U.S. Department of Homeland Security

DHS 4300A,

"*Information Technology System Security Program, Sensitive Systems*"

Attachment G

Rules of Behavior

Version 1.0

April 28, 2022

This page intentionally blank.

Document Change History

Version	Date	Description
1.0	April 28 , 2022	Reviewed and confirmed with no changes needed by HQ Policy Manager Tanyette Gatling-Miller

CONTENTS

1.0 INTRODUCTION GENERAL RULES OF BEHAVIOR

Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource, Appendix I" and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, "Guide for Developing Security Plans for Federal Information Systems" provide requirements for system-specific rules of behavior for general support systems (GSS) such as local area networks (LAN) and for major applications (MA). These requirements include the following:

- Rules of behavior shall contain a signature page on which the user acknowledges that they have read, have understood, and agree to abide by the Rules of Behavior. Electronic signatures are acceptable.
- Users shall read and sign rules of behavior before they are given access to Government systems. If the employee has a digital signature authenticated by a Personal Identity Verification (PIV) card, Personal Identity Verification Interoperability (PIV-I) card, Derived Alternate Credential (DAC), or Common Access Card (CAC), use of their digital signature is encouraged; new employees may physically sign.
- The rules shall delineate responsibilities and expected behavior of all users with access to a system and shall state the consequences of behavior not consistent with the rules.
- The rules shall cover such matters as teleworking, remote access, connection to the Internet, use of copyrighted works, unofficial use of Government equipment, assignment and limitation of system privileges, and individual accountability.
- The rules shall state appropriate limits on interconnections to other systems.
- The rules shall reflect technical security controls (e.g., rules regarding passwords should be consistent with technical password features).
- The rules shall include limitations on altering data, searching databases, and divulging information.
- The rules shall state that controls are in place to ensure individual accountability and separation of duties and to limit the processing privileges of individuals.

Section 1.8 of NIST SP 800-18, Rev. 1, "Guide for Developing Security Plans for Federal Information Systems," provides example rules of behavior.

Information system rules of behavior are a vital part of the DHS Cybersecurity Program and help ensure the security of systems and the confidentiality, integrity, and availability of sensitive information and systems.

Information system rules of behavior inform users of their responsibilities and educate them as to personal accountability for their actions when accessing DHS information systems. Information system rules of behavior apply to all users of the information system, including DHS employees, contractors, detailees, and all others with access to the system.

2.0 SYSTEM-SPECIFIC RULES OF BEHAVIOR

In accordance with OMB Circular A-130 and DHS 4300A, "*Information Technology System Security Program (ITSSP), Sensitive Systems*," DHS Components are responsible for developing specific rules of behavior for their information systems, ensuring that users of the systems read and acknowledge the rules via physical or electronic signature, and for maintaining the executed rules of behavior. System rules of behavior must be executed before a user is provided access to the information system. Components should collaborate with their respective Chief Human Capital Officer, Chief Privacy Officer, and Chief Counsel organizations on the development of their system rules of behavior.

Appended to this attachment are the minimum baseline Rules of Behavior that apply to all users of DHS systems. These Rules of Behavior are consistent with the IT security policy and procedures prescribed by DHS Management Directive 140-01, "*Information Technology Security Program*," DHS Policy Directive 4300A, "*Information Technology System Security Program (ITSSP), Sensitive Systems*." Components should tailor these Rules of Behavior to their own systems and IT devices; they establish rules more stringent than the baseline but may not remove any baseline rule.

Information system users that are not subject to Component-specific rule(s) of behavior must comply with the minimum baseline for the Department.

Any user not in compliance with applicable Rules of Behavior is subject to sanctions that may include verbal or written warning, denial of system access for a specific period of time, reassignment to other duties, termination of employment, civil sanctions, or civil or criminal prosecution.

APPENDIX: DHS GENERAL INFORMATION SYSTEM RULES OF BEHAVIOR

In accordance with the requirements of the Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource, Appendix I" and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, "Guide for Developing Security Plans for Federal Information Systems," DHS established minimum information system rules of behavior for the use of DHS information systems. These Rules of Behavior are consistent with the IT security policy and procedures identified in DHS Management Directive 140-01, "Information Technology Security *Program*;" and the DHS 4300A *"Information Technology System Security Program, Sensitive Systems."*

The following minimum Rules of Behavior apply to all users of DHS information systems and IT resources (e.g., networks; databases; applications; workstations; laptops; mobile computing devices, including cell phones, smartphones, and tablets; and removable media such as USB drives, CDs, or DVDs), including DHS employees, support contractors, detailees and all other system users.

These Rules of Behavior apply to users at their primary workplace; telework, satellite, or alternate worksite; and while traveling, domestically or internationally. Information system users that are not subject to Component-specific rule(s) of behavior must comply with this minimum baseline rules of behavior. Any user not in compliance with applicable Rules of Behavior is subject to sanctions that may include verbal or written warning, denial of system access for a specific period of time, reassignment to other duties, termination of employment, civil sanctions, or civil or criminal prosecution.

DHS Minimum Baseline Information System Rules of Behavior

System Access

- I understand that I am given access only to those systems to which I require access in the performance of my official duties.
- I will not attempt to access systems I am not authorized to access.

Passwords and Other Access Control Measures

- I understand that DHS has a goal of 100% strong identity authentication that will require use of my Personal Identity Verification (PIV) card and Personal Identification Number (PIN).
- In those instances where a password must be used, I will use a password that complies with the appropriate Defense Information Systems Agency (DISA) Security Technical

Implementation Guide (STIG) as specified by the system Information Systems Security Officer (ISSO).

- I will protect passwords and PINs from disclosure.
- I will not share passwords or PINs with anyone, including system administrators.
- I will not record passwords or PINs on paper or in electronic form.
- To prevent others from obtaining my password via "shoulder surfing," I will shield my keyboard from view when entering my password or PIN.
- I will promptly change my password or PIN whenever its compromise is known or suspected to have occurred.
- I will ensure that my PIV card is always in my personal possession while at work or performing work-related activities.
- I will promptly report the loss of my PIV card to my supervisor and the DHS Chief Security Office.
- I will not store my PIV card with DHS workstations, laptop computers, or mobile computing devices.
- I will not attempt to bypass access control measures.

Data Protection

- I will use only DHS equipment or DHS authorized and approved services, such as Workplace as a Service (WPaaS), to access DHS systems and information.
- I will protect sensitive information from disclosure to unauthorized persons or groups.
- I will only share information from DHS systems in accordance with all DHS privacy, legal, security, and policy requirements. Should I share personally identifiable information or special protected class data with unauthorized persons or entities, I will immediately report the incident to my component privacy office in accordance with *DHS 4300A, "Information Technology Security Program, Sensitive Systems,"* Attachment F, "Incident Response."
- I will lock my workstation or laptop computer by removing my PIV card or other secondary authentication device, or I will use a password-protected screensaver, whenever I am away from my work area for a short time.
- I will not access, process, or store classified information on DHS office equipment unless use of the equipment is authorized for classified information of the appropriate level.

Software

- I agree to abide by software copyrights and to comply with the terms of all licenses.

- I will not install on DHS equipment any unauthorized software, including software available for downloading from the Internet, software available on DHS networks, and personally owned software.

Use of Government Furnished Equipment, Internet, and Email

- I understand that I can only use Government systems for official Internet activities and email, with limited personal use allowed. Allowed personal use is described in DHS Directive 142-03, "Electronic Mail Usage and Maintenance" and DHS Directive 262-04, "DHS Web (Internet and Extranet Information)."
- I understand that government systems can only be accessed from approved locations and for work purposes. If traveling, GFE usage must be approved.
- I will not use Government systems for access to personal webmail.
- I will not forward government emails to my personal email account.
- I understand that my use of DHS information systems, equipment, and networks, including, but not limited to, Internet and email use may be monitored, and I consent to such monitoring.
- I will not use unauthorized cloud services or peer-to-peer (P2P) file sharing to connect remotely to other systems for the purpose of sharing files. I understand that these services can be a means of spreading viruses over DHS networks and may put sensitive government information at risk. I also understand that DHS 4300A "*Information Technology Security Program (ITSP), Sensitive Systems*" prohibits the use of P2P software other than that approved for use by the Department on any DHS-controlled or DHS-operated system.
- I will not provide personal or official DHS information if solicited by email, respond to requests for personal information, verify accounts, security settings, or open any links contained in email unless I know the sender and source have an authorized need to know. I will forward any suspicious or questionable email to my Component SOC Spam team and take no other action.
- I understand that only content managers designated by the Office of Public Affairs (OPA) may post material to Department and Component intranet sites.
- I understand that personal Internet activities which inhibit the security of DHS information and information systems, or cause degradation of network services are prohibited. Examples of such activity include streaming of audio or video, social networking, peer-to-peer networking, software or music piracy, online gaming, webmail, unauthorized Instant Messaging (IM), and hacking.
- I understand that the use of webmail or other personal email accounts are prohibited on DHS information systems.

- I understand that gambling and the viewing of pornographic or other offensive content is strictly prohibited on DHS furnished equipment and networks.

Teleworking

Employees approved for teleworking at any alternate workplace must adhere to the following additional rules of behavior:

- At my alternate workplace, I will follow security practices that are the same as or equivalent to those required of me at my primary workplace.
- I will physically protect any communications and computing equipment I use for teleworking when they are not in use.
- I will secure and separate official materials from all printed personal documents in my telework location.
- I will protect sensitive data at my alternate workplace. This includes disposing of sensitive information by shredding, burning, pulping, or pulverizing such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste. Alternatively, employees can secure materials in a locked file cabinet, locked desk drawer, or a similar locked container and return them to their duty location on recurring intervals for disposal, as outlined in Section K of DHS Directive 11042, Safeguarding Sensitive But Unclassified (For Official Use Only) Information
- If permitted to print at home, I will take reasonable and appropriate precautions to immediately remove official documents from printers to prevent inadvertent disclosure.

Laptop Computers and Mobile Computing Devices

Use of DHS communications and computing devices is subject to following additional rules of behavior:

- I will use only DHS-approved communications and computing devices to access DHS systems and information.
- I will keep Government Furnished Equipment (GFE) under my physical control at all times, or I will secure it in a suitable locked container under my control.
- I will password-protect any communications and computing devices I use.
- I will take all necessary precautions to protect GFE against loss, theft, damage, abuse, and unauthorized use (e.g., by employing lockable cases and keyboards, locking cables, and removable storage devices). If my equipment or PIV card is lost or stolen, I will immediately report the incident to my supervisor and to the DHS Chief Security Office (onecardssd@hq.dhs.gov).

- When contacted by technical support personnel who request actions on my part, I will verify their authenticity by calling my Component's Help Desk, or using the GAL or other DHS identity-search tool. When I have verified the caller's identity, I will call them as instructed by the Help Desk, and immediately comply with instructions from the technical support personnel to perform update actions, or to make equipment assigned to me available to technical support personnel for updating.
- I will use only DHS-authorized Internet connections or use DHS-approved VPN technology when connecting over the Internet
- I will not make any changes to any GFE system configuration unless I am directed to do so by an authorized DHS system administrator or field service technician.
- I will not program any GFE with sign-on sequences, passwords, or access phone numbers.
- I understand and will comply with the requirement that sensitive information stored on any laptop computer used in a residence or on travel shall be protected using encryption validated in accordance with Current NIST FIPS 140 federal requirements, "Security Requirements for Cryptographic Modules," and current NIST SP 800-52, NIST SP 800-63 requirements as applicable.
- I understand and will comply with the requirement that sensitive information processed, stored, or transmitted on mobile devices, CDs, and previously approved USB thumb drives must be encrypted using approved encryption methods.

Incident Reporting

- I will promptly report IT security incidents (suspected or confirmed) in accordance with DHS CISO procedures for detecting, reporting, and responding to information security incidents in accordance with DHS 4300A Sensitive Systems Handbook Attachment F, "Incident Response."

Accountability

- I understand that I have no expectation of privacy while using any DHS equipment and while using DHS networks or email services.
- I understand that I will be held accountable for all actions performed using my credentials on DHS systems and IT resources.

Acknowledgment Statement

I acknowledge that I have read, understand, and will comply with the DHS Rules of Behavior. I understand that failure to comply with the Rules of Behavior could result in one or more of the following actions: including verbal or written warning, denial of system access for a specific period of time, reassignment to other duties, termination of employment, civil sanctions, or civil or criminal prosecution.

Name of User (printed):_____

User's Phone Number:_____

User's Email Address:_____

DHS Component:_____

Location or Address:_____

Supervisor:_____

Supervisor's Phone Number:_____

User's Signature:_____ Date:_____

Please read the "Tips for Traveling with Laptops and Other Portable Devices" on the following page.

APPENDIX: TIPS FOR TRAVELING WITH LAPTOPS AND OTHER PORTABLE DEVICES

- Traveling internationally with DHS cell phones is prohibited, unless specifically authorized in advance
- Always keep portable devices or USB drives under your physical control at all times.
- At airport security, place the portable device on the conveyor belt only after the belongings of the person ahead of you have cleared the scanner. If you are delayed, keep your eye on the portable device until you can pick it up.
- Do not place the portable device in checked luggage.
- Do not store or check the portable device in an airport, a train or bus station, or any public locker.
- If you must leave a portable device in a car, lock it in the trunk so that it is out of sight.
- Avoid leaving a portable device in a hotel room. If you must leave it in a hotel room, lock it inside another piece of luggage or in an in-room hotel safe.
- Avoid connecting your portable device to any shared computer (e.g. at a library, hotel) or charging stations (e.g. at airport terminals) that you do not control and know it has not been compromised.
- Avoid connecting to public Wi-Fi networks offered at locations such as airports, hotels and cafés unless connecting through a VPN. Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network. Only use sites that begin with “https://” when conducting sensitive activities.
- Disable Bluetooth and other wireless technology (e.g. NFC, GPS) when not in use.
- Ensure your laptop and other portable devices are utilizing the latest updates to its operating system and applications.