ANNUAL COMPUTER SECURITY REFRESHER TRAINING

Northrop Grumman has a requirement to provide annual computer security training to all employees who have access to classified computing systems. This training will inform you of current policies and guidelines. It is provided to re-emphasize your continued responsibility for protecting classified information, Information Systems, and preventing classified data spills. As a reminder, some areas/sites may follow different requirements. If you have any questions about local policies and guidelines please seek guidance from your local Computer Security Representative.

INFORMATION SYSTEMS (IS)

What is an information system? An information system is computer hardware, software and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating or otherwise manipulating data, information and textual material. These systems include:

- Computers
- Test equipment
- Printers
- Laptops
- Electronic data managers
- Thumb drives/memory sticks
- Network equipment.

TERMINOLOGY

Below are terms used throughout this module:

**Information Systems Security Manager (ISSM):** Person responsible for an organization's information systems security program.

**Information Systems Security Officer (ISSO):** Responsible for the everyday security of the system; may be appointed for each individual IS.

- Technical interface between the program and the ISSM.

**System Security Plan (SSP):** Used to describe an IS and the necessary protections to allow the system to operate securely.

- Each network has at least one copy of the SSP available for all users.
- Some larger networks may have multiple copies throughout the area.
ACCESS CONTROL REQUIREMENTS

The following requirements must be met before you are granted a general user computer account:

Must be program briefed.

- Validated Need-to-Know.
- Completed initial general user information systems security training and annual general user refresher training current within one year.
- Signed General User Information System Acknowledgement Statement on file with the ISSO/ISSM.
- Completed Classified Information Systems Account Request Form.

The following are your responsibilities as a user:

- Logoff shared workstations if not in use for more than 15 minutes.
- Follow approved startup and shutdown procedures for periods processing systems (i.e. shared computer with multiple program removable hard drives) or systems with closed storage requirements.

SECURELY MANAGING COMPUTER SYSTEMS

Protect passwords, do not share or allow others to use your account. Unclassified passwords should never be written down or stored on files in the computer, per Northrop Grumman Corporate Procedure COR600 IT Device and Network Usage Compliance and Limitations. Customer policy discourages the writing down of classified passwords. If you must write it down:

- It must be marked with proper classification caveats,
- Sealed in an envelope,
- Marked eyes only,
- Attached with a classified coversheet; and
- Stored in a locked container which only you have access.

To minimize the need to share passwords, utilize file sharing by placing documents in a shared area. Maintain need-to-know protection by limiting access to shared areas. Report password compromises to Computer Security.

Lock your computer when you leave it unattended. It is not sufficient to wait for the automatic screen lock. At the end of the day, both classified and unclassified computers must be logged off or shut down. An unsecured computer is an open invitation for misuse.

To manually activate your screen lock you can use the following hot keys:

Windows NT, 2000
- Ctrl+Alt+Del then Enter

Windows XP, 7
• Ctrl+Alt+Del then Enter or
• Windows Key+L

MAC/UNIX/Other
• Call the Enterprise Solution Center or see your System Administrator for system specific procedure.

IS USER ACCOUNTS

There are two kinds of IS user accounts;

General users

• Have approval to input, modify, receive and transmit information on approved information systems.

Privileged users (i.e., System, Network and Database Administrators)

• Are those persons who have the authorization and accesses to change the configuration of the IS and administer the accounts and access right of General Users.

• Includes individuals who make changes to security relevant software.

  o A privileged user shall be cleared to the highest level of IS's accreditation and shall be the only person who may have access to those portions of the IS's hardware, software, or firmware that perform security functions.

  o Privileged users will have two accounts- one account as a general user and one account as a privileged user.

  o Must adhere to all general user requirements.

  o Notify and obtain approval from the ISSM or ISSO when making system changes or performing maintenance.

  o Privileged users have a greater responsibility than ordinary users to ensure they perform their duties in a secure manner.

GROUP ACCOUNTS

Group accounts are also sometimes referred to as shared accounts. These accounts are general accounts which multiple individuals have access to and are not tied to just one individual.

• Prior to being created, group accounts must be approved by the ISSO/ISSM and may need to be listed in the associated SSP and have received customer approval.

• Individual users must be pre-approved for access to a specific group account by a user's supervisor or their program management.

• When logging on and off of a group account, the user must complete the process for tracking group access. This may be a manual access log for that system which will be located in the area but can vary.
• Group accounts should not have administrator privileges. Some group accounts require additional certification per customer requirements. Speak with system ISSO/ISSM for system specific process.

COMPUTER USE AND AUDIT LOGS

Your use of classified program computers is monitored and audit logs are maintained.

• Program computers are for official program use only.
• Personal business on a classified computer may subject you to disciplinary action.
• All computer use is subject to monitoring.
  o Warning banner: “You are giving consent to monitoring every time you use a classified computer system”.
• Your computer activity is audited and the following information (at a minimum) is logged.
  o Date and time of your activities (logon, logoff, etc.).
  o Activities involved (file access attempts, software used, etc.).
  o System names where performing the activities (workstation, server, etc.).
  o Resources involved (network shares, printers, etc.).
• All software copyright laws and license agreements must be adhered to.
• "Misuse of computer systems” is one of the criteria used in adjudicating approval and/or revocation of security clearances.

STEPS TO INTRODUCING UNCLASSIFIED CDS

1. Create unclassified CD on a NGGN computer
2. Finalize CD with appropriate software (Roxio, Sonic, Sophos Close Disc Utility) and virus scan the CD.
3. Label CD accordingly
   1. "UNCLASSIFIED" (include NG Proprietary Level I or II as appropriate)
   2. Title
   3. Your name, organization/zone, telephone
   4. Date
4. Follow program procedures for upload and destruction.

See your requisite Security Representative for any site/program specific details.
PERSONALLY OWNED HARDWARE, SOFTWARE AND MEDIA

Personally owned hardware, software and media are prohibited in classified areas, see CTM J100 Company Security Manual. Examples of these include, but are not limited to.

- PDAs, thumb drives, digital music players. Check with your Security representative for specific guidance on these types of devices.
- Personally burned CDs and DVDs
- Personally owned photographic, video, and audio recording equipment
- Two-way radios or two-way pagers
- Cell phones (unless approved by the owner of the particular area)
- Laptop computers (unless approved by program security)
- Cameras and film (unless approved by program security)
- Commercial music CDs, CD players, and radio rules are defined by each program customer.

Seek guidance from program security or ISSM for specific policy exceptions.

MEDIA MARKING AND STORAGE

- All media must be labeled to indicate its classification level.
- All unmarked media is assumed to be classified and must be protected at the highest classification level of information processed in the area until reviewed by a knowledgeable person.
- Each user is responsible for any media they create.
- Do not co-mingle unclassified and classified program media.
- Store in unclassified and classified media separate containers or different folders within same container.

PRINTER SECURITY

Networked and local classified printers are a potential security risk. Since classified and unclassified pages may be co-mingled on classified printers, a compromise of classified information may occur.

Review every page printed on a classified printer prior to removal from the classified area. Classified material must be marked appropriately. During audits the customer will check for classification markings on the header and footer and portion marking throughout classified documents. Use appropriate cover sheets for all your printouts. Cover sheets should be stored near printers. Before leaving the classified area, Security must review all technical/program related printouts.
To prevent classified or proprietary information from being inadvertently printed after hours, classified printers are to be turned off or the paper tray pulled out as part of the security monitor checklist. To recycle toner cartridges, print one sheet of unclassified text and send to the recycling center.

Printers must be sanitized by IT Solutions before removal. Multi-Functional Devices and printers with internal hard drives must be registered, labeled and follow the same sanitization procedures as classified computers.

All unmarked printed material is assumed to be classified and must be protected at the highest classification level of information processed in the area until reviewed and marked by a knowledgeable person.

If classified material cannot be marked during printing, mark the material as soon as practical. Output must be protected from unauthorized access.

**DATA SPILLAGE**

A data spillage/system contamination, also called a Code Blue, occurs when classified information is introduced onto a system that is not approved for that level of information. In the event of a potential or confirmed data spillage of classified information either found on an unclassified computer, received via email, or uploaded to a collaboration system or file server, taking the appropriate actions as soon as the spillage is identified can contain the data and minimize further compromise.

- Do not delete or alter the file, attempt cleanup or use the system until cleared by security.
- Immediately contact Computer Security (ISSO/ISSM) or your Security Manager
- Do not forward the material to anyone, including Security
- Provide the name and phone number, Sector, whether it is a standard or restricted spill, date and time, type of system involved (Email, file share, desktop)

Disconnect any external connections and secure the computer. This may require moving it to a secure area or remain with the computer at all times until Computer Security provides additional guidance.

**As part of the cleanup, assist security by:**

Determining the origin of the file - Portable media, email or from a shared folder on a server?

Determining if the file has been shared or distributed - Has the file been sent as an email, uploaded to a shared space or saved to the hard drive?
When in doubt about what data is classified, see your program lead or Program Security Manager. If you suspect a virus is on a classified system, contact Computer Security immediately.

For additional guidance on data spillages visit: https://ess.myngc.com/Security/Pages/CodeBlue.aspx.

INCIDENT REPORTING

Report suspected or actual computer security incidents:

- Unauthorized access
- Fraud, waste, and abuse
- Non-compliance with computer security policy
- Misuse of Information Systems (workstation used for personal business or malicious intent)
- Allowing a non-program briefed individual to access a program system
- Not protecting computer media (CDs, DVDs, hard drives, etc.)
- Improper labeling or retention of computer media.

IS USER RESPONSIBILITIES

As an IS user you have certain responsibilities

- Attend logged-on systems at all times.
- When unattended, the screen must be locked. All classified media in use must be attended at all times.
- Never allow an uncleared person physical or visual access to a classified system.
- Monitors must be positioned to prevent unauthorized individuals from viewing information.
- Read the System Security Plans (SSPs) and know where they are located.
- You affirm your responsibility every time you logon to a program Information System and consent to monitoring (logon warning banner).

SUMMARY OF RESPONSIBILITIES

- Northrop Grumman computer and network resources are provided for Northrop Grumman business purposes only. Employees have no expectation of privacy while using Northrop Grumman computer resources. Northrop Grumman may monitor use at its sole discretion.
- Access to a classified Information Systems (IS), hardware, firmware or software is
restricted to authorized and briefed personnel. Review all information for need-to-know and proper classification before sending to others.

• Never introduce classified information or media onto an unclassified system.
• Computer systems to be used for classified processing must be approved by the ISSM prior to processing. Coordinate all location, status and configuration changes with Information System Security.
• Sharing of individual passwords is prohibited. Group accounts may be approved on a limited basis. When logged on, each user will ensure protection of the computer screen and printer output from unauthorized access.
• No software will be introduced or used on any classified computer without prior coordination and approval from the ISSM. Always coordinate approval prior to purchasing software intended for use on a classified system. All software copyright laws and license agreements must be adhered to.
• Label all media properly PRIOR to use. Secure media before you leave your work area.
• Never remove any classified computer hardware without PRIOR authorization. Always inform the ISSM and/or ISSO prior to a hardware change.
• Report all suspected security incidents such as a malicious code or virus, misuse, violation of system security, unprotected media, improper labeling and data spillage (e.g. classified data on unclassified systems) through the appropriate channels.
• After Hours - contact the Cyber Security Operations Center (CSOC) at 877-615-3535
• Contact the ISSO when you no longer need access to a classified system.

SCIF REMINDERS

• It is your responsibility to know the classification of the information that you are putting on the system.
• No devices with Wi-Fi, Bluetooth, or wireless transmitting abilities are permitted.
• Do not use the same password on multiple systems.
• Commercially produced music may be allowed in the classified area but is prohibited from being played in Company/Government equipment.
• Personal music players may be allowed in the classified area, but must not have recording, wireless, or Bluetooth capabilities.
• Personally owned hardware, software, and media are prohibited in classified areas
• Each user is responsible for any media that they create
• Do not mingle Unclassified and Classified program material
• Mark all classified printed material with the proper classification, headers, and footers on all pages
• Please see your requisite security representative for any site/program specific details.
This portion of the computer security refresher module covers DoD specific information.

**RESPONSIBILITIES**

There are three groups or people responsible for the overall protection of the IS:

**Defense Security Service (DSS)**
- Cognizant Security Authority.
- Oversees all contractor facilities in support of the DoD and other agencies.

**Information System Security Manager (ISSM)**
- Primary point of contact for all matters regarding the processing of classified information on an IS.
- Publishes a Master System Security Plan (MSSP) or a System Security Plan (SSP) for all ISs to be used for classified processing and obtain the accreditation from the DSS who is the designated approving authority (DAA).

**Information System Security Officer (ISSO)**
- Responsible for the everyday security of the system.
- Technical interface between the program and the ISSM.

**SYSTEM AND NETWORK APPROVALS**

All systems (including servers and workstations) must be certified prior to being utilized for classified processing.

Only DSS can certify systems. DSS may grant the ISSM self-certification authority for like systems.

- "Like" systems refers to systems which utilize the same operating system and security software as a system which had previously been inspected and approved by DSS.

Approval is granted based on a specific software and hardware configuration.

Any modifications must be recorded in the System Security Plan and can only be performed by cleared, trained and assigned personnel.

Each system/network is approved for a specific program or set of programs.

- Segregated by program and need-to-know.
- Are not interconnected.
• Program specific information and media cannot be moved between them without prior customer approval.

SYSTEM ACCESS – USER AUTHENTICATION

Password requirements

• 14 characters and at least three of the following:
  o Numbers
  o Uppercase
  o Lowercase
  o Special characters.
• Changed every 60 days or when compromised.
• Should not use dictionary definable passwords.

Passwords on classified systems must be protected at the same level as the system.

• May not be written down.
• May not be shared.
• Passwords should be unique across all of your user accounts, across all systems utilized.

Passwords to approved group accounts must be issued by an ISSO.

TRUSTED DOWNLOAD

Trusted download is the process of transferring a file from a classified system to unclassified/lower classified media.

• All users who need to perform trusted downloads must be authorized in writing by ISSM or their designee.
• An administrative record of each trusted download action will be generated and retained.

Media/electronic files: The following file formats are authorized by DSS to be released from the IS at or below the IS's accreditation level without an acknowledgement of risk from the government customer, but only after a comprehensive review:

• ASCII
• .html, .htm
• .jpg, .bmp and .gif
DATA TRANSFER

Data Transfer Policy involves the transfer of classified information from one classified system to another classified system (at the same level or higher) with the use of removable media. Examples include:

- Secret information moved to a Secret system
- Secret information moved to a Top Secret system

The number of users approved to perform data transfers using removable media should be kept to a minimum.

- The best practice would be to keep the total number of users approved to perform data transfers to 10%. However, the number of users approved per system is ultimately left to the local ISSMs discretion.

DOD CLOSED AREA RULES – MEDIA AND HARDWARE MARKING

- All media in closed areas must be marked, including unclassified, blank and personal media.
- Vendor media that retains original vendor labeling is considered unclassified.
- All equipment (capable of containing data) in closed areas must be marked to indicate security status, including company property from other sites and approved personal equipment.

SYSTEM SOFTWARE

All software must be licensed and acquired from reputable and authorized sources only:

- Approved vendors, Government Furnished Equipment (GFE), in-house developed.
- Personally-owned software is prohibited.

Restrictions on shareware, freeware, open source software and software from foreign sources:

- Must be tested for malicious code prior to receiving approval from ISSM/ISSO.
- Does not apply to routine software upgrades already stipulated in approved SSPs. (e.g., Anti-virus signature updates, etc.).
- Must be installed by an authorized privileged user after approval is granted by the ISSM.

Software Development

- If unclassified software is being developed internally or by a vendor for use on a classified system the following must occur:
  - Coordinate with Security first as there may be concerns regarding the development of the software.
The individuals developing the software must have a clearance to the level of the system that the software will be put on.

- If that is not possible, the software will be reviewed and tested by a cleared and knowledgeable person prior to being installed on the classified system.

### SYSTEM MAINTENANCE

All system maintenance must be coordinated through Security prior to occurring.

Must use a cleared technician when possible:

- Cleared company technician
- Cleared outside vendor technician

Uncleared technicians:

- Use only as a last resort
- Must be a U.S. Citizen
- Requires a technically knowledgeable "shoulder-to-shoulder" escort while in secure area.
- Prior sanitization of work areas as well as the systems in question.
- Use of dedicated, unclassified media for maintenance.
- If system has 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.

### DERIVATIVE CLASSIFIER

As a cleared contractor employee, if you create classified materials as a part of your job responsibilities either by incorporating, paraphrasing, restating or compiling information that is already classified. You are considered a derivative classifier.

To comply with government regulations, a derivative classifier must take training every two years to continue to create classified material or to have access to a classified computer system. If you are a derivative classifier, select the appropriate link to complete the additional training:

[Inside the NG Domain](#)

[Outside the NG Domain](#)
CONTACT INFORMATION

This concludes your annual Security refresher training.

For questions or guidance contact your local security representative, or call the Enterprise Security Shared Service at 855-737-8364; option 3, option 2.

If you are viewing this presentation, on some other area than the Learning Exchange (LX), email the ESSS Training Group at ESSS_DoDTraining@ngc.com stating you have completed the security refresher training. In your e mail include:

- Your legal first and last name
- Your MyID, and
- The training confirmation code (COMPSEC17)

If you are a derivative classifier, select the appropriate link to complete the additional training.

Inside the NG Domain

Outside the NG Domain