Research Security Cookbook

By: Kora Gwartney

UCCS

Office of Sponsored Programs
and Research Integrity

UNIVERSITY OF COLORADO
COLORADO SPRINGS

UCCS

Office of Sponsored Programs and Research Integrity

UNIVERSITY OF COLORADO
COLORADO SPRINGS

Table of Contents

UCCS

Office of Sponsored Programs
and Research Integrity

UNIVERSITY OF COLORADO
COLORADO SPRINGS

Data Security

Definition:

Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It's a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures. https://www.ibm.com/topics/data-security

Best Practices for Data Security and Research:

1. Remain current with Cybersecurity Practices
2. Install Anti-Virus
3. Update and Patch Operating System
4. Data Classification
5. Authentication
6. Data Backup
7. Data Recovery
8. Data Encryption
9. Physical Security
10. Policies and Procedures
11. Least Privilege
12. Separation of Duty

Additional Items:

13. Monitoring
14. Vulnerability Management
15. Risk Management

- https://www.cu.edu/ope/aps/6005
- https://www.ttu.edu/it4faculty/research/
- https://www.umassmed.edu/it/policies-and-guidelines/best-practices/securing-research-data/
- https://ria.princeton.edu/human-research-protection/data/best-practices-for-data-a

Awareness and Training

Definition:

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. **Awareness and training is defined as** "a learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure." https://csrc.nist.gov/glossary/term/awareness

UCCS Trainings:

For UCCS, the awareness and training courses required are presented through Skillsoft and include:

- CU: Controlled Unclassified Information (CUI) ID: _scorm12_cu_u00189_0001
- CU: Information Security and Privacy Awareness ID: _scorm12_cu_u00063_0001
- CU: Introduction to Export Controls ID: _scorm12_cu_u10065_0001
- https://oit.uccs.edu/security/security-program/awareness-and-training
- False Claims Act: https://universityofcolorado.skillport.com/skillportfe/main.action?path=summary/COURSES/lchr_01_d14_lc_enus

Other Skillsoft trainings for security available to staff are:

- Cybersecurity Awareness: Key Security Terms & Concepts ID: it_smbsadj_03_enus

Mitigating Security Risks: Cyber Security Risks ID:

These are some suggestions for potential introductory level security awareness and training courses available through Skillsoft. The key is to have awareness that is tailored and available to all users of a system. Every person who has access to a research system should at minimum have Information Security and Privacy Awareness training to ensure that users of the system can protect against potential infiltrations of the systems.

Anti-Virus/Anti-Malware

Anti-Virus and Anti-Malware Definition:

Anti-Virus is used to protect a computer from viruses. https://www.merriam-webster.com/dictionary/antivirus.

Anti-Malware is a type of software program created to protect information technology (IT) systems and individual computers from malicious software, or malware. https://www.techtarget.com/searchsecurity/definition/antimalware

UCCS Anti-Virus Information:

https://oit.uccs.edu/security/virus-and-malware

What is the difference?

Anti-Virus usually deals with older, more established threats, such as Trojans, viruses, and worms. Anti-Malware, by contrast, typically focuses on newer threats, such as polymorphic malware and malware delivered by zero-day exploits. https://blog.malwarebytes.com/101/2015/09/whats-the-difference-between-antivirus-and-anti-malware/

Which is better?

Both products layered to work together is the best approach to security but having one or the other is better than having neither.

Products:

The following lists provide a starting point to choose a product for Anti-Malware or Anti-Virus solutions. The paid and free products will outline how they work together. There are many types that work with only one operating system, so that should be a consideration when evaluating the products.

Antimalware and Antivirus:

1. UCCS uses Microsoft Defender for Endpoint for managed Windows systems.
2. For MAC OS UCCS uses SOPHOS Endpoint Protection.

Backups

Definition:

A backup is a copy of files and programs made to facilitate recovery, if necessary. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-25.pdf

Backup and Recovery:

Backing up data is only half of the battle. First, the data must be backed up, so it is available for recovery. Then, recovery must be tested. See the Recovery Recipe Card for more details on data recovery. There is not a single set schedule or answer for backing up data. If it is done in a manner that **works for the project**, then it is meeting the goal of being able to recover the data from the back up, if necessary for data loss.

Operating System Guidance for Backing Up Data:

Most operating systems today have a native backup and recovery ability built into them. Here are some references for major operating systems:

1. Windows:
    a. https://support.microsoft.com/en-us/windows/back-up-and-restore-your-pc-ac359b36-7015-4694-de9a-c5eac1ce9d9c
2. RHEL:
    a. https://www.redhat.com/sysadmin/rear-backup-and-recover
3. Ubuntu:
    a. https://help.ubuntu.com/stable/ubuntu-help/backup-how.html.en
4. Macintosh:
    a. https://support.apple.com/en-us/HT201250

Password Manager

What is a Password Manager?

A Password Manager, also known as a Password Safe, allows you to create a secured and encrypted username/password list safely and easily. With a Password Safe, all you must do is create and remember a single "Master Password" of your choice in order to unlock and access your entire username/password list. https://pwsafe.org/

Benefits and Disadvantages of a Password Manager:

Benefits:

1. Manage unique usernames and passwords securely
2. Allows for easy creation of unique, complex passwords
3. Storage of passwords is encrypted
4. Password Managers are recognized as secure by many compliance organizations, including the Department of Defense (DoD)

Disadvantages:

1. If the "Master" password is guessed, found, or cracked, then access to all stored passwords is available.

Some Recommended Password Managers:

1. Biwtarden https://bitwarden.com/ - Used by UCCS OIT and recommended
2. Apple's iCloud Keychain https://support.apple.com/guide/security/keychain-syncing-sec0a319b35f/web
3. KeePass http://keepass.info/
4. LastPass https://lastpass.com/

- https://www.cmu.edu/iso/governance/guidance/password-managers.html

University of Colorado Password Management:

- https://www.cu.edu/passwords
- https://oit.uccs.edu/services/identity-and-access/password

Monitoring

Definition of Monitoring:

Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected. Source(s): NIST SP 800-160 Vol. 1 from ISO Guide 73.

Why Monitor?:

Monitoring information systems provides valuable insight into all aspects of the usage of the information system. This includes who, what, when, where, and occasionally how. Monitoring is a simple way to ensure that the system is running as expected and to know what is going on within the information system (e.g., computers, networks).

Open-Source Tools to Assist with Monitoring:

1. Prometheus: https://prometheus.io/
2. Zabbix: https://www.zabbix.com/
3. Nagios: https://www.nagios.org/
4. Sensu: https://sensu.io/
5. Incinga: https://icinga.com/
6. Cacti: https://www.cacti.net/
7. LibreNMS: https://www.librenms.org/
8. Observium: https://www.observium.org/
9. SPLUNK: https://splunk.com/ - Splunk offers a free limited license for reseachers.

These are just some of the many available tools that could potentially be used to monitor a system. Monitoring is often a cybersecurity regulatory requirement that can be more or less stringent depending on the compliance authority.

Patching and Updating

Definition of Patching:

A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component. Source(s): CNSSI 4009-2015 from ISO/IEC 19770-2

Definition of Update:

New, improved, or fixed software, which replaces older versions of the same software. For example, updating an operating system brings it up to date with the latest drivers, system utilities, and security software. The software publisher often provides updates free of charge. Source(s): NIST SP 1800-15B from Computer Hope

Why updating/patching matters:

Security flaws that are patchable/repairable by updates provided by software companies remain in the top ten causes of data breaches resulting in the loss of data. Generally, security patches for operating systems and additional software are pushed directly to a user's computer, which can be applied to fix known issues that reduce the access a malicious actor would have to a valuable data.

If the fear of an update causing data loss is an issue, most operating systems allow for the creation of a rollback point ensuring that, even if a patch causes problems, it can be returned to a known good state.

UCCS Patching: https://oit.uccs.edu/security/security-standards

Windows Restore Point: https://support.microsoft.com/en-us/windows/create-a-system-restore-point-77e02e2a-3298-c869-9974-ef5658ea3be9

Macintosh Recover Point: https://smallbusiness.chron.com/apple-support-system-restore-previous-time-79881.html

Privacy

Definition of Privacy:

Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. Source(s): NISTIR 8053 from ISO/IEC 2382

Why privacy matters and what to look for:

Privacy has far-reaching extensions into the world of research as many aspects of research rely on individuals. Their information should be processed and handled within the regulations that are required by the country, federal, or state laws that are applicable. Three states in the United States have specific privacy laws, including Colorado. When working with the entirety of the European Union, the GDPR applies to their standards of privacy.

The following are examples of privacy laws that could be applicable to research:

Colorado Privacy Laws:

- https://coag.gov/resources/data-protection-laws/

California Privacy Laws:

- https://www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html
- https://oag.ca.gov/privacy/ccpa

Virginia Privacy Law:

- https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392

General Data Protection Regulation (GDPR):

- https://gdpr-info.eu/

Recovery

Definition:

The goal of the Recover function is to develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. https://csf.tools/reference/nist-cybersecurity-framework/v1-1/rc/
https://www.nist.gov/cyberframework/recover

Discussion on Recover:

Backing up data focuses on having data to recover. Recovery strategies are implemented to plan for the worst. Planning for an event that will cause data loss means having the ability to recover and continue as if the event did not happen. If the event turns into an incident, then operations can continue with backup data. Indicators of how a potential attacker compromised the system can sometimes be found in backed up and recovered data.

The most important part of backing up data is testing that you can recover it.

Operating System Guidance for Recovering Backed Up data:

Most operating systems today have a native backup and recovery ability built into them. Here are some references for major operating systems:

1. UCCS Standard Operating Procedure:
   a. https://kb.uccs.edu/display/KB/Missing+or+Corrupted+File+Recovery
2. Windows:
   a. https://support.microsoft.com/en-us/windows/back-up-and-restore-your-pc-ac359b36-7015-4694-de9a-c5eac1ce9d9c
3. RHEL:
   a. https://www.redhat.com/sysadmin/rear-backup-and-recover
4. Ubuntu:
   a. https://help.ubuntu.com/stable/ubuntu-help/backup-how.html.en
5. Macintosh:
   a. https://support.apple.com/en-us/HT201250

Physical Security

Definition of Physical Security:

These include limiting physical access to information systems, equipment, and any operating environments to authorized individuals. Source(s): NIST SP 800-171rev1

Best Practices for Physical Security:

1. Install access control and surveillance for any space that houses sensitive data, proprietary information, or personally identifiable information (PII), and secure key entry points, such as the front door, to prevent unauthorized individuals from gaining access.
2. Ensure that both internal teams and security system providers adhere to best practices for cybersecurity, including using multi-factor authentication (MFA), least-privilege access models, stringent data storage and retention policies, required security training, active system monitoring and threat detection, and frequent vulnerability testing.
3. Restructure security teams so that physical security and IT leaders work together to ensure the right technology is deployed and that the systems are functioning to maximize security across the entire organization.
4. Establish formal collaboration to give teams a better way to share information from their prospective systems and apply those learnings holistically to improve both cybersecurity and physical security.
5. Leverage data compiled from integrated systems for a more complete picture of security posturing across the entire organization.
6. https://meraki.cisco.com/blog/2021/06/merging-physical-security-and-cybersecurity/

UCCS Physical Security Point of Contact:

The Information Security Office is the main POC for Physical Security Questions please email: security@uccs.edu

Policies and Documentation

Definition of Policy:

A set of criteria for the provision of security services. Source(s): CNSSI 4009-2015 from NIST SP 800-53 Rev. 4

Definition of Documentation:

A cybersecurity document that is related to the Framework. Source(s): NISTIR 8204

Why have policies and documentation:

1. Policies provide clear guidance on what is and is not acceptable for an information system, and how taskings, like incident response or data security, need to be handled for the information system.
2. Documentation provides evidence that what should be done for compliance, regulations, or general best practice is being done.
3. Documentation also helps reduce the pressure of turnover and provides a historical view of how the information system or project has been run in the past.
4. Policy and documentation work together to build a clear picture of how the operation of a project is handled.
    a. https://vcaf.uccs.edu/sites/g/files/kjihxj1631/files/inline-files/2017 NOV 2 100-001Campus%20Policy%20Process-APPROVED.pdf

Risk Management

Definition:

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

Approaches:

There are many types of risk management frameworks that can be used for different types of projects. The important aspects of risk management are to identify and track potential risk to an information system as necessary. The major steps of most of the frameworks are:

1. Categorize Information Systems
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize Information Systems
6. Monitor Security Controls

Example of Security Controls:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

The goal of risk management is to provide a comprehensive understanding of risks to the project, systems, and organizations. Doing so allows a project risk to be identified early and mitigated prior to potential derogation of the system or project.

Vulnerability Management

Definition:

Vulnerabilities [Common Vulnerabilities and Exposures (CVEs)] on devices are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8011-1.pdf

Importance:

Any system that has standard software installed on it is susceptible to being targeted by a malicious actor, someone who could take advantage of a known vulnerability on an information system. Documenting and managing vulnerabilities and remediating vulnerabilities on information technologies reduces the risk to the system of a breach of information.

Tools:

These are paid tools that are good for vulnerability management:

- Qualys Vulnerability Management
- Rapid7 InsightVM / Nexpose
- Tenable.io

https://www.esecurityplanet.com/products/vulnerability-management-software/

Open-Source Vulnerability Management Tools:

- OpenVAS (http://www.openvas.org/)
- OpenSCAP (https://www.open-scap.org)
- Nmap (https://www.nmap.org)
- NESSUS/Tenable Essentials (free version) (https://www.tenable.com/products/nessus)

Encryption

There is a lot of information on encryption and cryptographic techniques and technologies that is not provided in this reference document. The intention of this document is to provide a reference for operating system and file/folder level encryption of data.

Why encrypt?

Encrypting your computer and mobile devices is the best what to protect information on the device, in the event the devices is lost or stolen.

Encryption offers protection by scrambling data, so only the owner of the key or password can read the data. This protects the confidentiality of the data so that if an unauthorized person gained access to the storage device or service, they would be unable to see the data. It also protects the integrity of the data so that it cannot be tampered with without the owner knowing it.

Definition:

Using one or more mathematical approaches to obscure or make data unreadable without the associated key or password is known as **encryption**.

How to Apply:

1. Navigate to:
    a. Full Disk Encryption Recipe Card
    b. File Level Encryption Recipe Card
    c. Mobile Device Encryption Recipe Card

Office of Sponsored Programs
and Research Integrity
UNIVERSITY OF COLORADO
COLORADO SPRINGS

External Storage Encryption

Definition:

External Storage Media includes hard drives, USBs or Cloud Storage, Encrypting an external devices means making it secure by encrypting the data stored on it using sophisticated mathematical functions. This can be done by using software or some other ways.

Operation Systems:

Generally, operating systems offer native encryption here are them most commonly used operating system external storage encryption methods and requirements.

1. Windows
   a. https://docs.microsoft.com/en-us/windows/security/information-protection/encrypted-hard-drive

2. Macintosh
   a. https://support.apple.com/guide/disk-utility/encrypt-protect-a-storage-device-password-dskutl35612/mac

3. Linux
   a. https://opensource.com/article/21/3/encryption-luks
   b. https://help.ubuntu.com/community/EncryptedFilesystemsOnRemovableStorage

Cloud Storage:

Storing data externally on the Cloud is a convenient and common way to store data. The following provides some generally information on common cloud storage platforms.

1. Microsoft OneDrive
   a. https://support.microsoft.com/en-us/office/how-onedrive-safeguards-your-data-in-the-cloud-23c6ea94-3608-48d7-8bf0-80e142edd1e1
2. Apple iCloud
   a. https://support.apple.com/en-us/HT202303
3. Google Cloud/ Google Drive
   a. https://cloud.google.com/storage/docs/encryption
   b. https://support.google.com/docs/answer/10519333?hl=en

UCCS

Office of Sponsored Programs
and Research Integrity

UNIVERSITY OF COLORADO
COLORADO SPRINGS

File and Folder Level Encryption

Definition:

File Level Encryption: form of disk encryption where individual files or directories are encrypted by the file system itself.

Folder Level Encryption: an encryption system where specific folders, files, or volumes are encrypted by a third-party software package or a feature of the file system itself.

Microsoft Windows 10/11:

File Encryption:

1. https://www.itpro.com/security/encryption/359167/how-to-encrypt-files-and-folders-in-windows-10
2. https://support.microsoft.com/en-us/windows/how-to-encrypt-a-file-1131805c-47b8-2e3e-a705-807e13c10da7

Folder Encryption:

1. https://www.itpro.com/security/encryption/359167/how-to-encrypt-files-and-folders-in-windows-10
2. https://support.microsoft.com/en-us/windows/how-to-encrypt-a-file-1131805c-47b8-2e3e-a705-807e13c10da7

Macintosh Operating Systems:

File Encryption:

1. https://www.intego.com/mac-security-blog/how-to-encrypt-and-password-protect-files-on-your-mac/
2. https://www.techradar.com/how-to/how-to-encrypt-files-and-folders-on-your-mac
3. https://www.macupdate.com/how-to/encrypt-files-folders-on-mac

(Cont)

Folder Encryption:

1. https://www.techradar.com/how-to/how-to-encrypt-files-and-folders-on-your-mac

   https://www.macupdate.com/how-to/encrypt-files-folders-on-mac

Red Hat Enterprise Linux (RHEL):

File Encryption:

1. https://www.lifewire.com/encrypt-decrypt-password-protect-files-linux-4582604
2. https://access.redhat.com/solutions/2318
   a. (requires a RHEL account which is simple and easy to setup)
3. https://devconnected.com/how-to-encrypt-file-on-linux/

Folder Encryption:

1. https://www.lifewire.com/encrypt-decrypt-password-protect-files-linux-4582604
2. https://access.redhat.com/articles/4779391
   a. (requires a RHEL account which is simple and easy to setup
3. https://www.baeldung.com/linux/encrypting-decrypting-directory

Ubuntu:

Ubuntu requires an additional tool for file and folder level encryption. Choose whatever tools works best for your use case. Below are a couple of options for file and folder encryption:

File Encryption:

1. https://www.makeuseof.com/tag/encrypt-files-folders-ubuntu/
2. https://www.lifewire.com/encrypt-decrypt-password-protect-files-linux-4582604
3. https://www.fosslinux.com/27018/best-ways-to-encrypt-files-in-linux.htm

Folder Encryption:

1. https://www.makeuseof.com/tag/encrypt-files-folders-ubuntu/
2. https://www.lifewire.com/encrypt-decrypt-password-protect-files-linux-4582604

UCCS

Office of Sponsored Programs
and Research Integrity

UNIVERSITY OF COLORADO
COLORADO SPRINGS

Mobile Device Encryption

Definition:

The process of encoding all data on a mobile device. The following is focused on mobile phones, but the same principles apply to tablets.

IOS:

1. Go to the Settings on your iPhone.
2. Go to Touch ID & Passcode.
3. Select the Turn Passcode On option if it's not already. From there, you will be able to set either a strong six-digit or longer numerical passcode, or alphanumeric password.
4. Set a strong passcode. Entering a code like "123456" will warn you that it's easy to guess.

https://www.zdnet.com/article/how-to-turn-on-iphone-ipad-encryption-in-one-minute/

Android:

1. Plug in the device to charge the battery (required).
2. Make sure a password or PIN is set in Security > Screen lock.
3. Go to Settings > Security.
4. Press the "Encrypt phone" option.
5. Read the notice and press "Encrypt phone" to start the encryption process.
6. Remember to keep the phone plugged in until complete.

https://spreadprivacy.com/how-to-encrypt-devices/

Google:

1. Open your device's Settings app.
2. Tap Security or Security & Location > Screen lock.
3. To choose your screen lock, tap Pattern, PIN, or Password.
4. You'll be asked to "further protect this device" by requiring your PIN, pattern, or password when your device starts. The first time that you choose this setting, it will encrypt your device.
5. Select Require starting device.
6. Tap Continue.
7. Set your PIN, pattern, or password. Follow the on-screen steps.

https://support.google.com/pixelphone/answer/2844831?hl=en#zippy=%2Cencrypt-your-nexus-device-on-android

Windows: https://www.windowscentral.com/how-enable-device-encryption-windows-10-mobile

Full Disk Encryption

******NOTE****** *For Full Disk Encryption, if there is data already on the drive, ensure that the encryption method does not require a clean/empty disk or data could be lost.*

Definition:

Full Disk Encryption: protects the entire volume and all files on the drive against unauthorized access.

Microsoft Windows 10/11:

Microsoft provides a lot of information on their support sites about their operating system, including how to turn on Bitlocker, the FIPS 140-2/3 compliant encryption method:

1. https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838

For any Windows Server Operating Systems, follow this Microsoft support document:

1. https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-deploy-on-windows-server

Macintosh Operating Systems:

Mac's FIPS 140-2/3 compliant application is FileVault 2. FileVault 2 is available in OS X Lion or later. When FileVault is turned on, your Mac always requires that you log in with your account password.
To enable FileVault on your system, follow the following tutorial:

1. https://support.apple.com/en-us/HT204837

Key Management

Definition:

Key management is the management of cryptographic keys in a cryptosystem. https://csrc.nist.gov/glossary/term/key_management

Most cryptographic keys follow a lifecycle which involves key:

1. Generation
2. Distribution
3. Use
4. Storage
5. Rotation
6. Backup/Recovery
7. Revocation
8. Destruction

Best Practices for Regulations and Standards:

1. Avoid hard-coding keys
2. Least privilege
3. Hardware Security Modules
4. Automation
5. Create and Enforce Policies
6. Separate Duties
7. Split Keys

For further information, please view the following:

- https://fortanix.com/blog/2021/05/10-key-management-best-practices-you-should-know/
- https://www.encryptionconsulting.com/education-center/what-is-key-management/

Key Management solutions should be designed for projects as necessary. For further resources, contact OIT or OSPRI representatives to assist with developing a compliant solution for your project.

Linux Operating Systems:

The variety of Linux distributions freely available on the internet are numerous. The following only covers two of the most used operating systems.

Red Hat Enterprise Linux (RHEL):

Luks is a free, FIPS compliant encryption used for Linux distributions. This site provides details about Luks and how to install it on a RHEL operating system:

1. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/encrypting-block-devices-using-luks_security-hardening

Ubuntu:

If it is necessary for the operation of the project, Ubuntu 20.04 LTS, https://ubuntu.com/blog/fips-certification-ubuntu-20-04-lts, is easier to maintain than previous Ubuntu version, for compliance and security requirements. Or an encryption method can be installed on the operating system that is already in use. Directions are found here:

1. https://ubuntu.com/core/docs/uc20/full-disk-encryption

Additional Resources

Resources:

These are additional resources related to Encryption, if you are looking for further information on Data Security please navigate to the section within the cookbook.

1. https://support.apple.com/guide/sccc/security-certifications-apple-t2-chip-sccc225ccbd21/1/web/1.0
2. https://searchsecurity.techtarget.com/feature/Apple-FileVault-2-Full-disk-encryption-software-overview
3. https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/certificates/140crt947.pdf
4. https://guardianproject.info/archive/luks/
5. https://github.com/guardianproject/luks/wiki
6. https://ubuntu.com/security/certifications/docs/fips-faq
7. https://oit.uccs.edu/services/file-transfer-and-storage/lionshare
8. https://oit.uccs.edu/services/file-transfer-and-storage/lionshare

Office of Sponsored Programs
and Research Integrity

UNIVERSITY OF COLORADO
COLORADO SPRINGS

DFARS Use Cases

Applicable DFARS/FARS Clauses:

1. FAR 48 CFR § 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems
2. DFAR 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls
3. DFAR 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

Applicable DFARS Clauses Related to the Cybersecurity Maturity Model Certification (CMMC):

4. DFARS 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements
5. DFARS 252.204-7020 NIST SP 800-171 DoD Assessment Requirements
6. DFARS 252.204-7021 Cybersecurity Maturity Model Certification Requirements

Why these clauses matter:

Federal Acquisition Regulation (FAR) clauses apply to all Federal contracts, and the Defense Federal Acquisition Regulation (DFAR) requires that due care and due diligence are applied to protecting information that is owned by the United States Government.

ANY contract that has these clauses in them have a signed document that states that the user is compliant with the clauses. Compliance is achieved by using the National Institute of Standards and Technologies (NIST) Special Publication 800-171 revision 2 documentation that outline security controls that must be implemented in the attester's information systems. If not, the attester can face administrative or legal actions under the False Claims Act.

The Cybersecurity Maturity Model Certificate (CMMC) adds additional clauses and requirements for the same use cases noted below. Please see the CMMC Recipe Card for specific information.

Contracts/Grants that may require these clauses:

1. Department of Defense (DoD)
2. Small Business Innovation Research (SBIR)
   a. https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course1-Tutorial3.pdf
3. Small Business Technology Transfer (STTR)
4. Federal Government Grants (some)

These clauses typically indicate the research is export controlled. Please contact **Export Controls** via email exportcontrol@uccs.edu if you anticipate these clauses. The export control officer will help develop any required technology control plans.

Access Control

Access Control Definition:

The process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances). Source(s): FIPS 201-3 under Access Control

How to be Compliant:

1. Have an Access Control Policy drafted for the information system. This policy should outline:
   a. How the controls are implemented
   b. Who to contact
   c. Where the policy is stored
   d. Who has access to the information system
2. Implement the Security Control Requirements outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the Access Control Policy
   a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be mapped and used for more detailed information.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pd

(Cont)

Security Control Requirements:

1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
2. Limit system access to the types of transactions and functions that authorized users are permitted to execute.
3. Control the flow of CUI in accordance with approved authorizations.
4. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
5. Employ the principle of least privilege, including for specific security functions and privileged accounts.
6. Use non-privileged accounts or roles when accessing non-security functions.
7. Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
8. Limit unsuccessful logon attempts.
9. Provide privacy and security notices consistent with applicable CUI rules.
10. Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
11. Terminate (automatically) a user session after a defined condition.
12. Monitor and control remote access sessions.
13. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
14. Route remote access via managed access control points.
15. Authorize remote execution of privileged commands and remote access to security-relevant information.
16. Authorize wireless access prior to allowing such connections.
17. Protect wireless access using authentication and encryption.
18. Control connection of mobile devices.
19. Encrypt CUI on mobile devices and mobile computing platforms.
20. Verify and control/limit connections to and use of external systems.
21. Limit use of portable storage devices on external systems.
22. Control CUI posted or processed on publicly accessible systems.

Audit and Accountability

Definition of Auditing:

The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures and to recommend any indicated changes in controls, policy, or procedures. Source(s): NISTIR 7316 under Audit

How to be Compliant:

1. Have an Audit and Accountability Policy drafted for the information system. This policy should outline:
   a. How the controls are implemented
   b. Who to contact
   c. Where the policy is stored
   d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the Audit and Accountability Policy
   a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, it's use case. This link provides the NIST SP 800-171rev2 .pdf document: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be mapped and used for more detailed information. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

(Cont)

Audit and Accountability Security Controls:

1. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
2. Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.
3. Review and update logged events.
4. Alert in the event of an audit logging process failure.
5. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
6. Provide audit record reduction and report generation to support on-demand analysis and reporting.
7. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
8. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
9. Limit management of audit logging functionality to a subset of privileged users.

Awareness and Training

Awareness and Training Definition:

Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance. Source(s): NIST SP 800-50 from NIST SP 800-16

How to be Compliant:

1. Have an Awareness and Training Policy drafted for the information system. This policy should outline:
    a. How the controls are implemented
    b. Who to contact
    c. Where the policy is stored
    d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the Awareness and Training Policy
4. https://www.open-scap.org / is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be mapped and used for more detailed information.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

(Cont)

Awareness and Training Security Controls:

1. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
2. Ensure that personnel are trained to carry out their assigned information security related duties and responsibilities.
3. Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Configuration Management

Definition of Configuration Management:

A collection of activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. Source(s): NIST SP 800-172, NIST SP 800-172A

How to be Compliant:

1. Have a Configuration Management Policy drafted for the information system. This policy should outline:
   a. How the controls are implemented
   b. Who to contact
   c. Where the policy is stored
   d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the Configuration Management Policy
   a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be mapped and used for more detailed information. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

(Cont)

Configuration Management Security Controls:

1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
2. Establish and enforce security configuration settings for information technology products employed in organizational systems.
3. Track, review, approve or disapprove, and log changes to organizational systems.
4. Analyze the security impact of changes prior to implementation.
5. Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
6. Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.
7. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
8. Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
9. Control and monitor user-installed software.

Identification and Authentication

Definition of Identification:

The process of discovering the identity (i.e., origin or initial history) of a person or item from the entire collection of similar persons or items. Source(s): FIPS 201-3 under Identification

Definition of Authentication:

Security measures designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. Source(s): NIST SP 800-59 under Authentication from CNSSI 4009

How to be Compliant:

1. Have an Identification and Authentication Policy drafted for the information system. This policy should outline:
    a. How the controls are implemented
    b. Who to contact
    c. Where the policy is stored
    d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the Identification and Authentication Policy
    a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

(Cont)

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be mapped and used for more detailed information.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Identification and Authentication Security Controls:

1. Identify system users, processes acting on behalf of users, and devices.
2. Authenticate (or verify) the identities of users, processes, or devices as a prerequisite to allowing access to organizational systems.
3. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
4. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
5. Prevent reuse of identifiers for a defined period.
6. Disable identifiers after a defined period of inactivity.
7. Enforce a minimum password complexity and change of characters when new passwords are created.
8. Prohibit password reuse for a specified number of generations.
9. Allow the use of temporary password for system logons with an immediate change to a permanent password.
10. Store and transmit only cryptographically protected passwords.
11. Obscure feedback of authentication information.

Incident Response

Definition of Incident Response:

The mitigation of violations of security policies and recommended practices. Source(s): CNSSI 4009-2015 from NIST SP 800-61 Rev. 2; NIST SP 800-61 Rev. 2 under Incident Handling

How to be Compliant:

1. Have an Incident Response and Handling Policy drafted for the information system. This policy should outline:
   a. How the controls are implemented
   b. Who to contact
   c. Where the policy is stored
   d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the Incident Response Policy
   a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be mapped and used for more detailed information. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

(Cont)

Incident Response Security Controls:

1. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
2. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
3. Test the organizational incident response capability.

Maintenance

Definition of Maintenance:

Aspect of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity. Source(s): NIST SP 800-171rev2

How to be Compliant:

1. Have a Maintenance Policy drafted for the information system. This policy should outline:
   a. How the controls are implemented
   b. Who to contact
   c. Where the policy is stored
   d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the Maintenance Policy
   a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be mapped and used for more detailed information. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

(Cont)

Maintenance Security Controls:

1. Perform maintenance on organizational systems.
2. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
3. Ensure equipment removed for off-site maintenance is sanitized of any CUI.
4. Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
5. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
6. Supervise the maintenance activities of maintenance personnel without required access authorization.

Media Protection

Definition of Media Protection:

System media include digital and non-digital media. Digital media include diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media include paper and microfilm. Source(s): NIST SP 800-171rev2

How to be Compliant:

1. Have a Media Protection Policy drafted for the information system. This policy should outline:
   a. How the controls are implemented
   b. Who to contact
   c. Where the policy is stored
   d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the Media Protection Policy
   a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be mapped and used for more detailed information. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

(Cont)

Media Protection Security Controls:

1. Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
2. Limit access to CUI on system media to authorized users.
3. Sanitize or destroy system media containing CUI before disposal or release for reuse.
4. Mark media with necessary CUI markings and distribution limitations.
5. Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
6. Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
7. Control the use of removable media on system components.
8. Prohibit the use of portable storage devices when such devices have no identifiable owner.
9. Protect the confidentiality of backup CUI at storage locations.

Personnel Security

Definition of Personnel Security:

The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities that require trustworthiness. Source(s): NIST SP 800-53 Rev. 5

How to be Compliant:

1. Have a Personnel Security Policy drafted for the information system. This policy should outline:
   a. How the controls are implemented
   b. Who to contact
   c. Where the policy is stored
   d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the Personel Security Policy
   a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be mapped and used for more detailed information. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

(Cont)

Personnel Security, Security Controls:

1. Screen individuals prior to authorizing access to organizational systems containing CUI.
2. Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Physical Security

Physical Security Definition:

Limiting physical access to equipment may include placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only; and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment. Source(s): NIST SP 800-171rev2

How to be Compliant:

1. Have a Physical Security Policy drafted for the information system. This policy should outline:
   a. How the controls are implemented
   b. Who to contact
   c. Where the policy is stored
   d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the Physical Security Policy
   a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be mapped and used for more detailed information. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

(Cont)

Physical Security, Security Controls:

1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
2. Protect and monitor the physical facility and support infrastructure for organizational systems.
3. Escort visitors and monitor visitor activity.
4. Maintain audit logs of physical access.
5. Control and manage physical access devices.
6. Enforce safeguarding measures for CUI at alternate work sites.

Risk Assessment

Risk Assessment Definition:

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. Source(s): NIST SP 1800-21B under Risk Assessment from NIST SP 800-53 Rev. 4; NIST SP 800-137 under Risk Assessment from CNSSI 4009

How to be Compliant:

1. Have a Risk Assessment Policy drafted for the information system. This policy should outline:
   a. How the controls are implemented
   b. Who to contact
   c. Where the policy is stored
   d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the Risk Assessment Policy
   a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be used for detailed information. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

(Cont)

Risk Assessment Security Controls:

1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of Controlled Unclassified Information (CUI).
2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
3. Remediate vulnerabilities in accordance with risk assessments.

Security Assessment

Security Assessment Definition:

The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Source(s): CNSSI 4009-2015 under security control assessment from NIST SP 800-37 Rev. 1

How to be Compliant:

1. Have a Security Assessment Policy drafted for the information system. This policy should outline:
   a. How the controls are implemented
   b. Who to contact
   c. Where the policy is stored
   d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the Security Assessment Policy
   a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls
   b. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be mapped and used for more detailed information.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-

(Cont)

Security Assessment Security Controls:

1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
4. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

System and Communication

System and Communication Definition:

Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Source(s): NIST SP 800-171rev2

How to be Compliant:

1. Have a System and Communication Policy drafted for the information system. This policy should outline:
   a. How the controls are implemented
   b. Who to contact
   c. Where the policy is stored
   d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the System and Communication Policy
   a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls
   b. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP

(Cont)

System and Communication Security Controls:

1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
3. Separate user functionality from system management functionality.
4. Prevent unauthorized and unintended information transfer via shared system resources.
5. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
6. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
7. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
8. Implement cryptographic mechanisms to prevent unauthorized disclosure of Controlled Unclassified Information (CUI) during transmission unless otherwise protected by alternative physical safeguards.
9. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
10. Establish and manage cryptographic keys for cryptography employed in organizational systems.
11. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
12. Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
13. Control and monitor the use of mobile code.
14. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
15. Protect the authenticity of communications sessions.
16. Protect the confidentiality of CUI at rest.

System and Information Integrity

System and Information Integrity Definition:

Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Source(s):NIST SP 800-171rev2

How to be Compliant:

1. Have a System and Information Integrity Policy drafted for the information system. This policy should outline:
   a. How the controls are implemented
   b. Who to contact
   c. Where the policy is stored
   d. Who has access to the information system
2. Implement the Security Controls outlined in the following section
3. Test to ensure the security controls are implemented on the information system and document the results in the System and Information Integrity Policy
   a. https://www.open-scap.org/ is a free tool that can automate part of the testing requirements for these controls

The National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171rev2 provides general guidance for how to complete each control. The security controls should be tailored to the information system, its use case. This link provides the NIST SP 800-171rev2 .pdf document: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

For more granularity or additional control information, the NIST SP 800-53rev5 Security Controls can be mapped and used for more detailed information. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

(Cont)

System and Information Integrity Security Controls:

1. Identify, report, and correct system flaws in a timely manner.
2. Provide protection from malicious code at designated locations within organizational systems.
3. Monitor system security alerts and advisories and take action in response.
4. Update malicious code protection mechanisms when new releases are available.
5. Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
6. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
7. Identify unauthorized use of organizational systems.

UCCS

Office of Sponsored Programs
and Research Integrity

UNIVERSITY OF COLORADO
COLORADO SPRINGS

HIPAA For Researchers

Points of Contact:

- Associate Director OPSRI - Sponsored Research
    - Mike Sanderson
        - msander3@uccs.edu
- Director of Campus Compliance
    - Debi O’Connor
        - doconnor@uccs.edu
- Information Security Officer
    - Neil Kautzner
        - nkautzne@uccs.edu

When does HIPAA apply to my research?

- The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
    - an adequate plan to protect the identifiers from improper use and disclosure;
    - an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
    - adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.
- The research could not practicably be conducted without the waiver or alteration; and
- The research could not practicably be conducted without access to and use of the protected health information.

https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html

(Cont)

What Resources are available to me as a Researcher to compile with HIPAA?

- OIT uses OneDrive for HIPAA regulated data storage
- https://compliance.uccs.edu/news/health-insurance-portability-and-accountability-act-1996-hipaa

A violation of the HIPAA law can be intentional or unintentional and, under the Omnibus Rule, fines are issued accordingly based on the violation. Violations are tiered:

1. Tier 1: A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules.
2. Tier 2: A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care (but falling short of willful neglect of HIPAA Rules).
3. Tier 3: A violation suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation.
4. Tier 4: A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation.

UCCS

Office of Sponsored Programs
and Research Integrity

UNIVERSITY OF COLORADO
COLORADO SPRINGS

Protect Health Information (PHI) and Electronic Protect Health Information (ePHI)

Points of Contact:

- Associate Director OSPRI
    - Mike Sanderson
        - msander3@uccs.edu
- Director of Campus Compliance
    - Debi O'Connor
        - doconnor@uccs.edu
- Information Security Officer
    - Neil Kautzner
        - nkautzne@uccs.edu

How does it affect me, as a researcher?

As an individual, you would not want someone to misuse your private health information. So, as a researcher, it is ethical to maintain the privacy and security of others' information. HIPAA violations can result in legal actions and hefty fines.

What are some steps I can take to Protect PHI?

- Ensure that email and locally and remotely stored data are encrypted when they contain PHI and ePHI.
- Follow HIPAA guidelines to ensure that PHI/ePHI is properly protected.
- https://compliance.uccs.edu/news/health-insurance-portability-and-accountability-act-1996-hipaa

(Cont)

Protected Health Information, or PHI, is any personal health information that can potentially identify an individual, that was created, used, or disclosed while providing healthcare services, whether it was a diagnosis or treatment. Electronic Protected Health Information (ePHI) is any PHI found in electronic format on a computer or mobile device.

1. PHI can include:
   a. The past, present, or future physical health or condition of an individual
   b. Healthcare services rendered to an individual.
   c. Past, present, or future payment for the healthcare services rendered to an individual, along with any of the identifiers.