United States Department of Health & Human Services

Office of the Chief Information Officer

HHS POLICY FOR RULES OF BEHAVIOR FOR USE OF INFORMATION AND IT RESOURCES

Document #: HHS-OCIO-OIS-2019-05-004

Version #: 2.2

Status: Approved

Last Reviewed: June 7, 2019

Next Review: June 7, 2022

Owner: OCIO/OIS

Approved By: Jose Arrieta, Chief Information Officer

TABLE OF CONTENTS

1. Nature of Changes

Version 1.0: released on July 2013. First Issuance of policy.

Version 2.0: released on December 2016. Added new statements to:

- Prohibit the use of personally owned devices and unapproved non-GFE to conduct HHS business;
- Restrict personal social media use during official work duty;
- Restrict the connection to public, unsecure Wi-Fi from GFE; and
- Prohibit the use of HHS e-mail address to create personal commercial accounts.

Version 2.1: released on August 2017. As recommended by OpDivs in the first-round review, Policy for Personal Use of IT Resources was combined with the Rules of Behavior, since the documents overlapped.

Version 2.1: released on February 2018. Update to policy for use of personal email as recommended by Department.

Version 2.1: released on March 2018. Removed the policy requirement restricting the use of personal email from HHS networks as requested by OCIO.

Version 2.1: released on April 2018. Replaced Controlled Unclassified Information (CUI) with “sensitive information” per OGC and PIM recommendation.

Version 2.1: released on June 2018. Policy obtained NTEU clearance.

Version 2.2: released on May 2019. Changed Webmail access policy to block only access from public Internet and encourage OpDivs to reduce its use. Added requirement to restrict the use of personal email, storage services and devices to conduct HHS business and store HHS data.

2. Purpose

The purpose of this HHS policy is to define the acceptable use of HHS/Operating Divisions (OpDivs) information and Information Technology (IT) resources and establish the baseline requirements for implementing the HHS Rules of Behavior (RoB) that govern the appropriate use of HHS/OpDiv information systems and resources for all employees, contractors, and other personnel who have access to HHS information and information systems. RoB regarding access to and use of HHS information and IT resources are an important part of the HHS Information Security Program.

This document includes baseline requirements for three RoB categories: General Users, Privileged Users, and System Specific. These RoB categories provide requirements and guidelines for implementation of each RoB category. This policy also includes acceptable personal use of HHS/OpDiv information resources and use of personal devices to conduct HHS business.

OpDivs may customize this policy and RoB to include OpDiv specific information, create their own policy, or supplement the specified RoB, provided the OpDiv policy and RoB are compliant with and at least as restrictive as the baseline policy and RoB stated herein.

This Policy uses the term sensitive information to refer to Personally Identifiable Information (PII), Protected Health Information (PHI), financial records, proprietary data, and any information marked Sensitive but Unclassified (SBU), Controlled Unclassified Information (CUI), etc.[1]

3. Background

The executive branch of the federal government serves the American people through hundreds of thousands of employees located in offices across the nation. Increasingly, the government is called upon to deliver more and better services to a growing population that continues to expect ever-increasing improvements in service delivery. The relationship between the executive branch and the employees who administer the functions of the government is one based on trust. Consequently, employees are expected to follow rules and regulations and to be responsible for their own personal and professional conduct. The Standards of Ethical Conduct for Employees of the Executive Branch published by the U.S. Office of Government Ethics states that, "Employees shall put forth honest effort in the performance of their duties" [Section 2635.101 (b) (5)].

The HHS Rules of Behavior for Use of HHS Information and IT Resources includes the policy and the rules that govern the appropriate use and protection of all Department of Health and Human Services (HHS or Department) information resources and help to ensure the security of information technology (IT) equipment, systems, and data as well as their confidentiality, integrity and availability. This policy applies to all HHS personnel, contractors, and other information system users and is issued under the authority of the HHS Information Security and Privacy Policy (IS2P).

4. Scope

This policy and RoB rescind and replace the *HHS-OCIO Policy for Personal Use of Information Technology Resources*, dated August 1, 2013 and *Rules of Behavior for Use of HHS Information Technology Resources*, dated July 24, 2013. This Policy does not supersede any other applicable law or higher-level agency directive, or existing labor management agreement in effect as of the effective date of this Policy.

This HHS policy and RoB shall apply to all users of HHS/OpDiv information and IT resources whether working at their primary duty station, while teleworking, at a satellite site or any other alternative workplaces, and while traveling.

5. Authorities

The following are the primary authoritative documents driving the requirements in this policy:

- Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, 128 Stat. 3073, codified at 44 U.S.C. Chapter 35, Subchapter II.

[1] CUI is defined in Executive Order (EO for official use only (FOUO)) 13556, *Controlled Unclassified Information (CUI)*, and the HHS *Controlled Unclassified Information Policy*, forthcoming. There are numerous categories and subcategories of CUI listed in the National Archives and Records Administration (NARA) CUI Registry. Examples of CUI categories include *Privacy*, *Procurement and Acquisition*, *Proprietary Business Information*, and *Information Systems Vulnerability Information*

- 5 U.S.C. Section 552a (the Privacy Act.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems,* February 2010.
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013.
- Office of Management and Budget (OMB), Circular A-130, *Managing Information as a Strategic Resource,* July 2016.
- HHS Information Security and Privacy Policy (IS2P) - 2014 Edition.
- HHS Memorandum for the Usage of Unauthorized External Information Systems to Conduct Department Business, January 8, 2014.

6. Policy

The following are the baseline requirements for implementing the HHS RoB that govern the appropriate use of HHS/OpDiv information systems and resources for all employees, contractors, and other personnel who have access to HHS information and information systems.

6.1. Acceptable Use of HHS Information and IT Resources – User Requirements

A. HHS permits personnel to have limited personal use of HHS/OpDiv information and IT resources, including HHS/OpDiv e-mail, systems, instant messaging (IM) tools, and government-furnished equipment (GFE) (e.g. laptops, mobile devices, etc.) only when the personal use shall:

1. Involve no more than minimal additional expense to the government;
2. Be minimally disruptive to personnel productivity;
3. Not interfere with the mission or operations of HHS; and
4. Not violate HHS/OpDiv security and privacy policies.

B. HHS expects personnel to conduct themselves professionally in the workplace and to refrain from using GFE, email, third-party websites and applications (TPWAs) (e.g., HHS social media sites and cloud services, etc.) and other HHS information resources for activities that are not related to any legitimate/officially-sanctioned HHS business purpose, except for the limited personal use stated above. Personnel shall not misuse HHS/OpDiv information and IT resources or conduct unapproved activities using HHS/OpDiv information and IT resources including, but not limited to:

1. Engaging in activities that could cause congestion, delay, or disruption of service to any HHS information resource (e.g., sending chain letters via email, playing streaming videos, games, music, etc.);
2. Accessing, downloading and/or uploading illegal or criminal content from/to the Internet (e.g., pornographic and sexually explicit materials, illegal weapons, terrorism activities, and other illegal activities);

3. Conducting or supporting commercial "for-profit" activities, managing outside employment or business activity, or running personal business;
4. Engaging in any outside fund-raising, endorsing any product or service, lobbying, or engaging in partisan political activity;
5. Using HHS/OpDiv information resources for activities that are inappropriate or offensive to fellow personnel or the public (e.g., hate speech or material that ridicules others on the basis of race, creed, religion, color, age, gender, disability, national origin, or sexual orientation);
6. Creating a website, TPWA, or social media site on behalf of HHS or uploading content to a website, TPWA, or social media site without proper official authorization;[2]
7. Using personal devices and unauthorized third-party systems, storage services, or applications (e.g., Dropbox, GoogleDocs, mobile applications, etc.) to store, transmit, process HHS information, and conduct HHS business without proper official authorization;
8. Automatically (auto) forwarding HHS/OpDiv email to both internal and external email sources or forwarding email/files that contain sensitive information to unauthorized systems and devices that are used for non-HHS and non-OpDiv business purposes;
9. Accessing and using HHS/OpDiv Webmail without proper official authorization;
10. Connecting personal devices to HHS systems without proper official authorization; and
11. Using an HHS/OpDiv email address and other information resources to create personal commercial accounts for the purpose of receiving notifications (e.g., sales discounts, marketing, etc.), setting up a personal business or Website, and signing up for personal memberships that are not work related.

C. Users of HHS/OpDiv information resources, systems and GFE shall have no expectation of privacy and may be monitored, recorded, and audited, in accordance with the HHS memorandum Policy for Monitoring of Employee Use of HHS IT Resources, dated June 26, 2013, and OpDivs' monitoring policies.[3] Any HHS/OpDiv information resources, systems and GFE shall be used with the understanding that such use may not be secure, is not private, is not anonymous, and may be subject to disclosure under the Freedom of Information Act (FOIA), 5 U.S.C. § 552 or other applicable legal authority.

---

[2] All third-party web applications, social media sites, storage and cloud services must be authorized prior to use and/or deployed into production by obtaining an authorization to operate (ATO) or included under an existing system's ATO boundary in accordance with the IS2P. If an ATO cannot be obtained or the service/application cannot be included under an existing ATO, a Waiver must be documented and approved by the OpDiv Chief Information Officer (CIO). In addition, only authorized personnel must post only authorized content on public- facing websites and social media sites.

[3] And Article 35, Section 4 of the Master Labor Agreement (MLA) between the Centers for Medicare & Medicaid Services (CMS or Agency) and the American Federation of Government Employees, Local 1923 (AFGE)

D. Users shall be formally notified that their electronic data communications and online activity may be monitored and disclosed to external law enforcement agencies or Department/OpDiv personnel when related to the performance of their duties in accordance with the HHS memorandum Policy for Monitoring of Employee Use of HHS IT Resources, dated June 26, 2013, and OpDivs' monitoring policies. For example, after obtaining management approval, HHS authorized technical staff may employ monitoring tools in order to maximize the utilization of HHS resources.

E. Users shall not use personal email, storage/service accounts or personal devices to conduct HHS business or store/transmit HHS data without official written approval.

6.2. Acceptable Use of HHS Information and IT Resources – OpDiv Requirements

A. OpDivs shall take steps to reduce the use of Webmail and allow access only when necessary.

B. OpDivs shall ensure all users read and acknowledge the RoB for General User and users with significant security responsibilities read and acknowledge the RoB for privileged users at onboarding and annually thereafter (see baseline RoB for both general and privileged users in Appendix D.)

C. OpDivs shall develop and implement system specific RoB (see additional guidance in Appendix C.)

D. OpDivs shall implement technical controls to:

1. Prohibit auto-forwarding of email;
2. Block the use of HHS/OpDiv Webmail access from the public Internet;
3. Appropriately secure mobile devices used for conducting HHS business;
4. Monitor user activities and privileged user accounts; and
5. Disable unnecessary/unauthorized permissions, services, and system/user accounts.

6.3. Non-Compliance

This HHS RoB for Use of HHS Information IT Resources Policy cannot account for every possible situation. Therefore, where this policy does not provide explicit guidance, personnel shall use their best judgment to apply the principles set forth in the standards for ethical conduct to guide their actions and seek guidance when appropriate from the OpDiv Chief Information Officer (CIO) or his/her designee.

Non-compliance with this policy and RoB specified herein may be cause for disciplinary and non-disciplinary actions. Depending on the severity of the violation and management discretion, consequences may include one or more of the following actions:

1. Suspension of access privileges;
2. Revocation of access to federal information, information systems, and/or facilities;
3. Reprimand;
4. Termination of employment;

5. Suspension without pay;
6. Removal or disbarment from work on federal contracts or projects;
7. Monetary fines; and/or
8. Criminal charges that may result in imprisonment.

7. Roles and Responsibilities

7.1 HHS Chief Information Officer (CIO)

The HHS CIO or representative shall:

A. Ensure that the HHS RoB for Use of HHS Information and IT Resources Policy is disseminated and implemented Department-wide; and

B. Ensure RoB are developed, maintained, and implemented for all information system users, privileged users, and information systems (when deemed applicable) Department- wide role.

7.2 OpDiv CIO

The OpDiv CIO or representative shall:

A. Ensure that an acceptable use of HHS information resources policy is implemented throughout the OpDiv;

B. Ensure RoB are developed, approved, maintained, and implemented for all information system users, privileged users, and information systems (when deemed applicable) OpDiv-wide; and

C. Assign or appoint a designee to approve all exceptions to RoBs.

7.3 OpDiv Chief Information Security Officer (CISO)

The OpDiv CISO shall:

A. Implement HHS RoB policy or develop OpDiv RoB for use of HHS information resources policy;

B. Develop and implement OpDiv RoB for general and privileged users;

C. Ensure system specific RoB are developed and implemented when deemed applicable;

D. Ensure all users read, acknowledge and adhere to RoB for all three RoB categories (general users, privileged users, and system specific users) as applicable; and

E. Ensure records are maintained for signed RoB forms.

7.4 Managers and Supervisors

The OpDiv Managers and Supervisors shall:

A. Inform users of their rights and responsibilities, including the dissemination of the information in this policy to individual users;

B. Address inappropriate use by personnel who report to them and disseminate

information to relevant stakeholders for the purpose of incident handling and investigations;

C. Receive and review reports of inappropriate use of IT resource from management officials and allow access to these reports to designated authorities, as applicable, in accordance with HHS standard operating procedures; and

D. Notify, when appropriate, senior Department officials of inappropriate use and/or abuse of HHS IT resources.

7.5 System Owner (SO)

The OpDiv SOs shall:

A. Develop and appropriately disseminate system specific RoB when deemed applicable;

B. Ensure all users with access to the information system(s) under their purview read, acknowledge and adhere to the General User RoB and system specific RoB (if deemed applicable) prior to obtaining access and at least annually thereafter;

C. Automate, to the extent possible, the security and privacy controls that are required to be implemented to protect systems and information;

D. Ensure all users with privileged access rights to the information system(s) under their purview read, acknowledge and adhere to the Privileged User RoB;

E. Review system specific RoB periodically and at least every three years;

F. Maintain records of all the signed system specific RoB;

G. In accordance with the Privacy Act, maintain an accounting of disclosures made by HHS of records about individuals to persons, organizations, and other agencies; and

H. Not maintain records about individuals longer than needed for HHS business without scheduling them with the National Archives and Records Administration (NARA).

7.6 Information and System Users

All users of HHS information, GFE and systems shall:

A. Always secure HHS information resources and assets they have access to or entrusted with at all times (e.g., while at their duty station, when traveling, teleworking, etc.);

B. Report any loss, compromise, and unauthorized use of HHS information and systems immediately upon discovery/detection in accordance with HHS/OpDiv policies; and

C. Seek guidance from their supervisor and other officials if unclear about HHS/OpDiv security and privacy policies.

8. Information and Assistance

HHS Office of the Chief Information Officer, Office of Information Security is responsible for the development and management of this policy. Questions, comments, suggestions,

and requests for information about this policy should be directed to HHS.Cybersecurity@hhs.gov.

9. Effective Date and Implementation

The effective date of this policy is the date on which the policy is approved. This policy must be reviewed, at a minimum, every three (3) years from the approval date. The HHS CIO has the authority to grant a one (1) year extension of the policy. To archive this policy, approval must be granted, in writing, by the HHS CIO.

OpDivs shall implement this policy and the standard RoB within **one hundred eighty days (180) days** from the issuance date.

10. Approval

/S/

Jose Arrieta, Deputy Assistant Secretary for Information Technology and Chief Information Officer (CIO)

6/4/2019

11. Concurrence

/S/

Scott Rowell, Assistant Secretary for Administration (ASA) 6/7/2019

Appendix A: Procedures

Please note that this appendix is subject to change at any time. The current version of this policy will always reside in the OCIO Policy Library.

OpDivs may develop their specific procedures document(s) to implement this policy.

Appendix B: Standards

Please note that this appendix is subject to change at any time. The current version of this policy will always reside in the OCIO Policy Library.

Standard Rules of Behavior

OpDivs are responsible for implementing adequate security controls to ensure a high level of protection for all HHS information and information systems commensurate with the level of risk. In addition, they shall ensure that all employees, contractors, and other personnel using HHS information resources, have the required knowledge and skills to appropriately use and protect HHS information and information systems. All OpDivs may use the RoB included in Appendix D or they may develop their own RoB provided they are, at a minimum, compliant with the HHS RoB.

A. RoB are provided for the following three categories:

   1. Appendix C includes supplemental RoB for specific systems; and
   2. Appendix D contains the RoB for general users and the RoB for privileged users.

B. The RoB shall inform users of their responsibilities and let them know that they will be held accountable for their actions while they are accessing HHS/OpDiv systems and using HHS/OpDiv information resources.

C. All HHS employees, contractors, and other personnel with access to HHS information and information systems shall read, acknowledge, and adhere to the HHS/OpDiv General User RoB prior to accessing and using HHS information resources and IT systems. The acknowledgment of the RoB, which affirms that all users have read and understand the HHS/OpDiv RoB, may be obtained by either hardcopy written signature, or by electronic acknowledgement or signature. This acknowledgement shall be completed at HHS/OpDiv onboarding or prior to start of work on an HHS contract, grant, or other agreement, and at least annually thereafter, and/or in combination with the HHS information cybersecurity awareness training.

D. All privileged users (e.g., network/system administrators, developers, etc.) shall read, acknowledge and adhere to the HHS/OpDiv Privileged User RoB prior to obtaining a privileged user account and at least annually thereafter. The acknowledgment of the RoB, which affirms that privileged users have read and understand the HHS/OpDiv RoB for Privileged Users, may be obtained by either hardcopy written signature or by electronic acknowledgement or signature.

E. Per the HHS IS2P, OpDivs shall develop and implement system specific RoB, when deemed advisable, to address system specific requirements to protect the system and information.

F. All RoB (General, Privileged, and System Specific) shall be reviewed and if necessary updated, at least every three years.

G. Any exceptions to this policy and specified RoB shall be approved by the OpDiv Authorizing Official or designee.

Appendix C: Guidance

Please note that this appendix is subject to change at any time. The current version of this policy will always reside in the OCIO Policy Library.

Supplemental Rules of Behavior for HHS Systems

Operating Divisions (OpDivs) are responsible for developing system-specific Rules of Behavior (RoB) and for ensuring that users read, acknowledge, and adhere to them. Supplemental RoB shall be created and developed for systems that require users to comply with rules beyond those contained in the RoB on Appendix D and Appendix E deemed applicable. In such cases, users must comply with ongoing requirements of each individual system in order to access and retain access (e.g., reading and acknowledging the RoB prior to access and re-acknowledging it each year) to the information system(s). OpDiv System Owners must document any additional system specific RoB and any recurring requirement to acknowledge the respective RoB in their system security plans.

Office of Management and Budget (OMB) Circular A-130 *Managing Information as a Strategic Resource*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 18, Guide *for Developing Security Plans for Federal Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* provide requirements for system specific rules of behavior. At a minimum, the system specific RoB shall:

A. Be in writing;

B. Delineate responsibilities for any expected user of the system and behavior of all users, and shall state the consequences of behavior which violates the rules;

C. State appropriate limits on interconnections to other systems and shall define service provision and restoration priorities;

D. Cover such matters including, but not limited to, teleworking, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Government equipment, assignment and limitation of system privileges, and individual accountability;

E. Reflect technical security controls (e.g., rules regarding passwords shall be consistent with technical password features);

F. Include limitations on changing data, searching databases, or divulging information;

G. State that controls are in place to ensure individual accountability and separation of duties and to limit the processing privileges of individuals;

H. State any other specific rules, limitation or restriction that may apply to the use of the system; and

I. Include consequences for failing to comply with the breach reporting requirements as described in OMB M-17-12 and HHS policy.

Finally, National Security Systems (NSS), as defined by the Federal Information Security Modernization Act of 2014 (FISMA), must independently or collectively implement their own system specific rules.

Appendix D: Forms and Templates

Please note that this appendix is subject to change at any time. The current version of this policy will always reside in the OCIO Policy Library.

1. Rules of Behavior for General Users

These *Rules of Behavior (RoB) for General Users* apply to all Department of Health and Human Services (HHS) employees, contractors, and other personnel who have access to HHS information resources and information technology (IT) systems. Users of HHS information and information systems shall read, acknowledge, and adhere to the following rules prior to accessing data and using HHS information and systems.

1.1. HHS Information Systems

When using and accessing HHS information resources and systems, I understand that I must:

A. Comply with federal laws, regulations, and HHS/Operating Division (OpDiv) policies, standards, and procedures and that I must not violate, direct or encourage others to violate HHS policies, standards or procedures;

B. Not allow unauthorized use and access to HHS information and information systems;

C. Not circumvent or bypass security safeguards, policies, systems' configurations, or access control measures unless authorized in writing;

D. Limit personal use of information and IT Resources to the extent that it does not:

   1. Disrupt my productivity,

   2. Interfere with the mission or operations of HHS, and

   3. Violate HHS security and privacy policies.

E. Have no expectation of privacy while using and accessing HHS information resources and assets at any time, and I understand that any actions and activities are subject to HHS monitoring, recording, and auditing;

F. Complete all mandatory training (e.g., security and privacy awareness, role-based training, etc.) prior to accessing HHS systems and periodically thereafter as required by HHS policies;

G. Be accountable for my actions while accessing and using HHS information, information systems and IT resources;

H. Not share passwords or provide passwords to anyone, including system administrators. I must protect my passwords, Personal Identity Verification (PIV) card, Personal Identification Numbers (PIN) and other access credentials from disclosure and compromise;

I. Promptly change my password when required by HHS policy and if I suspect that it has been compromised;

J. Not use another person's account, identity, password/passcode/PIN, or PIV card or allow others to use my GFE and/or other HHS information resources provided to me to

perform my official work duties and tasks;

K. Not reconfigure systems and modify GFE, install/load unauthorized/unlicensed software or make configuration changes without proper official authorization;

L. Properly secure all GFE, including laptops, mobile devices, and other equipment that store, process, and handle HHS information, when leaving them unattended either at the office and other work locations, such as home, hoteling space, etc. and while on travel. This includes locking workstations, laptops, placing GFE in locked drawer, cabinet, or simply out of plain sight, and removing my PIV card from my workstation.

M. Only use authorized credentials, including PIV card, to access HHS systems and facilities and will not attempt to bypass access control measures; and

N. Report all suspected and identified information security incidents and privacy breaches to the Helpdesk, Incident Response Team (IRT) and/or Privacy Incident Response Team (PIRT) as soon as possible, without unreasonable delay and no later than within ***one (1) hour*** of occurrence/discovery.[4]

1.2. Internet and Email

When accessing and using the Internet and email, I understand that I must:

A. Not access HHS/OpDiv Webmail from the public Internet;

B. Not use personal email and storage/service accounts to store/transmit HHS data and conduct HHS business;

C. Not use personal devices to conduct HHS business unless authorized by HHS/OpDiv Official;

D. Limit access to personal social media and networking sites (such as YouTube, Twitter, Facebook, etc.) while utilizing GFE and during official working hours and to the extent that it does not:

1. Disrupt my productivity,
2. Interfere with the mission or operations of HHS, and
3. Violate HHS security and privacy policies.

E. Limit activities during official work hours, which may adversely affect the security of HHS information, services, information systems, coworkers or cause network degradation (e.g., using social media, large amounts of storage space or bandwidth for personal reasons, such as digital photos, music, or video, using HHS email to create personal sites or subscribe to personal services and memberships, etc.);

F. Not click on links or open attachments sent via email or text message Web links from untrusted sources and verify information from trusted sources before clicking attachments;

[4] CSIRC and IRT points of contact are available at: https://intranet.hhs.gov/it/cybersecurity/hhs_csirc/index.html. Provide all necessary information that will help with the incident investigation.

G. Not auto-forward HHS email to external and internal email sources;

H. Not provide personal or official HHS information to an unsolicited email. If an email is received from any source requesting personal or organizational information or asking to verify accounts or security settings, I will report the incident to the Helpdesk and/or the Computer Security Incident Response Center (CSIRC)/Computer Security Incident Response Team (CSIRT) immediately;

I. Not connect GFE or contractor-owned equipment to unsecured Wi-Fi networks (e.g. airports, hotels, restaurants, etc.) and public Wi-Fi to conduct HHS business unless the Wi-Fi is at a minimum password protected;[5]

J. Not upload or disseminate information which is at odds with departmental missions or positions or without proper authorization, which could create the perception that the communication was made in my official capacity as a federal government employee or contractor; and

K. Only disseminate authorized HHS information related to my official job and duties at HHS to internal and external sources.

1.3. Data Protection

When handling and accessing HHS information, I understand that I must:

A. Take all necessary precautions to protect HHS information and IT assets, including but not limited to hardware, software, sensitive information, including but not limited to Personally Identifiable Information (PII), Protected Health Information (PHI), federal records [media neutral], and other HHS information from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse, and in accordance with HHS policies;[6]

B. Protect sensitive information (e.g., sensitive information, such as confidential business information, PII, PHI, financial records, proprietary data, etc.) at rest (stored on laptops or other computing devices) regardless of media or format, from disclosure to unauthorized persons or groups. This includes, but is not limited to:

   1. Never store sensitive information in public folders, unauthorized devices/services or other unsecure physical or electronic locations;

   2. Always encrypt sensitive information and in transit (transmitted via email, attachment, media, etc.);

   3. Always disseminate passwords and encryption keys out of band (e.g., via text message, in person, or phone call) or store password and encryption keys separately from encrypted files, devices and data when sending encrypted emails or transporting encrypted media;

   4. Access or use sensitive information only when necessary to perform job

[5] Note: Wi-Fi connections found in airports, hotels, restaurants and other public venues may not be secure and subject your device to malicious attacks. CMS employees and contractors must be sure to launch the secure Cisco VPN that is installed on all GFE Laptops prior to accessing any CMS resource to ensure a secure connection.

[6] HHS IT assets are defined as hardware, software, systems, services, and related technology assets used to execute work on behalf of HHS. This definition is adapted from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, *Guide for Conducting Risk Assessments*

functions, and do not access or use sensitive information for anything other than authorized purposes; and

5. Securely dispose of electronic media and papers that contain sensitive data when no longer needed, in accordance with the HHS Policy for Records Management and federal guidelines.

C. Immediately report all suspected and known security incidents (e.g., GFE loss or compromise, violation of security policies, etc.), privacy breaches (e.g., loss, compromise or unauthorized access and use of PII/PHI), and suspicious activities to the Helpdesk and/or CSIRC/CSIRT pursuant to HHS incident response policy and/or procedures[7];

D. Review Office of Security and Strategic Information (OSSI) requirements and policy on use of GFE during foreign travel prior to traveling abroad with GFE or to conduct HHS business; and

E. Notify my Personnel Security Representative (PSR) when there is a need to bring GFE on foreign travel (per requirements defined by the OSSI).

1.4. Privacy

I understand that I must:

A. Collect information about individuals only as required by my assigned duties and authorized by a program-specific law, after complying with any applicable notice or other requirements of laws such as the Privacy Act of 1974, the Paperwork Reduction Act, and agency privacy policies and OMB memoranda, such as OMB Memorandum M-17-06 governing collection of PII on agency websites;

B. Release information to members of the public (including individuals, organizations, the media, individual Members of Congress, etc.) only as allowed by the scope of my duties, applicable HHS policies, and the law;

C. Not access information about individuals unless specifically authorized and required as part of my assigned duties;

D. Not use non-public HHS data for private gain or to misrepresent myself or HHS or for any other unauthorized purpose;

E. Use information about individuals (including PII[8] and PHI[9]) only for the purposes

---

[7] Please review the OMB M-17-12 for the specific distinctions between incident response and breach response.

[8] PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. For other examples see: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

[9] Protected Health Information, as defined in the HIPAA Privacy Rule, is information, including demographic data, that relates to:

- The individual's past, present or future physical or mental health or condition;
- The provision of health care to the individual;
- The past, present, or future payment for the provision of health care to the individual; and/or
- Individual's information for which there is a reasonable basis to believe that it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g. name, address, birth date, Social Security Number) (available at: https://www.hhs.gov/hipaa/for-professionals/privacy).

for which it was collected and consistent with conditions set forth in stated privacy notices such as those provided to individuals at the point of data collection or published in the *Federal Register* (to include System of Records Notices [SORNs]);

F. Ensure the accuracy, relevance, timeliness, and completeness of information about individuals, as is reasonably necessary and to the extent possible, to assure fairness in making determinations about an individual; and

G. Maintain no record describing how an individual exercises his or her First Amendment rights, unless it is expressly authorized by statute or by the individual about whom the record is maintained, or is pertinent to and within the scope of an authorized law enforcement activity.

1.5. Strictly Prohibited Activities

When using federal government systems and equipment, I must refrain from the following activities, which are strictly prohibited:

A. Conducting official HHS business using personal email or personal online storage/service account;

B. Using personal devices to conduct HHS business without written official authorization;

C. Unethical or illegal conduct (e.g. pornography, criminal and terrorism activities, and other illegal actions and activities);

D. Sending or forwarding chain letters, e-mail spam, inappropriate messages, or unapproved newsletters and broadcast messages except when forwarding to report this activity to authorized recipients;

E. Sending messages supporting or opposing partisan political activity as restricted under the Hatch Act and other federal laws and regulations;

F. Using peer-to-peer (P2P) software except for secure tools approved in writing by the OpDiv CIO (or designee) to meet business or operational needs;

G. Sending, retrieving, viewing, displaying, or printing sexually explicit, suggestive or pornographic text or images, or other offensive material (e.g. vulgar material, racially offensive material, etc.);

H. Creating and/or operating unapproved/unauthorized Web sites or services;

I. Using, storing, or distributing, unauthorized copyrighted or other intellectual property;

J. Using HHS information, systems, and devices to send or post threatening, harassing, intimidating, or abusive material about anyone in public or private messages or any forums;

K. Exceeding authorized access to sensitive information;

L. Using HHS GFE for commercial or for-profit activity, shopping, instant messaging (for unauthorized and non-work related purposes), playing games, gambling, watching movies, accessing unauthorized sites, and hacking;

M. Using an official HHS e-mail address to create personal commercial accounts for the purpose of receiving notifications (e.g., sales discounts, marketing, etc.), setting

up a personal business or website, and signing up for personal memberships. Professional groups or memberships related to job duties at HHS are permissible;

N. Removing data or equipment from the agency premises without proper authorization;

O. Sharing, storing, or disclosing sensitive information with third-party organizations and/or using third-party applications (e.g. DropBox, Evernote, iCloud, etc.) unless authorized and with formal agreement in accordance with HHS policies;

P. Transporting, transmitting, e-mailing, texting, remotely accessing, or downloading sensitive information unless such action is explicitly permitted in writing by the manager or owner of such information and appropriate safeguards are in place per HHS policies concerning sensitive information; and

Q. Knowingly or willingly concealing, removing, mutilating, obliterating, falsifying, or destroying HHS information.

SIGNATURE

I have read the above *RoB for General Users*, and understand and agree to comply with the provisions stated herein. I understand that violations of these RoB or HHS information security policies and standards may result in disciplinary action and that these actions may include termination of employment; removal or debarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment.

I understand that exceptions to these RoB must be authorized in advance in writing by the designated authorizing officials. I also understand that violation of federal laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

User's Name: _____

(Print)

User's Signature: _____

Date Signed: _____

The record copy is maintained in accordance with the General Records Schedule (GRS) 1, 18.a.

2. Rules of Behavior for Privileged Users

The following *HHS Rules of Behavior (RoB) for Privileged Users* is an addendum to the *Rules of Behavior for General Users* and provides mandatory rules on the appropriate use and handling of HHS information technology (IT) resources for all HH privileged users, including federal employees, interns, contractors, and other staff who possess privileged access to HHS information systems.[10] Privileged users have network accounts with elevated privileges that grant them greater access to IT resources than non-privileged users. These privileges are typically allocated to system, network, security, and database administrators, as well as other IT administrators.[11] The compromise of a privileged user account may expose HHS to a high-level of risk; therefore, privileged user accounts require additional safeguards.

A Privileged User is a user who has been granted significantly elevated privileges for access to protected physical or logical resources. A privileged user has the potential to compromise the three security objectives of confidentiality, integrity and availability. Such users include, for example, security personnel or system administrators who are responsible for managing restricted physical locations or shared IT resources and have been granted permissions to create new user accounts, modify user privileges, as well as make system changes. Examples of privileged users include:

A. Application developer
B. Database administrator
C. Domain administrator
D. Data center operations personnel
E. IT tester/auditor
F. Helpdesk support and computer/system maintenance personnel
G. Network engineer
H. System administrator.[12]

Privileged users shall read, acknowledge, and adhere to the RoB for Privileged User and any other HHS policy or guidance for privileged users, prior to obtaining access and using HHS information and information systems and/or networks in a privileged role. The same signature acknowledgement process followed for the Appendix D, General RoB, applies to the privileged user accounts. Each OpDiv must maintain a list of privileged users, the privileged accounts those users have access to, the permissions granted to each privileged account, and the authentication technology or combination of technologies required to use each privileged account[13].

---

[10] Per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, privileged roles include, for example, key management, network and system administration, database administration, and Web administration

[11] Office of Management and Budget (OMB), OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 30, 2015.

[12] The definition is derived from the *Identity, Credential & Access Management (ICAM) Privileged User Instruction and Implementation Guidance.*

[13] Per National Institute of Standards and Technology (NIST) White Paper, *Best Practices for Privileged User PIV Authentication*, April 21, 2016

I understand that as a Privileged User, I must:

A. Use Privileged User accounts appropriately for their intended purpose and only when required for official administrative actions;

B. Protect all Privileged User account passwords/passcodes/Personal Identity Verification (PIV)/ personal identified numbers (PINs) and other login credentials used to access HHS information systems;

C. Comply with all system/network administrator responsibilities in accordance with the HHS IS2P and any other applicable policies;

D. Notify system owners immediately when privileged access is no longer required;

E. Properly protect all sensitive information and securely dispose of information and GFE that are no longer needed in accordance with HHS/OpDiv sanitization policies;

F. Report all suspected or confirmed information security incidents (security and privacy) to the OpDiv Helpdesk and/or the OpDiv Security Incident Response Team (CSIRT) and my supervisor as appropriate; and

G. Complete any specialized role-based security or privacy training as required before receiving privileged system access.

I understand that as a Privileged User, I must **not:**

A. Share Privileged User account(s), password(s)/passcode(s)/PIV PINs and other login credentials;

B. Conduct official HHS business using personal email or personal online storage account;

C. Install, modify, or remove any system hardware or software without official written approval or unless it is part of my job duties;

D. Remove or destroy system audit logs or any other security, event log information unless authorized by appropriate official(s) in writing;

E. Tamper with audit logs of any kind. Note: In some cases, tampering can be considered evidence and can be a criminal offense punishable by fines and possible imprisonment;

F. Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls for unauthorized purposes;

G. Introduce unauthorized code, Trojan horse programs, malicious code, viruses, or other malicious software into HHS information systems or networks;

H. Knowingly write, code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses;

I. Use Privileged User account(s) for day-to-day communications and other non-privileged transactions and activities;

J. Elevate the privileges of any user without prior approval from the system owner;

K. Use privileged access to circumvent HHS policies or security controls;

L. Access information outside of the scope of my specific job responsibilities or expose non-public information to unauthorized individuals;

M. Use a Privileged User account for Web access except in support of administrative related activities;

N. Modify security settings on system hardware or software without the approval of a system administrator and/or a system owner; and

O. Use systems (either government issued or non-government) without the following protections in place to access sensitive HHS information:

1. Antivirus software with the latest updates;

2. Anti-spyware and personal firewalls;

3. A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access; and

4. Approved encryption to protect sensitive information stored on recordable media, including laptops, USB drives, and external disks; or transmitted or downloaded via e- mail or remote connections.

SIGNATURE

I have read the above *Rules of Behavior (RoB) for Privileged User*s and understand and agree to comply with the provisions stated herein. I understand that violations of these *RoB* or HHS information security policies and standards may result in disciplinary action and that these actions may include termination of employment; removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that exceptions to these *RoB* must be authorized in advance in writing by the designated authorizing official(s). I also understand that violation of federal laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which these *RoB* draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

User's Name: _____

(Print)

User's Signature: _____

Date Signed: _____

The record copy is maintained in accordance with the General Records Schedule (GRS) 1, 18.a.

Appendix E: References

Legislative

- Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, 128 Stat. 3073, codified at 44 U.S.C. Chapter 35, Subchapter II, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.
- 5 U.S.C. Section 552a (the Privacy Act), https://www.justice.gov/opcl/overview-privacy-act- 1974-2015-edition.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.
- NIST SP 800-88, *Guidelines for Media Sanitization*, December 2014, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.
- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, February 2006, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800- 18r1.pdf.
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 53r4.pdf.
- National Institute of Standards and Technology (NIST) White Paper, *Best Practices for Privileged User PIV Authentication*, April 21, 2016, http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf.

OMB Guidance

- Office of Management and Budget (OMB), Circular A-130, Managing Information as a Strategic Resource, July 2016, https://www.whitehouse.gov/omb/information-for- agencies/circulars.
- OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17- 12_0.pdf.
- OMB M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-05.pdf.

- OMB M-17-09, Management of High Value Assets, https://www.whitehouse.gov/omb/information-for-agencies/memoranda.
- OMB M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements, October 2015, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-03.pdf.
- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, as amended, https://www.whitehouse.gov/omb/information-for-agencies/circulars.

HHS Guidance

- HHS Information Security and Privacy Policy (IS2P) - 2014 Edition, https://intranet.hhs.gov/it/cybersecurity/policies/index.html.
- HHS Policy and Plan for Preparing for and Responding to a Breach of PII, June 29, 2017.
- HHS Standard for Encryption of Computing Devices and Information, December 14, 2016, https://intranet.hhs.gov/it/cybersecurity/policies/index.html.
- HHS Memorandum for Use of GFE during Foreign Travel, December 9, 2016, https://intranet.hhs.gov/it/cybersecurity/policies/index.html.
- HHS Memorandum for the Updated Departmental Standard for the Definition of Sensitive Information, May 18, 2009, http://intranet.hhs.gov/it/cybersecurity/policies/index.html.
- Usage of Unauthorized External Information Systems to Conduct Department Business, January 8, 2014
- HHS Waiver/Risk Acceptance Form, retrievable from: https://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/Waiver/hhs_policy_waiver_201 10729.pdf.

Glossary and Acronyms

Audit Log - A chronological record of information system activities, including records of system accesses and operations performed in a given period. (Source: NIST SP 800-171)

Authentication - A process that provides assurance of the source and integrity of information that is communicated or stored, or that provides assurance of an entity's identity. (Source: NIST SP 800-175A)

Backup (system backup) - The process of copying information or processing status to a redundant system, service, device or medium that can provide the needed processing capability when needed. (Source: NIST SP 800-152)

Breach - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. (Source: OMB Memorandum M-17-12)

Cloud service - External service that enable convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. (Source: NIST SP 800-144)

Compromise - The unauthorized disclosure, modification, substitution or use of sensitive data (e.g., keying material and other security-related information). (Source: NIST SP 800-175B)

Confidentiality - The property that sensitive information is not disclosed to unauthorized entities. (Source: NIST SP 800-175A)

Controlled Unclassified Information (CUI) - Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. (Source: Executive Order 13556) Note: See sensitive information definition below.

CUI Privacy – A category of CUI. Refers to personal information, or, in some cases, "personally identifiable information," as defined in OMB M-17-12, or "means of identification" as defined in 18 USC 1028(d)(7). (Source: National Archives and Records Administration, *CUI Registry*)

CUI Privacy-Health Information – A subcategory of CUI Privacy. As per 42 USC 1320d(4), "health information" means any information, whether oral or recorded in any form or medium, that (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. (Source: National Archives and Records Administration, *CUI Registry*)

Direct Application Access - A high-level remote access architecture that allows teleworkers to access an individual application directly, without using remote access software. (Source:

NIST 800-46 Revision 2)

External Email Source - Email that is not an official HHS.gov email account.

External Information System (or component) – An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. (Source: SP 800-53; CNSSI-4009)

Federal Information - Information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form. (Source: OMB Circular A-130, OMB Memorandum M-17-12)

Federal Information System - An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. (Source: NIST SP 800-53 Revision 4)

Full Disk Encryption (FDE) - The process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product. (Source: NIST SP 800-111)

HHS Information Technology (IT) Assets - Defined as hardware, software, systems, services, and related technology assets used to execute work on behalf of HHS.

HHS Information Assets - Any information created, developed, used for or on behalf of HHS. This includes information in electronic, paper, or other medium format.

Hoteling Space - Term that involves temporary or shared space for working and workstation usage.

Incident - An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. (Source: OMB Memorandum M-17-12)

Information Resources - Information and related resources, such as personnel, equipment, funds, and information technology. (Source: 44 U.S.C., Sec. 3502, CNSSI No. 4009)

Information System (IS) - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems. (Source: 44 U.S.C. Sec 3502, OMB Circular A-130)

Information Technology (IT) - Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the

performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use. (Source: OMB Circular A-130)

Integrity - The property that protected data has not been modified or deleted in an unauthorized and undetected manner. (Source: NIST SP 800-175A)

Media - Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. (Source: NIST SP 800-53 Revision 4) **NOTE**: See **Removable Media**.

Mobile device - A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations.

Examples include smart phones, tablets, and E-readers. (Source: NIST SP 800-79-2)

Mobile Device Management - Mobile enterprise security technology used to address security requirements. (Source: NIST SP 800-163, page 9).

Personal Identity Verification (PIV) card -The physical artifact (e.g., identity card, "smart" card) issued to an applicant by an issuer that contains stored identity markers or credentials (e.g., a photograph, cryptographic keys, digitized fingerprint representations) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable) (Source: NIST SP 800-79 Revision 2)

Personally Identifiable Information (PII) - Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (Source: OMB M-17-12, OMB Circular A-130) **NOTE**: Per NIST SP 800-122, this includes any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Personally Owned Device A non-organization-controlled client device owned by an individual. These client devices are controlled by the owner, who is fully responsible for securing them and maintaining their security. (Source: Adapted from NIST SP 800-46 Revision 2) **NOTE**: Also referred to as a Bring Your Own Device (BYOD).

Privileged User - Privileged users have network accounts with privileges that grant them greater access to IT resources than non-privileged users have. These privileges are typically allocated to system, network, security, and database administrators, as well as other IT administrators. (Source: NIST SP 800-53 Revision 4)

Protected Health Information (PHI) - Individually identifiable health information (IIHI) that is: transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. (Source: NIST SP 800-122)

Remote Access - The ability for an organization's users to access its non-public computing resources from external locations other than the organization's facilities. (Source: CNSSI 4009) **NOTE**: Per NIST SP 800-53 Revision 4, this also applies to a process acting on behalf of a user.

Remote Access Method - Mechanisms that enable users to perform remote access. There are four types of remote access methods: tunneling, portals, remote desktop access, and direct application access. (Source: Adapted from NIST, SP 800-46 Revision 2)

Remote Desktop Access - A high-level remote access architecture that gives a teleworker the ability to remotely control a particular desktop computer at the organization, most often the user's own computer at the organization's office, from a telework client device. (Source: NIST, SP 800-46 Revision 2)

Removable Media - Portable data storage medium that can be added to or removed from a computing device or network. Note: Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external/removable hard drives; external/removable Solid State Disk (SSD) drives; magnetic/optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD). (Source: CNSSI 4009)

Sanitize - A process to render access to Target Data on the media infeasible for a given level of effort. Clear, Purge, and Destroy are actions that can be taken to sanitize media. (Source: NIST, SP 800-88 Revision 1)

Sanitization - Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs. (Source: NIST SP 800-53 Revision 4)

Sensitive information - Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act); that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Source: NIST SP 800-53 Revision 4)

System of Records - A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. (Source: NIST SP 800-122 and *The Privacy Act of 1974*, 5 U.S.C. § 552a (a) (5))

Telework - The ability for an organization's employees, contractors, business partners, vendors, and other users to perform work from locations other than the organization's facilities. (Source: NIST, SP 800-46 Revision 2)

Telework Client Device - A PC or mobile device. (Source: NIST SP 800-46 Revision 2)

Third-Party-Controlled Device - A client device controlled by a contractor, business partner, or vendor. These client devices are controlled by the remote worker's employer who is ultimately responsible for securing the client devices and maintaining their security. (Source: Adapted from NIST, SP 800-46 Revision 2)

Unknown Device - A client device that is owned and controlled by other parties, such as a kiosk computer at hotels, and a PC or mobile device owned by friends and family. The device is labeled as "unknown" because there are no assurances regarding its security posture. (Source: Adapted from NIST, SP 800-46 Revision 2)

Virtual Disk Encryption - The process of encrypting a container, which can hold many files and folders, and permitting access to the data within the container only after proper authentication is provided. (Source: NIST, SP 800-111)

Virtual Private Network (VPN) - A virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks. (Source: NIST, SP 800-46 Revision 2)