Division of Personnel Security and Access Control (DPSAC)

General Rules of Behavior for Users of DPSAC Systems that Access, Store, Receive, or Transmit Sensitive Information

The following rules of behavior apply to all DPSAC employees, contractors and vendors who access DPSAC systems and other information technology (IT) resources such as laptop and desktop computers to access, store, receive, or transmit sensitive information. These Rules of Behavior (ROB) are in accordance and consistent with the NIH IT General Rules of Behavior[1] and the NIH Policy for Access to Information Technology Systems and Networks[2].

DPSAC ROB apply to users at their primary workplace, while teleworking or at any alternative workplaces, and while traveling.

System Access

- I understand that all staff must authenticate using a PIV card or other NIH-authorized derived PIV credential (PIV-D) to access NIH IT systems, applications, networks, and data, including NIH-networked desktop and laptop computers.
- I must use government-furnished equipment or contractor-furnished equipment that meets or exceeds NIH requirements for patching, anti-virus, etc. to access DPSAC systems, applications, networks, and data in accordance with NIH Manual Chapter 2814 NIH Policy on the Prohibited Use of Non-Government Furnished (Non-GFE) IT Equipment[3], NIH Manual Chapter 2810 NIH Remote Access Policy[4], and other NIH Information Security policies as described in the NIH Information Security Handbook[5].
- 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 for access.

Passwords and Other Access Control Measures

- I understand that Personal Identity Verification (PIV) cards, Personal Identification Numbers (PIN), passwords and other access credentials must be protected from disclosure and compromise and never shared.
- I must change passwords when required by NIH policy and/or if I suspect it's been compromised.
- I understand access to DPSAC systems and networks (including NIH-networked desktop and laptop computers) will only be granted by using PIV card authentication.
- I will never use another person's account, identity, password/passcode/PIN, or PIV card.
- I will only use authorized credentials, including PIV cards, to access NIH systems and facilities.
- I understand remote access to NIH IT resources requires use of a PIV card (or other approved NIH Smart Card or Secure ID token) and use of the NIH Virtual Private Network or other NIH approved remote access mechanism (e.g., CITRIX).
- I will never connect GFE to unsecured Wi-Fi networks (e.g. airports, hotels, restaurants, etc.) or public Wi-Fi to conduct NIH business unless the Wi-Fi is at minimum password protected.

Data Protection

- I will take all necessary precautions to protect DPSAC information and IT resources, including but not limited to hardware, software, sensitive information, federal records [media neutral], and other NIH information from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse, and in accordance with NIH information handling policies.
- I will use only DPSAC equipment, and never personally owned equipment, to access DPSAC systems and information.
- I will protect sensitive information (e.g., personally identifiable information (PII)[6] , protected health information (PHI)[7], confidential business information, financial records, proprietary data, etc.) stored on laptops or other computing devices, regardless of the media or format, from disclosure to unauthorized persons or groups.
- I will log off or lock my workstation or laptop computer, or I will use a password- protected screensaver, whenever I step away from my work area, even for a short time; I will log off when I leave for the day.
- I will not access, process, or store classified information on DPSAC office equipment that has not been authorized for classified information of commensurate level.
- I will not use personal email and storage/service accounts to conduct NIH business.
- I will never use personal devices to conduct NIH business or store/transmit NIH data without official approval.

Use of Government Office Equipment

- I understand that my use of DPSAC office equipment may be monitored, and I consent to this monitoring.
- I understand that the use of webmail or other personal email accounts is prohibited on DPSAC information systems.
- I understand that Internet activities which inhibit the security of DPSAC 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, Instant Messaging (IM), and hacking.
- I understand that the viewing of pornographic or other offensive content is strictly prohibited on DPSAC furnished equipment and networks.

Software

- I agree to abide by software copyrights and to comply with the terms of all licenses.
- I will not install on DPSAC equipment unauthorized software, including software available for downloading from the Internet, software available on DPSAC networks, and personally owned software.

Internet and E-mail Use

- I understand I may not access NIH Webmail from the public Internet.
- I understand I may not auto-forward from an NIH email account.
- I will not provide personal or official NIH information to an unsolicited email.
- I will only disseminate authorized NIH information related to my official job and duties at NIH to internal and external sources.

Teleworking

If I am approved for teleworking at any alternate workplace, I 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 laptops I use for teleworking when they are not in use.
- I will protect sensitive data at my alternate workplace.

Laptop Computers and Portable Electronic Devices

Use of DPSAC laptop and desktop computers are subject to the following additional rules of behavior:

- I will use only DPSAC laptops or desktops to access DPSAC systems and information.
- I will always keep Government Furnished Equipment (GFE) under my physical control.
- I will take all necessary precautions to protect GFE against loss, theft, damage, abuse, and unauthorized use by employing lockable cases, and keyboards and locking cables.
- I will keep antivirus and firewall software on the laptop up to date.
- I will use only DPSAC-authorized internet connections that conform to DPSAC security and communications standards.
- I will not make any changes to a laptop's system configuration unless I am directed to do so by a DPSAC system administrator.
- I will not program the laptop with sign-on sequences, passwords, or access phone numbers.
- I will not connect personal electronic devices to GFE for any purpose (e.g. charging).

Strictly Prohibited Activities while using DPSAC Systems and Equipment

- I will not engage in unethical or illegal conduct (e.g. pornography, criminal and terrorism activities, and other illegal actions and activities);
- I will not forward email spam, inappropriate messages, or unapproved newsletters and broadcast messages except when forwarding to report this activity to authorized recipients;
- I will not engage in outside fund-raising, endorsing any product or service, lobbying, or engaging in partisan political activity.
- I understand and will comply with the requirement that sensitive information processed, stored, or transmitted on wireless devices must be encrypted using approved encryption methods.

Incident Reporting

- I will within one (1) hour of occurrence/discovery, notify the NIH IT Service Desk and the NIH Information Security Program to report:
    - All security incidents (e.g., actual or potential loss of control or compromises (whether intentional or unintentional, of your login name and password), PII and other sensitive NIH information maintained or in possession of NIH or information processed by contractors and third parties on behalf of NIH).
    - Emails that request NIH personal or organizational information or ask you to verify NIH accounts or security settings.
    - Lost or stolen NIH-issued equipment.

Accountability

- I understand that I have no expectation of privacy while using any DPSAC equipment and while using DPSAC Internet or email services.
- I understand that I will be held accountable for my actions while accessing and using DPSAC systems and IT resource.

Acknowledgment Statement

I acknowledge that I have read, understand, and will comply with the above NIH DPSAC Rules of Behavior (ROB) dated January 31, 2021. Furthermore,

- I understand that violations of these NIH Rules or information security policies and standards may result in disciplinary action, up to and including 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 Rules must be authorized in advance in writing by the NIH Chief Information Officer or his/her designee.
- I also understand that violation of federal laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the NIH Rules draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

User's Signature	**Date**

Endnotes

[1] *NIH Information Technology (IT) General Rules of Behavior*. ocio.nih.gov/InfoSecurity/Policy/Documents/NIH%20IT%20General%20Rules%20of%20Behavior%20v2.0.pdf.

[2] "2811 - NIH Policy for Access to Information Technology Systems and Networks." *National Institutes of Health*, U.S. Department of Health and Human Services, policymanual.nih.gov/manage/chapter/view/2811.

[3] "2814 - NIH Policy on Remote Access." *National Institutes of Health*, U.S. Department of Health and Human Services, policymanual.nih.gov/manage/chapter/view/2814.

[4] "2810 - NIH Policy on the Prohibited Use of Non-Government Furnished (Non-GFE) IT Equipment." *National Institutes of Health*, U.S. Department of Health and Human Services, policymanual.nih.gov/manage/chapter/view/2810.

[5] *NIH INFORMATION SECURITY (InfoSec) POLICY HANDBOOK*, 9 Jan. 2019, ocio.nih.gov/InfoSecurity/Policy/Documents/NIH%20InfoSec%20Policy%20Handbook_V5.0_Final_Signed.pdf.

[6] *Rules and Policies - Protecting PII - Privacy Act*, www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act.
Personally Identifiable Information (PII) The term "PII," as defined in OMB Memorandum M-07-1616 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual.

[7] "45 CFR § 160.103 - Definitions." *Legal Information Institute*, Legal Information Institute, www.law.cornell.edu/cfr/text/45/160.103.
Protected health information Protected health information means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years.