e.g. an ID, token or key)

VPN
Within the context of this document, Virtual Private Network (VPN) refers to VCU's VPN installation that allows an individual from outside of the VCU network to access internal VCU network resources following the successful authentication of the individual.

Section I. Basic security guideline for research

The following guideline applies to all research study involving any data, and unless otherwise required by the research, should be followed by all research projects.

- ☐ Ensure all accounts on project computers are password protected with strong passwords, and the protection meets the University password standards (10 characters minimum, complex)
- ☐ Avoid using shared login accounts, and consider using individual login accounts where possible.
- ☐ Enable firewall on the computer and block all unnecessary inbound and outbound communications.
- ☐ Ensure University supplied anti-virus software is installed on all project computers.
- ☐ Ensure Operating Systems and Applications on project computers are patched against known vulnerabilities. Department, school, or University managed centralized patch management system is recommended for this purpose.
- ☐ Avoid making project computers accessible from outside of the University without VPN where possible, to reduce the risk of compromise.
- ☐ Install only necessary software on project computers and avoid installing unneeded software or applications, to reduce the number of potentially vulnerable applications on the computers.
- ☐ Ensure all VCU project personnel have completed their annual security awareness training.
- ☐ Ensure physical data such as printed reports and raw data files are stored in a physically secure environment. (e.g. in locked cabinets, behind locked office doors).
- ☐ Provide access to project data and computer resources on a need-to-know basis, avoid granting excessive access to data.
- ☐ Consider removing administrative rights for project personnel who do not need them, to reduce the risk of virus infections and the installation of unneeded software.
- ☐ Respect software copyrights and ensure that all software and applications used on the project computers are properly licensed for use.
- ☐ Avoid storing sensitive research data on third party or cloud based data storage services such as DropBox, SkyDrive, Amazon, etc. Seek consultation from School IT department or VCU Information Security Office if data must be stored at or transmitted to locations outside of the University environment.

Section II. Security guideline for sensitive research

In addition to the guideline listed above, the following items should be considered and implemented if the research project involves any sensitive or confidential information. Sensitive and confidential information (Category I information) includes the following:

- First Name or First Initial and Last Name in combination with any of the following:
  - Social Security Number
  - Student Grades / Evaluations / Transcripts / Academic Standing / Demographics / Class Schedule
  - Driver's License or State / Federal ID Numbers
  - Credit Card / Debit Card Numbers
  - Medical or Mental History
  - Medical Treatment or Diagnoses information
  - Health Insurance Policy Numbers
  - Other Electronic Protected Health Information as defined by HIPAA
  - Other Regulated / Private / Protected Information
- Private sponsored research information with non-disclosure requirements
- Research information that are regulated by any United States export control laws (Please refer to the Compliance with United States Export Control Laws Policy for definition of export controlled research information)

Additional information security guideline for the handling of sensitive and confidential information includes the following items. Some of the items listed below replace ones stated in the above section:

☐ Any storage of HIPAA regulated (healthcare) and export controlled information outside of the University environment is strictly prohibited due to stringent legal and regulatory requirements.

☐ Project personnel with access to HIPAA regulated data must complete HIPAA privacy training.

☐ Use of shared accounts to access sensitive research data is strictly prohibited due to stringent regulatory and legal requirements. Unique and individual accounts must be assigned and used to access sensitive research data

☐ University supplied Antivirus system or a compensating, but equally effective anti-virus / protection mechanism must be implemented on IT systems used to store, access, or transmit sensitive research data.

☐ Storage and handling of export controlled information must not utilize any technology that is operated by non-U.S. persons or foreign / multi-national corporations. For example, Google Drive or Gmail as well as other cloud based data storage or processing solutions must not be used to handle or store export controlled information.

☐ Remote access to IT systems containing such information from off-campus should always require VPN. Administrative remote access should always require VPN with two-factor authentication.

☐ Ensure all access to project data, whether electronic or physical, regardless of the storage medium used, requires proper authentication. Unauthenticated access to data must not be allowed.

☐ Ensure audit logs are enabled to record authentication attempts into an IT system. Forward audit logs of servers containing sensitive information to VCU Information Security Office for tracking and analysis. (Your server administrator should contact VCU Information Security Office at infosec@vcu.edu for more information)

☐ When possible project data should always be stored on centrally managed university file servers. Storage of project data on local computers should be avoided whenever possible.

☐ Ensure any project data not stored on centrally managed university file servers are encrypted with strong encryption techniques. University supplied system encryption technology should be installed on all local computers used to store project data.

☐ Ensure project data are not stored on non-encrypted removable media (e.g. off-the-shelf USB flash drives). Encrypted USB drives such as IronKeys should be used as the appropriate removable media for project data storage.

☐ Any transmission of project data should employ strong encryption techniques. Project data should not be sent over email in unencrypted form.

☐ Project data should not be uploaded and / or shared using consumer cloud storage services such as DropBox, Google Drive, SkyDrive or other similar services in an unencrypted format.

☐ Consider limiting or removing connection to the Internet and / or network on project computers if Internet / network connection is not needed. Removal of network connection will greatly reduce the risk of data compromise.

☐ Consultation with the department IT support and VCU information security team is strongly recommended for any research projects involving the handling and storage of sensitive information.

Section III. Data Encryption Recommendations

Encryption of project data using strong encryption techniques can prevent unauthorized access to the file or device contents, even when an individual has access to the device or the encrypted file itself. This technique allows the avoidance of data breach notifications if the data file or the device containing the data file is lost or stolen. Properly encrypted data cannot be accessed by any individual without the needed password or key. The encryption of data can be achieved in various ways. The following section demonstrates some methods to encrypt project data.

Encryption with Microsoft Office Products

Microsoft Office 2007 and above can be used to effectively encrypt documents. (Any versions of Microsoft Office prior to 2007 do not offer adequate security to properly encrypt documents, and should not be used) To encrypt a Microsoft Office document (Word, Excel, Access, etc.), simply click on the Office button or the File button, and choose protect document under the Info section, and choose the Encrypt with Password option. (Figure 1), please keep in mind, the password used to encrypt the document should be long and complex.

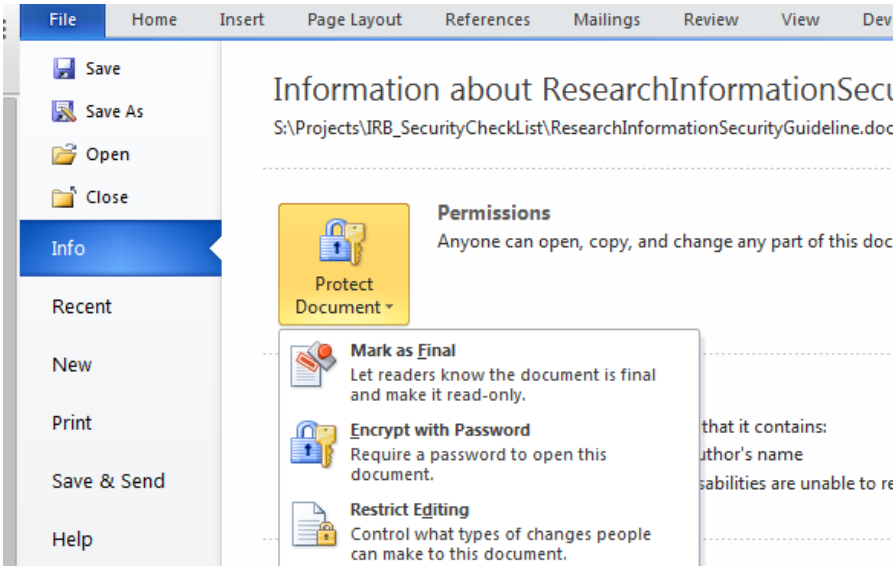


Figure 1. Encryption with Microsoft Office 2010

Encryption with Email

Emails and associated attachments can be encrypted. It is important to ensure that emails containing sensitive information are encrypted before they are sent out. To encrypt an email using the VCU email system, simply type the word "**secure**" in all lower case, minus the quotes in the subject line before sending the email. For example, if a message with the subject of "This is a confidential message" will be sent out, simply enter the subject as "secure This is a confidential message" to encrypt the message.

Figure 2. Encrypting an email message

Encryption of local computer

Computers can be encrypted so that any files stored on them are also encrypted while the files are stored on the computer. The University provides computer encryption software to ensure the encryption of data on computers and the verification of encryption if the device is lost or stolen. Individuals storing sensitive data on local computers, especially portable laptop computers should speak to their IT support group and request the computer encryption software.

Encryption of mobile devices

Mobile devices such as android phones, tablets or iPhones/iPads can also be encrypted if they are used to access sensitive project information.

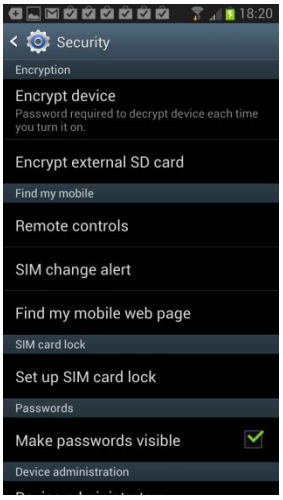
iPhone / iPad Encryption

iPhones and iPads (operating on iOS 3.0 or above) can be easily encrypted by implementing a password or passcode on them. To do so, simply open Settings app, tap General > Passcode lock, and choose to Turn passcode on. For added protection, you can turn off the simple passcode (4 digit pin) and use a password or passphrase to protect the device. The require passcode option should be set to no more than immediately to ensure adequate protection.

In addition to enabling the password, you should also enable the Erase data setting that will lock and erase the content of the device once the wrong password or passcode is entered 10 times.

Android phone / tablet encryption

Similar to iOS devices, Android 3.0 and later devices can also be encrypted; To do so, tap the settings app, and then choose security > Encrypt device (or Encrypt phone).



As additional security measures, similar to iPhones and iPads, Android devices should also be protected with a password or passcode.

Who to Contact with Questions:

For additional information on information security, VCU Information Security Office can be contacted at infosec@vcu.edu. For research and regulatory related questions, Office of research can be contacted at: _____.