# Rules of Behavior for General Users v. 3.0

These *Rules of Behavior (RoB) for General Users* apply to all HHS personnel (employees, contractors, interns, etc.) and any other individuals who are granted access to HHS/OpDiv information resources and IT systems. Users of HHS/OpDiv information, IT resources and information systems must read, acknowledge, and adhere to the following rules prior to accessing data and using HHS/OpDiv information and IT resources.

## A. HHS/OpDiv Information and IT Resources

When using and accessing HHS/OpDiv information and IT resources, I understand that I must:

1. Comply with federal laws, regulations, and HHS/OpDiv policies, standards, and procedures and that I must not violate, direct, or encourage others to violate HHS/OpDiv policies, standards, or procedures.
2. Not allow unauthorized use and access to HHS/OpDiv information and IT resources.
3. Not circumvent or bypass security safeguards, policies, systems' configurations, or access control measures unless authorized in writing.
4. Limit personal use of information and IT resources so that it:
   a) Involves no more than minimal additional expense to the government
   b) Is minimally disruptive to my personal productivity
   c) Does not interfere with the mission or operations of HHS
   d) Does not violate HHS/OpDiv security and privacy policies.
5. Refrain from using GFE, email, third-party websites, and applications (TPWAs) (e.g., HHS/OpDiv social media sites and cloud services, etc.) and other HHS/OpDiv information resources for activities that are not related to any legitimate/officially sanctioned HHS/OpDiv business purpose, except for the limited personal use stated above.
6. Complete all mandatory training (e.g., security and privacy awareness, role-based training, etc.) when initially granted access to HHS/OpDiv systems and periodically thereafter as required by HHS/OpDiv policies.
7. Be accountable for my actions while accessing and using HHS/OpDiv information, information systems and IT resources.
8. Not reconfigure systems and modify GFE, install/load unauthorized/unlicensed software or make configuration changes without proper official authorization.
9. Properly secure all GFE, including laptops, mobile devices, and other equipment that store, process, and handle HHS/OpDiv 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, storing GFE in a locked drawer, cabinet, or simply out of plain sight, and removing my PIV card from my workstation.
10. Must return all GFEs and Government issued PIV Card on or before last day of employment or contract termination.
11. Report all suspected and identified information security incidents and privacy breaches to the Helpdesk, HHS/OpDiv Computer Security Incident Response Center (CSIRC), or OpDiv

Computer Security Incident Response Team (CSIRT) as soon as possible, without unreasonable delay and no later than within one (1) hour of occurrence/discovery.[1]

## B. No Expectation of Privacy

When using and accessing HHS/OpDiv information and IT resources, I understand that I would have no expectation of Privacy. I acknowledge the following:

1. There would be no expectation of privacy when using HHS/OpDiv information resources, systems and GFE and may be monitored, recorded, and audited at any time.
2. My use any HHS/OpDiv information resources, systems and GFE is 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.
3. My 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 at any time. For example, after obtaining management approval, HHS/OpDiv authorized technical staff may employ monitoring tools in order to maximize the utilization of HHS/OpDiv resources.[2]

## C. Password Requirement

When creating and managing my password, I understand that I must comply with the following baseline requirements:

1. Comply with all HHS/OpDiv password requirements.
2. Create passwords with minimum of 15 characters.[3]
3. Not use common or compromised passwords.
4. Protect my passwords, Personal Identity Verification (PIV) card, Personal Identification Numbers (PIN) and other access credentials from disclosure and compromise.
5. Promptly change my password if I suspect or receive notification that it has been compromised.
6. Immediately select a new password upon account recovery.
7. Not use another person's account, identity, password/passcode/PIN, or PIV card or allow others to use my GFE and/or other HHS/OpDiv information resources provided to me to perform my official work duties and tasks. This includes not sharing passwords or provide passwords to anyone, including system administrators.
8. Only use authorized credentials, including PIV card, to access HHS/OpDiv systems and facilities and will not attempt to bypass access control measures.
9. Select the PIV card to conduct HHS/OpDiv business whenever possible when both the PIV and

[1] CSIRC and IRT points of contact are available at: https://intranet.hhs.gov/about-hhs/org-chart/asa-offices/office-of-the-chief-information-officer-ocio/csirc . Provide all necessary information that will help with the incident investigation.
[2] See the HHS memoranda *Policy for Monitoring Employee Use of HHS IT Resources* and *Updated Department Standard Warning Banner* available at Memoranda | Community for HHS Intranet
[3] See *NIST SP 800-209 Security Guidelines for Storage Infrastructure,* available at https://csrc.nist.gov/publications/detail/sp/800-209/final.

password options are available for authentication.

## D. Internet and Email

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

1. Not access HHS/OpDiv Webmail from the public internet.
2. Handle personal devices in the following manner:
   a) Not connecting personal devices to HHS/OpDiv systems without proper official authorization
   b) Not conducting official HHS/OpDiv business using non-HHS/OpDiv email or personal online storage/service accounts without written authorization from HHS/OpDiv or OpDiv CISO or designee
   c) Not using personal devices, non-HHS/OpDiv email, and unauthorized third-party systems, storage services, or applications (e.g., Dropbox, Google Docs, mobile applications, etc.) to store, transmit, process HHS/OpDiv information, and conduct HHS/OpDiv business without proper official authorization such as written approval from the HHS/OpDiv or OpDiv CISO or their designee.
3. Not automatically (auto) forward HHS/OpDiv email to any internal and external email sources or forwarding email/files that contain HHS/OpDiv information to unauthorized systems and devices that are used for non-HHS/OpDiv and non-OpDiv business purposes.
4. Not use 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.
5. Not provide official HHS/OpDiv information to an unsolicited email if prohibited. 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 CSIRC/ CSIRT immediately.
6. Only disseminate authorized HHS/OpDiv information related to my official job and duties at HHS/OpDiv to internal and external sources.
7. 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.
8. 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/OpDiv business unless Wi-Fi access is at a minimum, protected with an unshared, unique user password access.

## E. Data Protection

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

1. Take all necessary precautions to protect HHS/OpDiv information and IT assets, including but not limited to hardware, software, sensitive information, including but not limited to PII, PHI, federal records [media neutral], and other HHS/OpDiv information from unauthorized access,

use, modification, destruction, theft, disclosure, loss, damage, or abuse, and in accordance with HHS/OpDiv policies.[4]

2. 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:
    a) Never store sensitive information in public folders, unauthorized devices/services or other unsecure physical or electronic locations
    b) Always encrypt sensitive information at rest and in transit (transmitted via email, attachment, media, etc.)
    c) 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
    d) Access or use sensitive information only when necessary to perform job functions, and do not access or use sensitive information for anything other than authorized purposes
    e) Securely dispose of electronic media and papers that contain sensitive data when no longer needed, in accordance with the HHS/OpDiv Policy for Records Management and federal guidelines.
3. 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, or use of PII/PHI), and suspicious activities to the Helpdesk and/or CSIRC/CSIRT at CSIRC@HHS.gov or call 1-866-646-7514 pursuant to HHS/OpDiv incident response policies and/or procedures.5
4. Not take permanently issued GFE devices with me during official foreign travel. Only carry loaner GFE (including mobile computing, phone, and storage devices) during official foreign travel. If there is a need to take GFE on personal foreign travel, submit a request and get approved by a designated government official within the OpDiv. Upon approval, obtain a loaner GFE and adhere to the HHS policy in the memorandum Use of Government Furnished Equipment (GFE) During Foreign Travel. Additional requirements include:
    a) Reviewing Office of Security and Strategic Information (OSSI) requirements and the requirements within the Memorandum on the Use of GFE During Foreign Travel prior to traveling abroad with GFE or to conduct HHS/OpDiv business
    b) Notifying my Personnel Security Representative (PSR) when there is a need to bring GFE on foreign travel (per requirements defined by the OSSI in accordance with the Memorandum on the Use of GFE During Foreign Travel).

[4] HHS/OpDiv 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 NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments, available at* https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

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

## F. Privacy

I understand that if I am working with PII, I must:

1. Protect PII[6] from inappropriate disclosure, loss, or compromise.
2. Only collect, use, maintain, and disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose.
3. Disclose PII only to those who need to know the information to execute their work and are authorized to receive it.
4. Comply with applicable legal and regulatory privacy safeguards. For example:
   a) Report suspected or confirmed breaches of PII in accordance with the *HHS/OpDiv Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII*)
   b) Submit a privacy impact assessment (PIA) for systems or electronic information collections collecting PII.
5. Be transparent about information policies and practices with respect to PII, provide clear and accessible notice regarding collection, use, maintenance, and disclosure of PII, and seek consent for the collection, use, and disclosure of PII as appropriate.
6. Enable individuals to access, correct, or amend their PII as appropriate, and ensure PII is accurate, relevant, timely and complete to guarantee fairness to individuals.
7. Not access PII unless specifically authorized and required as part of assigned duties.
8. Collect, use, and disclose PII only for the purposes 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 HHS' SORN website (to include System of Records Notices [SORNs]).
9. 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.
10. Consult with my OpDiv privacy program or Senior Official for Privacy (SOP)7 before initiating or making significant changes8 to a system or collection of PII.

## G. Telework and GFE

When teleworking, I understand that I must:

1. Telework only when approved by management and conduct myself with the same professionalism remotely as required in the workplace.
2. Safeguard any GFE provided for telework.
3. Safeguard HHS/OpDiv information, equipment, including GFE. Protecting HHS/OpDiv information including PII, CUI and any sensitive information is just as important at a telework location as it is in an HHS/OpDiv building.

---

[6] Personally identifiable information (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. Office of Management and Budget (OMB). (2016, July 27). *Circular No. A-130, Managing Information as a Strategic Resource*, p. 21. Available at: Review-Doc-2016--466-1.docx (whitehouse.gov).

[7] To contact your OpDiv SOP, visit https://www.hhs.gov/web/policies-and-standards/hhs-web-policies/privacy/index.html#HHS-Privacy-Officials.

[8] Examples of significant changes include, but are not limited to, changes to the way PII are managed in the system, new uses or sharing, and the merging of data sets.

4. Only connect additional devices to GFE as necessary to conduct official government business with OpDiv approval, if the devices are not on the prohibited vendor list.[9]
   a) Only connect GFE to printers by opening a ticket with the helpdesk.
   b) Contact OpDiv Help Desk to have drivers installed to GFE prior to connecting printer.
   c) Connect printers to GFE via USB or other physical port. Wireless connections between GFE and printers may require OpDiv approval.
5. Not install any software to GFE whether it is free or free downloadable unless authorized or approved.
6. Use my home Wi-Fi network to provide the connectivity for telework but my home networks must be set up in accordance with guidance from HHS/OpDiv or OpDiv;10
7. Not connect hardware to GFE via Bluetooth unless necessary for official use must keep Bluetooth turned off and only turn on when needed.
8. Protect all sensitive information, including CUI and PII.

## H. Strictly Prohibited Activities

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

1. Accessing any social media websites (such as YouTube, Twitter, Facebook, etc.) while utilizing GFE, unless required for official HHS/OpDiv business.
2. Accessing, downloading, or clicking on unknown links, particularly on social media sites such as "Malware Alert notices".
3. Clicking 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. I must report suspected phishing attempts using the Report Phishing button or forward suspicious emails as an attachment to Spam@hhs.gov.
4. Engaging in activities that could cause congestion, delay, or disruption of service to any HHS/OpDiv information resource (e.g., sending chain letters via email, playing streaming videos, games, music, etc.).
5. Accessing, downloading and/or uploading unethical, illegal, or criminal content from/to the internet (e.g., pornographic, and sexually explicit materials, illegal weapons, criminal and terrorism activities, and other illegal actions or activities).
6. 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.).
7. Using non-public HHS/OpDiv data for private gain or to misrepresent myself or HHS/OpDiv or for any other unauthorized purpose.

[9] see CISA CAPACITY ENHANCEMENT GUIDE: Printing While Working Remotely, available at https://www.cisa.gov/sites/default/files/publications/CISA_CEG_Printing_While_Working_Remotely_508C_1.pdf.
[10] For additional information, see https://intranet.hhs.gov/news/blog-posts/cybercare/home-network-security-annual-checkup as well as https://intranet.hhs.gov/policy/hhs-policy-for-securing-wireless-local-area-networks.

8. Sending messages supporting or opposing partisan political activity as restricted under the Hatch Act and other federal laws and regulations.
9. Engaging in any outside fund-raising, endorsing any product or service, lobbying, or engaging in partisan political activity.
10. 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).
11. Creating a website, TPWA, or social media site on behalf of HHS/OpDiv or uploading content to a website, TPWA, or social media site without proper official authorization.[11]
12. 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.
13. 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.
14. Creating and/or operating unapproved/unauthorized Web sites or services.
15. Using, storing, or distributing, unauthorized copyrighted or other intellectual property.
16. Using HHS/OpDiv information, systems, and devices to send or post threatening, harassing, intimidating, or abusive material about anyone in public or private messages or any forums.
17. Exceeding authorized access to sensitive information.
18. Using HHS/OpDiv GFE for commercial or for-profit activity, shopping, instant messaging (for unauthorized and non-work-related purposes), managing outside employment or business activity, or running personal business, playing games, gambling, watching movies, accessing unauthorized sites, or hacking.
19. Using an official HHS/OpDiv 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/OpDiv are permissible.
20. Removing data or equipment from the agency premises without proper authorization.
21. Sharing, storing, or disclosing sensitive information with third-party organizations and/or using third-party applications (e.g., Drop Box, Evernote, iCloud, etc.) unless, in very limited circumstances, is authorized by HHS/OpDiv or OpDiv CISO or designee.
22. Storing sensitive data in external platforms, such as personal Google Docs.
23. 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/OpDiv policies concerning sensitive information.
24. Knowingly or willingly concealing, removing, mutilating, obliterating, falsifying, or destroying HHS/OpDiv information.

[11] All third-party web applications, social media sites, storage and cloud services must be authorized prior to use. Only authorized personnel can post only authorized content on public-facing websites and social media sites.

25. Accessing or visiting any unknown website(s) which may be infected with malware, responding to phishing emails, storing credentials in an unsecured location. This may cause to create an Incident and require having additional Awareness and Security training.
26. Using any file sharing program without agency's permission.

**SIGNATURE**

I have read the above *Rules of Behavior for General Users* and understand and agree to comply with the provisions stated herein. I understand that violations of these RoB or HHS/OpDiv information security policies and standards may result in disciplinary action and that these actions may include reprimand, suspensive of access privileges, revocation of access to federal information, IT resources, information systems, and/or facilities, deactivation of accounts, suspension without pay, monetary fines, termination of employment; removal or debarment from work on federal contracts or projects; criminal charges that may result in 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/OpDiv 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: _____