CLASSIFIED GENERAL USER COMPUTER TRAINING

THE SECURITY TEAM

The different roles within the classified computing security team are shown below. These team members ensure we maintain a successful classified computing capability at Northrop Grumman.

Cyber Information System Security

- Information System Security Manager (ISSM)— Responsible for Information Assurance (IA) on the program's information systems. The ISSM is appointed by the FSO, CPSO, or CSSO.
- Information System Security Officer (ISSO)—Responsible for the everyday IA security of the program's information systems and is the technical interface between the program and ISSM.
- For Special Access Programs (SAP), the ISSM/ISSO is appointed by the Information system owner (ISO)/Program Manager (PM).

IT Support

System Administrators (SysAdmins) respond to all system and network issues and create and unlock all program user accounts.

Industrial Security

- Collateral Facility Security Officer (FSO) or Site Security Manager—Responsible for supervising and directing security measures at the facility.
- SAP Contractor Program Security Officer (CPSO) or Site Security Manager—Responsible for supervising and directing personnel and physical security measures at the facility.
- SCI Contractor Program Security Officer (CPSO)/Contractor Special Security Officer (CSSO) or Site Security Manager—Responsible for supervising and directing personnel and physical security measures at the facility

WHAT IS AN INFORMATION SYSTEM?

An information system is computer hardware, software, and firmware used to manipulate, store, or send data and information.

A classified Information System is an information system configured and authorized to display, process, and store classified data.

An Information System includes but is not limited to:

- Computers
- Test equipment
- Printers
- Laptops
- Media/thumb drives/memory sticks
- Network equipment

SYSTEM AUTHORIZATIONS

All classified information systems must be authorized for classified processing, including all hardware and software. Any modifications must be approved and recorded in the authorization documentation.

Modifications can only be performed by cleared, trained, and assigned personnel. Some modification might require re-authorization before use. Each system is approved for a specific program or set of programs.

- Segregated by program and need-to-know.
- Program-specific information and media cannot be moved between systems without prior customer approval.

See your Information System Security Manager (ISSM) for specific authorization documentation.

ACCOUNT TYPES AND ROLES

There are three basic account types that include specific roles.

General Users Accounts

- Have the approval to view, input, modify, receive, and transmit information on approved information systems.

Privileged Users Accounts (each role requires a separate briefing)

- Auditors
- Data Transfer Agents
- Administrators (System, Network, Database, etc.)

Group Accounts

- Group Accounts must be approved by the Authorizing Official. See ISSM for additional details.

SYSTEM ACCESS REQUIREMENTS

The criteria and requirements needed to obtain a general user computer account are:

- Validated need-to-know.
- Completed initial general user training or annual general user refresher training current within one year.
- Signed General User and Acknowledgement Briefing on file with the ISSO/ISSM.
- Completed Classified Information Systems Account Request (CISAR) form.
- Derivative Classifier training, if required
- Customer-provided mandatory training, if applicable
- Program security briefing, if applicable

When your account is no longer required, contact ISSO/ISSM.

PASSWORD REQUIREMENTS

The requirements for password minimum length and complexity vary based on the program or environment. Contact your Information System Security Officer or Information System Security Manager for specific requirements.

Examples of required elements for your classified computer system password are:

- Uppercase letters
- Lowercase letters
- Numbers
- Special characters
- New passwords must differ by at least 4 characters from the previous password

Some do’s and don’ts when handling your password are:

Do’s:

- Report discovery of unauthorized use, possession, or downloading of a password cracking tool to the ISSO or ISSM.
- Immediately report suspected misuse or compromise of a password to the ISSM.
  - Accidental entry of password in the username box
  - Account lockout

Don’ts:

- Do not use the same password for different information systems.
- Do not use the same password to access accounts with different permission levels on the same system.

- Do not write down passwords or store passwords electronically.
- Do not share passwords with anyone.

The ISSM will direct password changes required in response to a compromise or other incident, if necessary.

COMPUTER MONITORING AND USE

Users must acknowledge the consent to monitor warning banner before accessing the system. System monitoring supports the company's Insider Threat Program and includes:

- Logon date, time, and system utilized.
- File access attempts.
- Resource usage. As well as other activities as appropriate.

Remember:

- "Misuse of computer systems" is one of the criteria used in adjudicating approval and/or revocation of security clearances.
- Classified systems are not for personal use.
- Users must lock classified workstation when they are away from desk.
  - When in doubt, lock workstation!
- Users must log off the system at the end of each day.
  - If access is required for overnight processing, the ISSO/ISSM must grant permission.

PROHIBITED ITEMS – PORTABLE ELECTRONIC DEVICES

A Portable Electronic Device (or PED) is any easily transportable, personally owned or government or contractor-issued electronic device that has the capability to record, copy, store, or transmit data, digital images, video, or audio.

The items below are prohibited from entering closed or restricted areas unless permitted by the governing security personnel.

Examples of a PED include but are not limited to:

- Pagers
- Laptop computers
- Cell phones
- Radios (AMFM, satellite)
- Compact disc players, cassette players, and recorders

- Personal digital assistants (e.g., palmtops, BlackBerrys, iPads)
- Digital audio devices (e.g., MP3 players, iPods)
- Cameras
- Camcorders
- Calculators
- Electronic book readers (e.g., Kindles, Nooks)
- Digital picture frames
- Smart watch and fitness trackers

Check with your Security Team for specific guidance on medical devices.

HARDWARE/MEDIA MARKING

Each user is ultimately responsible for the marking, handling, and storage of media and paper documents in their area.

All media and paper documents must be appropriately marked and protected.

Security markings will be displayed on the following, but not limited to:

- All servers
- All server racks/cabinets
- Desktops
- Laptops
- Removable hard drives
- Externally attached hard drives
- Internal hard drives
- Monitors
- Printers
- Thin clients

Notify someone from the Security Team immediately if you notice items not marked or stored correctly.

HARDWARE/MEDIA SANITIZATION AND DESTRUCTION

All classified hardware must be sanitized or destroyed before removal from classified program areas. All classified media must be destroyed when no longer needed. Contact your Industrial Security team for guidance regarding destruction and updating the tracking of that material.

Sanitization is the process of removing information from storage devices or equipment such that data recovery is prevented.

- Removal of data from the storage device
- Removal of all labels, markings, and activity logs

Destruction is the process of physically damaging media so that it is not usable and there is no known method of retrieving the data.

- Degaussing, incineration, shredding, grinding, embossing, chemical immersion, etc.
- Do not remove any hardware, media or anything without security approval.

INTRODUCTION OF MEDIA TO CLASSIFIED SYSTEMS

Introducing media into a classified system requires close attention and compliance with that particular concept of operations. Contact the ISSO or ISSM for any site or program specific details.

When introducing media (e.g., CDs, DVDs, flash media) to classified information systems:

- Follow local procedures (data transfer, ConOps, etc.)
- Scan media with approved antivirus software.
- If require, close/write protect CD/DVD sessions

MEDIA ACCESS AND STORAGE

All digital media must be authorized and scanned for viruses prior to use within classified program areas. In addition, media must be labeled to indicate its classification level, including unclassified and blank media.

Media must be labeled to indicate its classification level, including unclassified and blank media.

Users must secure all media (electronic or paper), regardless of classification, when leaving the work area and/or at the end of the workday, as required for that area.

- GSA-approved safe for classified media
- Lockable cabinet for unclassified media

Users are responsible for setting access control rights to files they create, if needed to protect the data.

PRINTER SECURITY

Network and local classified printers are a potential security risk, since classified and unclassified pages could be commingled on printers.

CLASSIFIED PRINTER SECURITY

Classified printing should follow the guidelines as shown.

- Where possible, physical access to classified printers will be limited to only authorized personnel.
- Hardcopy outputs (print jobs) must be retrieved immediately from printer.
- Hardcopies must be marked appropriately.
  - Printouts will be marked with the highest level of the classified information contained within the document.
  - The overall marking of the document shall be conspicuously marked in the header and footers of the document.
- Any hardcopies left of classified printer must be treated as classified and properly destroyed.
  - Seek guidance from Security on destruction.
  - When in doubt, secure material in approved GSA safe.
- Printing reduces the vulnerabilities associated with electronic media and is the preferred method of data transfers.
- A comprehensive review of printed media must be performed by a subject matter expert before removal from the program area, if allowed.

SECURITY EVENTS AND INCIDENTS

Security events, incidents, and protentional threats to a system should be immediately reported to Industrial Security.

A security INCIDENT is an event that results in the damage or risk to the information system, or related operations.

Some examples of these types of occurrences are:

- Open safe
- Unsecured media
- Misuse of a classified system
- Improper marking or labeling
- Data spill
- Malicious code or virus
- Suspicious activity

INCIDENT RESPONSE

Incident reporting, response, and follow-up actions are critical to the continuing security of classified processing.

All personnel with access to the classified Information System (IS) are responsible for notifying their system responsible Security point of contact as soon as possible when an incident is suspected.

Industrial Security will immediately notify the cognizant Security Office of serious incidents such as the following:

- Incident posing grave danger to the United States or warfighters due to potential loss of information
- Access or compromise of classified or sensitive information
- Compromise originating from a foreign source

DATA SPILL INCIDENT (CODE BLUE)

Classified data is spilled when it is transferred to an unclassified information system or to an information system with a lower level of classification or access.

Code Blue is the unclassified name established by Northrop Grumman to describe the occurrence and remediation process used when government classified information is introduced into unclassified and other unauthorized Northrop Grumman information systems and/or media and portable devices within Northrop Grumman facilities. This response process is in place to minimize damage to the customer and mitigate loss of information.

How do data spills happen:

- Compilation of unclassified data
- Assured File Transfers from higher classification system to a lower classification system
- Receiving data marked at a higher classification than the system used to review data
- Updates to Security Classification Guides (SCGs)

If you suspect a data spill has occurred, immediately contact the Security Team at your site.

DATA SPILL CONTAINMENT

Containing the data spill should be your top priority. Follow the steps shown and actions as described in your system standard practices and procedures. If you are unable to reach your Security Team, contact the Cyber Security Operations Center.

Users should do the following to assist with containing the spill:

- Disconnect system from network (this may vary by site).
- Do not use workstations, servers, or mobile devices until Security has given permission.
- Do not forward contaminated information or attempt to delete it.
- Do not attempt to clean it up.
- Do not log into another system until cleared by Security.

When in doubt about what data is classified, contact your program lead or Program Security Manager.

For additional guidance on data spills, visit: Code Blue (sharepoint.us)

SUSPICIOUS ACTIVITY INDICATORS

All users must be aware malicious code and suspicious system activity indicators. Malicious code is software that does damage or creates unwanted behaviors. Some effects include modified, corrupt, or destroyed files, as well as compromise or even loss of information.

As always, report any suspicious system behavior to your Security point of contact.

Suspicious behaviors:

- Slow and/or abnormal system performance
- Anti-virus alert
- Random pop-up windows or screens
- Slow network performance
- Unresponsive web/file services
- Unexplained account lockout
- Unknown persons loitering within area
- Random phone calls asking for detailed information about you and the company

CONFIGURATION MANAGEMENT

Every information system has an established configuration control process for tracking and approving changes.

Any changes a user wants to make to an Information System must be approved in writing by the configuration control process and implemented by authorized information technology or system administrators.

Users are not authorized to:

- Add, move, remove, or modify system hardware, software, or firmware
- Modify security-related configuration settings
- Disconnect classified systems from the network

Contact ISSM/ISSO for details on change control process for your program.

SYSTEM SOFTWARE

If unclassified software is being developed internally or by a vendor for use on a classified system, the following must occur:

- All software must be approved, contact you ISSM for additional guidance.
- Internally developed software should be developed by cleared program personnel or have code reviewed by a cleared program person.

SYSTEM MAINTENANCE

All system maintenance must be coordinated through Security prior to occurring. A cleared company technician or cleared outside vendor technician must be used when possible. Uncleared technicians are used only as a last resort, and they must be a U.S. citizen. The uncleared technicians require a technically knowledgeable shoulder-to-shoulder escort while in the work area. Prior sanitization of work areas as well as the systems in question must be performed. Only use dedicated, unclassified media for maintenance. If the system has a fixed internal drive, restrict access to all input and output devices. Diagnostic equipment with internal storage may not be connected to a classified system without coordinating with the ISSM.

PHYSICAL ACCESS TO CLASSIFIED INFORMATION SYSTEMS

Classified computing systems are protected using a variety of measures and techniques. Following procedures ensures the ongoing protection of our nation’s sensitive information.

- All information systems are protected by physical barriers.
  - Access control systems
  - Combination locks
  - Alarm systems
- Only personnel with verified need-to-know, have met the clearance requirements, and have program access (if applicable) may have authorized physical access to classified information systems.
- Secure closed area/restricted areas:
  - If no authorized personnel are present in the area

  - If the room will be left unoccupied
  - At the end of scheduled workday
- Contact Industrial Security for more information.

RULES OF BEHAVIOR AND TECHNOLOGY PROTECTION

Below are the expected rules of behavior that will ensure the protection of the technology to which you have been granted access.

- Comply with all security measures necessary to prevent unauthorized disclosure, modification, or destruction of information.
- By accepting the warning banner, you consent to monitoring.
- The information system must not be used for personal benefit or privacy.
- Authenticators to the information system will be protected at the highest classification level of data processed on the system or network.
- Users must lock workstation or log off before walking away from system.
- Users must seek approval prior to conducting unattended processing.
- Users must follow all physical security procedures for opening, leaving, and securing closed area.
- Users will not introduce prohibited items into any classified area.
- Users must follow all processes when performing escorting duties for uncleared or non-program briefed personnel.
- Users must protect all data and outputs and contact an ISSO or ISSM immediately if any device is not marked appropriately.
- Users must not post work-related information on social networking or commercial websites.
- Users must never share information system account information.
- Users with elevated privileges must use local or remote access to perform authorized tasks or mission related functions only.
- Users will be responsible for all activity that occurs while logged into the system under their assigned user ID.
- Users will not attempt to “hack” the network or any connected information system.
- Users will not attempt to gain access to data to which they do not have authorization for.
- Users must read and sign the General User Acknowledgement of Briefing form before access to the information is authorized.

CONCLUSION

As a trusted user, you are responsible to protect all sensitive information.

- Only utilize systems to which you have been granted access.
- Protect information from unauthorized disclosure.
- Immediately report incidents to the Security Team.

CONTACT INFORMATION

If you have questions or comments, contact your local Security Representative.

If you cannot view this video on the Learning Exchange (LX), email the ESSS Training Group at ESSS_DoDTraining@ngc.com stating you have completed the Computer Security Specials training. In your e mail include:

- Your legal first and last name
- Your MyID
- Title of training completed: **Computer Security Specials**