



CNCS Cybersecurity User and Privacy Training

FY2017



Aggregated Sources for PII

PII Aggregation: When two or more pieces of data can be combined to identify a unique individual

- Information from multiple sources enables an attacker to successfully distinguish and establish your identity, even though these pieces of information may not individually trace back to you. Some examples are:
 - **Website or IT information**
 - IP address
 - Cookies
 - Login name, screen name, nickname, and password
 - Email address
 - **Third-party related**
 - Health, insurance, treatment, or medical information
 - Criminal history
 - **Device related**
 - Location/GPS data
 - Network communications data
 - **Financial related**
 - Banking/credit card data

87% of the U.S. population can be uniquely identified using only gender, date of birth and ZIP code¹

Attacks on PII

Phishing (e-mail) or SMSishing (text message) attacks seek and exploit an individual's personal information by luring or tricking them into downloading malware and/or sending their personal information. Examples:

-----Original Message-----
From: Help Desk [<mailto:haywood@carlperkinscenter.org>]
Sent: Wednesday, July 20, 2016 1:00 PM
To: CNCS Employee <employee@cns.gov>
Subject: Scheduled Maintenance & Upgrade

Help Desk

Scheduled Maintenance & Upgrade

Your account is in the process of being upgraded to a newest Windows-based servers and an enhanced online email interface inline with internet infrastructure Maintenance. The new servers will provide better anti-spam and anti-virus functions, along with IMAP Support for mobile devices to enhance your usage.

To ensure that your account is not disrupted but active during and after this upgrade, you are required to kindly confirm your account by stating the details below:

- * Domain\user name:
- * Password:

This will prompt the upgrade of your account.

Failure to acknowledge the receipt of this notification, might result to a temporary deactivation of your account from our database. Your account shall remain active upon your confirmation of your login details.

We appreciate your patience as this maintenance is performed and we do apologize for any inconveniences caused.

Sincerely,
Customer Care Team

Note who is sending the email and from what organization.

Never provide account information in an email.

Help Desk will never ask you for your password.

No specific contact info provided for follow-up questions

Where is PII Stored at CNCS?

The following systems are approved to process and store PII:

- eSPAN (ESP)
- Grants Members Management (GMM)
- AmeriCorps Childcare Benefits System (ACB)
- Momentum (MOM)
- NCCC Health Benefits (NHB)
- VISTA Health Benefits (VHB)

The following systems can store limited amounts of PII but do not collect it:

- Network (GSS) to include any SharePoint/cloud storage

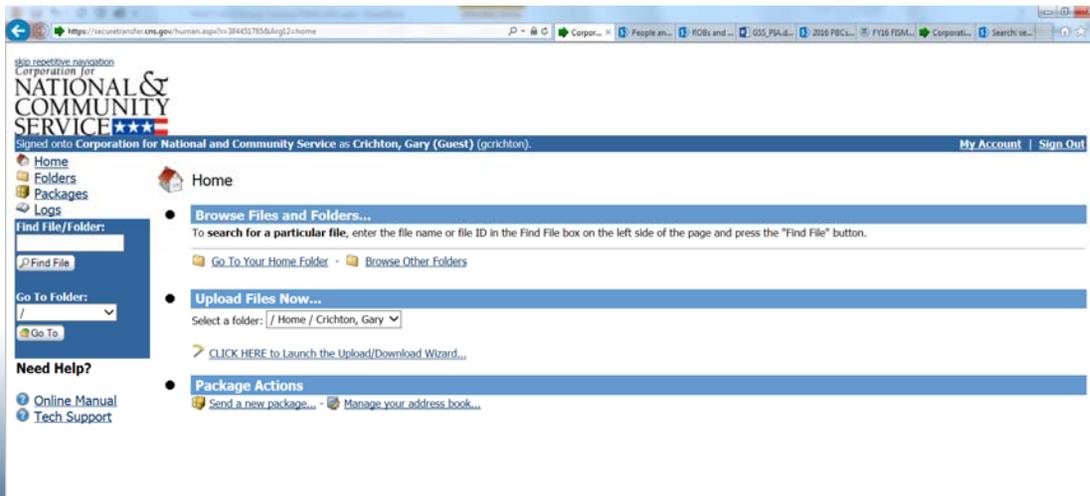
The following systems CANNOT collect, store, or process any PII:

- CNCS Public Websites (PUB)

Secure File Transfer

Secure File Transfer is a secure web portal that must be used when PII (or any sensitive data) needs to be sent to someone (or received from) outside the CNCS network

- <https://securetransfer.cnsc.gov/>
- Upload the file containing PII and designate the individual who can access the file



PII being sent outside the organization should follow guidance from your supervisor or the Chief Privacy Officer!

Creating Passwords

Using a Password Chart simplifies the process

- **Why should I use this spreadsheet password chart?**
 - Creating and remembering strong passwords can be very difficult
 - Using a password chart to convert a key-phrase makes it easier to create and use complex passwords
 - Creating passwords with this chart will meet the minimum CNCS standard
 - An enterprise-wide password change can be issued without having to relearn a new password. Just discard your old chart, print a new one, and continue using as accustomed

Password Chart					
a	b	c	d	e	f
N<4h	U2k!	t7D#	sU/7	d2*G	G,7o
g	h	i	j	k	l
Nm7>	y<F7	k<B9	C9z	!@#	n7C#
m	n	o	q	r	
Rq#1	u1S:	Ww	!L	k5M!	T<1k
s	t	v	w	x	
Ch9:	EY,	!V9	H8>f	a\$G1	Ca1:
y		0	1	2	3
V#3h	U.m6	a4U:	X.h9	oX.8	D3.y
4	5	6	7	8	9
y6#Y	j6Z<	Qo*2	a4U:	Sv7>	Eb>3

Location? [OIT->Cyber Public Documents->Cyber Training](https://cns.gov.sharepoint.com/sites/extranet/OIT/Cybersecurity/layouts/15/DocIdRe.dir.aspx?ID=25QQF44XQPZD-1045098590-41)
<https://cns.gov.sharepoint.com/sites/extranet/OIT/Cybersecurity/layouts/15/DocIdRe.dir.aspx?ID=25QQF44XQPZD-1045098590-41>

Prevent Tailgating

Ensure only authorized people are allowed access to your workspace; all unauthorized people are denied access

- Do not let unknown people through locked doors or elevators
- Direct guests to front desk or guard for assistance
- Request identification
- Contact the person being visited to provide an escort



Insider Threat

What is an Insider Threat?

- Typically described as a disgruntled or unscrupulous employee trying to gain access to information they shouldn't and sharing it for personal gain, espionage, or revenge
- Current or former employees or contractors who
 - Intentionally exceeded or misused an authorized level of network, system, or data access in a manner that affected the security of the organizations' data, systems, or daily business operations



What to look for?

- Mood changes or mood swings
- Change in routine
- Frustration with company or co-workers
- Change in productivity
- Questions about areas outside of their direct function

Contact the Help Desk if you notice suspicious behavior.

Social Engineering

Be cautious of social engineering



If someone calls or emails asking for sensitive information,
it's okay to say **NO**

Call the company directly to verify credentials before giving out
any information

Stop. Think. Connect. Before you...

....Click, Open, or Download

Attachments or links in email can contain malicious software. If unexpected or suspicious, simply delete it



.... Plug something into your computer

Malware can be spread through infected flash/USB drives, external hard drives, and even smartphones



....Connect to WiFi spots

Check to be sure site security is enabled and that the CNCS VPN is being used

Contact the OIT Help Desk Immediately

Contact the OIT Help Desk
202-606-6600; OITHD@cns.gov



Immediately contact them when.....

- Your laptop or iPhone has a suspected malware or virus infection
- PII has been lost, stolen, improperly handled, or disclosed
- You have accidentally responded to a phishing email
- Your laptop or iPhone is stolen or lost
- Anytime your Government Furnished Equipment (GFE) is behaving out of the ordinary

CNCS Cybersecurity User Rules of Behavior

Introduction

What is the Purpose of the Cybersecurity Rules of Behavior?

The intent of the CNCS Cybersecurity Rules of Behavior (ROB) is to provide guidance for all CNCS employees, contractors, interns/temporary employees, and volunteer personnel working for CNCS concerning information and personal security and to obtain written certification that personnel have read and understand these Rules of Behavior. Everyone plays a major role in preventing security vulnerabilities that can lead to system compromises and hinder our mission or facilitate unauthorized disclosure of sensitive information. An individual's actions can affect the security of CNCS information and information technology (IT) systems. Knowledgeable users are the foundation of a successful Cybersecurity program.

Who is Covered by the Rules of Behavior?

The Rules of Behavior extend to all CNCS federal employees, contractors, interns, temporary employees, and volunteers using CNCS IT systems or accessing CNCS information under formally established agreements. Users must be fully aware of, and abide by, the Rules of Behavior and CNCS Cybersecurity policies.

What is Sensitive Information?

Sensitive information contains data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization. Protection of sensitive information may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for business/proprietary considerations. Some examples of sensitive information include the following: medical, procurement, budget, system/application vulnerability, and personally identifiable information (PII). Sensitive information must be protected against loss, disclosure, or alteration because of the risk and magnitude of harm that could result.

What is Personally Identifiable Information (PII)?

The term PII refers to any data field that could potentially identify a specific individual, either by itself or when combined or linked to other identifiable information. PII must be protected from disclosure. The following are examples of PII:

- Name and at least one other piece of information that links back to one specific person
- Social Security Number
- Date of birth
- Place of birth
- Fingerprints
- Non-business phone numbers, emails, and addresses
- Photos
- Mother's maiden name
- Passport number
- Driver's license number
- Taxpayer identification number
- Bank account information
- Credit card numbers.

PII includes any other information that is linked or linkable to an individual's identity, such as:

- Medical
- Educational
- Financial
- Employment.

User Rules of Behavior

PII - Access Restrictions and Protections

- ❑ I will access PII only as needed to complete authorized CNCS work and in accordance with CNCS Privacy Policy.
- ❑ I will ensure there is no unauthorized sharing of either verbal or written PII, (e.g., in response to links in emails, queries on websites, questions asked).
- ❑ I will not save PII to non-CNCS equipment including when accessing PII via the CNCS virtual private network (VPN), mobile devices, or any other means.
- ❑ I will ensure that written or verbal PII is disclosed only to recipients who have a need to know, and are authorized to handle and process it.
- ❑ I will minimize the collection and use of PII in performance of my official duties.
- ❑ I will not attempt to gain unauthorized access to systems or information (including PII).
- ❑ I will protect PII as described in CNCS Privacy Policy, the CNCS Privacy SharePoint Page, and the CNCS Cybersecurity User Training.
- ❑ I will use Secure File Transfer (available via the CNCS portal, <https://securetransfer.cns.gov/>), rather than email, for distributing documentation with PII to recipients outside of the CNCS network; (i.e., recipients with an email address not ending with '@cns.gov').
- ❑ I understand that I may share PII or other sensitive information with people outside the CNCS network only when:
 - The information is needed to complete official CNCS business – for questions, contact your supervisor, records management, Chief Privacy Officer (CPO) or Cybersecurity.
 - The information is sent using Secure File Transfer or is retained in an authorized CNCS Records Management System such as SharePoint/OneDrive, using controlled access privileges.
- ❑ I will protect PII on my mobile devices. I understand that I must **not** send to or store CNCS sensitive information or PII on non-Government Furnished Equipment (GFE) devices (e.g. personal smartphones, tablets, etc.).
- ❑ ***I will use 'Secure Print' and remove the hard copy from the machine after the print job is complete.***
- ❑ I will immediately dispose of hard copy that has PII or other sensitive information when it is no longer needed; for disposal, I will place it in the designated locked containers in copy rooms for secure shredding.
- ❑ I will not disclose any PII contained in any system of records, except as authorized by applicable laws, regulations, or CNCS policies.

Access to the CNCS System

- ❑ I understand that I will be held accountable for my actions while accessing CNCS systems.
- ❑ I will complete the new employee training and all other the mandatory CNCS Cybersecurity training within the specified timeframes. I understand that not completing training will result in the loss of access to CNCS information and information resources.
- ❑ I agree to become familiar with and abide by all Office of Information Technology (OIT) policies and the Records Management Policy.
- ❑ I understand that I am only authorized access to systems required to perform my official duties.
- ❑ I understand that I have no expectation of privacy when using any GFE and accessing any CNCS information systems. All of my communications, searches, and instant messaging (i.e. Skype/Lync), may be monitored, logged, or audited.

Cybersecurity User Rules of Behavior

- I understand that by accessing and logging in to the CNCS network, I am consenting to the monitoring of my activities.
- I will connect to CNCS systems only through the following approved methods:
 - Using CNCS-issued equipment or GFE
 - Using a CNCS token with a non-CNCS workstation via the CNCS VPN.
- I understand the Rules of Behavior apply to all CNCS systems; including the CNCS Guest Wireless Network.

Acceptable Use

- I understand government resources such as email, instant messaging, SharePoint, texting, photos, or any other communication methods should not be used for inappropriate or illegal activities; including but not limited to the following:
 - Sexually explicit/oriented content or anything that is in violation of sexual harassment or hostile workplace laws
 - Ethnic, racial, sexist, or other offensive comments
 - Fraud or gambling
 - Illegal weapons, terrorist activities, or the planning or commission of any crime
- I understand that accessing such prohibited activities through intermediary accounts (e.g., personal email or home Internet service providers) does not affect the prohibition. If I am using a government computer or accessing a government network, I may not engage in prohibited activities at *any time*.
- I will refrain from engaging in inappropriate IT activity (e.g., accessing peer-to-peer (P2P) music/file sharing sites; clicking on questionable hyperlinks in email or unfamiliar websites; visiting questionable websites) that could increase the exposure of the CNCS network and all of its users to viruses and malware from malicious sites.
- I will periodically review the My SPAM Report, quarantined email, and other sources provided to monitor the security status of my CNCS emails.
- I will refrain from using CNCS network resources for non-work related reasons (e.g., audio/video streaming, storing non-CNCS data on CNCS systems, etc.).
- I understand that GFE and services are to be used for official business; GFE includes, but is not limited to, the following: workstations, laptops, mobile phones, mobile hot spots, printers, copiers, and external hard drives. Limited personal use of government IT equipment and services is permitted when use:
 - Is not illegal, inappropriate, or offensive to others.
 - Is conducted on the employee's own time with little or no impact on employee productivity.
 - Does not incur any additional expense to the government (e.g., calling 411 on GFE phones except in emergency situations.)
 - Is in accordance with the CNCS Mobile Device Policy.

Passwords and Other Access Control Measures

- I will not use account credentials that belong to someone else.
- I understand that I am responsible for all activity that occurs under my CNCS user account.
- I will choose strong passwords (minimum number of characters required by CNCS with numbers, special characters, upper/lower case letters, and no dictionary words) and take the necessary precautions to protect my account.
- I will change my passwords (to other strong passwords) at least as often as required.
- I will protect passwords and access numbers from disclosure.
- I will not store passwords in an unsecure manner or on unencrypted devices.

Cybersecurity User Rules of Behavior

- I will not share my access with or disclose my account passwords to anyone. I will immediately report attempts to obtain this information (e.g., phone call, phishing¹ email) to OIT Help Desk via email (OITHD@cns.gov) or phone call (202-606-6600).
- I will protect any token or Personal Identity Verification (PIV) card and immediately inform OIT Help Desk via email (OITHD@cns.gov) or phone call (202-606-6600); if it is lost or stolen.

Information Protection (electronic and hardcopy data)

- ***I will lock the session on my workstation or laptop computer whenever I step away.***
- I will abide by this Rules of Behavior agreement when accessing CNCS information systems in any manner (via CNCS VPN, personal computer, any CNCS wireless service, etc.).
- I will protect all PII from unauthorized disclosure, modification, or destruction.
- I understand that the Bitlocker tool will force encryption of removable storage media (e.g., USB drives, portable hard drives, memory cards).
- I understand that CNCS information stored on local drives is not backed up, so information must be saved to appropriate backup locations.
- I will use my official CNCS email account and other CNCS-approved communications options (e.g. Lync, Skype) to transact agency business. (See items under *Records Retention* below.)
- I will store electronic files containing sensitive information or PII data in properly secured folders that only allow access to those with a need to know. I will not store or distribute sensitive information or PII data on unapproved systems (e.g., Google Drive, Dropbox, Box, etc.).
- I will ensure that all hard/soft copy of PII are stored in a secured location for a length of time in accordance with the approved CNCS record retention schedule(s); then disposed of properly.

Government Furnished Equipment and Telework

- I understand these Rules of Behavior apply when working offsite.
- I will not modify the configuration of any GFE computer or tablet without permission from OIT.
- I will take precautions to protect government property (including badge or PIV card) and secure government information and information resources in my possession from unauthorized disclosure, theft, destruction, or misuse.
- I will take all reasonable steps towards safeguarding GFE (e.g., not leaving a device, badge, or PIV in plain sight in an unattended vehicle, etc.) when outside of my work location.
- I will dispose of media (hard copy and electronic) using approved means of destruction.
- When teleworking, I will follow security practices that are equivalent to those required of me at my primary workplace.
- I will not store sensitive data in non-GFE at alternative work sites.
- I understand that laptops, mobile, tablets and small items are subject to theft and I will protect them to the best of my ability.
- I will immediately report the theft or loss of any IT-related asset (including my badge or any token) to OIT Help Desk via email (OITHD@cns.gov) or phone call (202-606-6600).

¹ Phishing is a dishonest electronic communication attempt (i.e., an email, a link on an untrusted website) to obtain sensitive information such as usernames, passwords, and/or credit card details by masquerading as a trustworthy entity.

Cybersecurity User Rules of Behavior

Incident Reporting

- Evidence of an incident may be as subtle as a device acting erratically; therefore, I will report any unusual behavior immediately.
- I will promptly report any suspected incidents or actual violations of CNCS security and/or privacy policies via email (OITHD@cns.gov) or phone call (202-606-6600).

Records Retention

- I understand my obligation to retain records as defined by the CNCS Records Management policy. A record is defined as any material, physical or electronic, made or received by you in connection with the transaction of public business. Records reflect the transaction of agency business by documenting agency functions, policies, decisions, procedures, and/or transactions. Transacting agency business generally does not include logistical, scheduling, or administrative communications.
- I will use my official CNCS email account and other CNCS approved communications options (e.g. Lync, Skype) only to transact agency business. I will not routinely use any unofficial electronic messaging account (i.e., your personal email account or any text message account) to transact agency business, and never send sensitive information or PII via any unofficial electronic messaging account. When I cannot use my official CNCS email account to transact/email agency business, I understand that the Federal Records Act requires that I must either copy my official CNCS email account on the message or forward a complete copy of the record to my CNCS email account within 20 days of transmitting the record.

Supervisors and Contracting Officers' Representatives (CORs)

- I will ensure that all individuals for whom I am responsible complete all CNCS required privacy and security training.
- I will ensure that all individuals for whom I am responsible are made aware of the specific security requirements for protecting information (e.g., privacy, procurement, budget, paper copies, etc.) and information systems as part of their job performance.
- I will ensure the timely completion of all on-boarding and off-boarding activities (including documentation of transfers) using the appropriate system(s).

Penalties for Noncompliance

Users who do not comply with the Rules of Behavior are subject to penalties that may be imposed under federal law. These penalties include the following:

- Written reprimands
- Reimbursement to the government for unauthorized charges
- Suspension of system privileges
- Temporary suspension from duty
- Removal from current position
- Termination of employment
- Criminal prosecution

Rules of Behavior for Cybersecurity User and Privacy Training

My signature certifies that I have completed the Corporation for National and Community Service Cybersecurity User training. I have read and understood the Cybersecurity User Rules of Behavior Agreement. I understand that violation of these rules could result in administrative punishment and/or criminal prosecution.

Print Name: _____

Department/Company: _____

Print CNCS Username (if known): _____

Signature: _____ Date: _____

Please print and sign this signature page and then scan and email it to cybersecurity@cns.gov.