FEDERAL STUDENT AID – FINANCIAL MANAGEMENT SYSTEM (FMS)

General Security Awareness Training

September 2022

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

AGENDA

- **Purpose of Training**
- **FMS Security Profile**
- **User Security Responsibilities**
  - Rules of Behavior
  - Password Management
  - User Contact Information
  - Information Protection
  - System Access Controls
  - Incident Reporting
- **Computer Security Threats**
  - Malicious Software/Programs
  - Social Engineering
  - Theft of Data and/or Equipment
- **Review**
- **Training Acknowledgement**

PURPOSE OF TRAINING

- Raise the security awareness level of FMS users
- Inform FMS users of information security responsibilities
- Inform users of FMS policies
- Educate users on basic data protection and system security
- This training satisfies the annual requirement for FMS Information Security Training; however, your employer or agency may require completion of additional training on a periodic basis.

FMS SECURITY PROFILE

- FMS is rated a mission important system by Federal Student Aid
- FMS Data Sensitivity Ratings
  - Confidentiality = Moderate
  - Integrity = Moderate
  - Availability = Moderate
- FMS contains data protected under the Privacy Act
- FMS undergoes system certification and accreditation at least every three years, or after a major system change, and is currently enrolled in the Ongoing Security Authorization Program.
- FMS user security awareness training is required annually for all users

USER RESPONSIBILITIES – RULES OF BEHAVIOR

- Prior to being granted access to FMS, all users must read the Rules of Behavior and submit a signed Security Access Agreement.
- Every user must be made aware of their responsibilities for the use, protection, and release of sensitive Department of Education information under their control. This applies to outsourced support and contractors, as well as government employees.
- Each new user is a risk to the system and to other users of the system. Therefore, everyone must be versed in the rules of the system, or acceptable behavior, before being permitted to access the system. Training is tailored to the needs of the user and the system security requirements.
- Effective security is a team effort involving the participation and support of everyone. It is the responsibility of each user to know and follow these guidelines.

USER RESPONSIBILITIES – RULES OF BEHAVIOR (CONTINUED)

- All new users requesting FMS access MUST receive and maintain a favorable result to a documented background investigation completed by their organization or agency.
- The FMS User Access Request Form contains the Rules of Behavior for FMS.
- There should be *no expectation of privacy*. Users must consent to monitoring with each login to FMS.

USER RESPONSIBILITIES – PASSWORD MANAGEMENT (EXTERNAL USERS)

- First time passwords must be changed within 30 days, or the account is deactivated. Contact the FMS help desk for account reactivation assistance.
- Users who have forgotten their passwords or experience a locked account due to 3 consecutive unsuccessful logon attempts, must contact the FMS help desk for assistance.
- FMS passwords must comply with the following requirements:
  - Passwords expire every 30 days
  - Passwords must be at least 16 characters in length and are case sensitive
  - Passwords must contain at least one number (0-9), one upper case letter (A-Z), one lower case letter (a-z), and one special character (!,@,#,$,&,*)
  - Passwords must not contain the User ID
  - Passwords must not contain repeating characters (e.g., aaa, eee, rrr, @@)

USER RESPONSIBILITIES – CREATE STRONG PASSWORD (EXTERNAL USERS)

- A strong password should appear as a string of random characters.
- Add complexity by combining letters, numbers, and symbols or characters. The greater variety of characters you have in your password, the harder it is to guess.
- Use words and phrases that are easy for you to remember but difficult for others to guess.
- Passwords cannot be the same as the User ID and cannot contain the word "password" in any form.

USER RESPONSIBILITIES – PASSWORD MANAGEMENT-EXTERNAL USERS (CONTINUED)

Use the following concepts to create a password that is easily remembered, but difficult to guess. Your actual FMS password must be at least 16 characters in length:

- Change letters to numbers and symbols in a string of several words to create a “pass phrase” (e.g., 4U2know!).
- Exchange certain letters in a word with a number and symbol, instead of a letter (e.g., 4AHoMeRUN% would become 4AH@M3Run% by using the symbol @ for the letter ‘O’ and the number 3 for the letter ‘E’).
- Insert punctuation, numbers and symbols or special characters into a word, and deliberately misspell the word to comply with the “no repeating character” requirement (i.e., 1P@YReiz!).
- Combine several personal facts to create a “pass phrase” (e.g., Ye11owBAS3BaLL@31797SKI).
- Create an acronym from words in a song, a poem, or another known sequence of words (e.g., 4_S&7yA! from the Gettysburg address, “Four score and seven years ago…”).

USER RESPONSIBILITIES - PASSWORD MANAGEMENT – EXTERNAL USERS (CONTINUED)

- Keep your password secret!
- Do not share your password. The owner of the password could be held criminally liable for any illegal acts performed using his/her User ID and password.
- Your password is the key you use to access FMS information – protect it!
- Never provide your password over the telephone, via email, or to anyone requesting this information.
- For detailed information regarding creating strong passwords, you may visit Microsoft’s site on creating and protecting strong passwords.

USER RESPONSIBILITIES – USER CONTACT INFORMATION

- Keep your contact information and email address current.
- The email address on your FMS user access agreement will be used to notify you of FMS security changes, when your access will expire, and when renewals are due.
- Report any change in your email address to the FMS Help Desk.

USER RESPONSIBILITIES – INFORMATION PROTECTION

- Output/Media Markings – All output media (e.g., documents, hard drives, CD_ROMs, DVDs, flash drives, and tapes) shall be marked according to the sensitivity and criticality of the information contained therein. Information handled by the Department is generally placed in two categories: “Unclassified” and “Sensitive But Unclassified” (SBU).
  - Unclassified information requires no special handling and is available for public release.
  - SBU data is strictly controlled on a need-to-know basis to preserve confidentiality and integrity. This group of data shall be evaluated by the user for its sensitivity level and handled appropriately, based on policies and procedures established by the Department, as well as applicable Federal laws. Privacy Act data and Personally Identifiable Information are SBU data.

USER RESPONSIBILITIES – INFORMATION PROTECTION (CONTINUED)

- Distribute information only to authorized personnel.
- Destroy electronic and/or hard-copy material when discarded (degauss or shred).
- “Clear Desk Policy” - Lock your computer desktop and secure all sensitive data before leaving your desk or workspace.
- Employees, contractors, and partners must take all possible security precautions to secure and protect personal privacy information.
- Zip and password protect sensitive but unclassified data. This would include Privacy Act Data and Personally Identifiable Information.
    - An easy way to protect privacy information using email is with WinZIP encryption.
        - Password distributed separately over email or phone communication
        - AES 256-bit encryption required
        - Complex Password, 12 characters (uppercase and lowercase letters, numbers, and special characters)

USER RESPONSIBILITIES – INFORMATION PROTECTION (CONTINUED 2)

- All sensitive documents and media shall be double packaged in opaque materials that are approved by the shipping agent (e.g., DHL, FedEx, UPS, USPS, etc.)
- The outermost container/package material shall not identify the sensitivity of the contents.
- The receipt and delivery of media containing sensitive data shall be monitored and accounted for to ensure that data is not lost and potentially compromised in transit.

USER RESPONSIBILITIES - INFORMATION PROTECTION – PERSONALLY IDENTIFIABLE INFORMATION (PII)

- PII refers to any information about an individual maintained by including but not limited to, education, financial transactions, medical history, criminal or employment history and information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.
- Privacy Act Data is all data protected under the Privacy Act of 1974, 5 USC Section 552A.

USER RESPONSIBILITIES – PORTABLE DEVICES

- All sensitive information (PII, non-public financial information, and proprietary information) must be encrypted when stored on any portable device.
- Encryption must use the AES encryption algorithm with a minimum key length of 256 bits.
- When an access password is used to encrypt or decrypt the information, the password must be 12 characters in length and use three of the following: upper case letters, lower case letters, numbers, and special characters.

USER RESPONSIBILITIES – SYSTEM ACCESS CONTROLS

- Users are permitted access to the system based on their role (role-based-access).
- Application users are restricted from accessing the operating system, other applications, and system resources not needed in the performance of their duties.
- Demonstration/training users are not permitted access to live production environments.
- Federal Software Usage
  - No software should be used to gain unauthorized access to the network or scan the network.
  - Do not copy federally owned and provided software for personal use.
- Email
  - Do not send unencrypted sensitive information via email.
  - ed.gov e-mail addresses are for official FMS related e-mail correspondence only and are not to be used to create or forward chain letters or “spam” mail.

USER RESPONSIBILITIES – INCIDENT REPORTING

- Report security problems and suspicious activity or incidents.
- “Incidents” include, but are not limited to:
  - Data and Equipment Theft and Loss
  - Fraud and Scams
  - System and Data Misuse
  - Phishing, Pharming, Vishing
  - Viruses and Malware
- Report security problems and suspicious activity or incidents.

USER RESPONSIBILITIES – INCIDENT REPORTING (CONTINUED)

- Attempts to exploit a known or suspected flaw in the application or security systems are viewed as malicious activity and can be considered a crime.
- If you lose privacy-protected personal information, contact your immediate supervisor and your Information System Security Officer (ISSO) immediately. This type of incident must be reported ***within one-hour*** under federal guidelines.

USER RESPONSIBILITIES – INCIDENT REPORTING PROCEDURES

Incident Reporting Procedures

- Immediately report incidents to the FMS Information System Security Officer (ISSO):
  - Clinton Swart
  - Email: Clinton.Swart@ed.gov
- If the FMS ISSO is not available, report incidents to Federal Student Aid Chief Information Security Officer (CISO), then contact the FMS ISSO as soon as possible:
  - Devin Bhatt
  - Email: Devin.Bhatt@ed.gov
- Request email "read receipt" to document receipt of incident report regardless of to whom the incident is reported. DO NOT put sensitive details regarding security incidents or vulnerabilities in email or send in documents that are unencrypted. This could pose a security risk and incident.

THREATS – SYSTEM SECURITY THREATS

System Security Threats

- Malicious Software/Programs
  - Malware (viruses, worms) - parasitic programs written intentionally to “infect” or damage program and system performance.
  - Spyware - programs designed to intercept or take partial control of a computer’s operation without the consent of the machine’s owner.

THREATS – SYSTEM SECURITY THREATS (CONTINUED)

- Social Engineering - an act of deceiving unsuspecting people into revealing confidential information. Includes:
  - Phishing - attempting to fraudulently acquire sensitive information, such as PINs, social security numbers, account numbers, passwords, or credit card information, by pretending to be the person or business with whom the victim does business.
  - Vishing - or “voice phishing” occurs when a scammer sends an email hoping that a victim will telephone a voice mailbox to disclose sensitive financial and personal information.
  - Pharming – an attack aiming to redirect a website's traffic to another (bogus) website. Pharming can be conducted either by changing the host’s file on a victim’s computer or by exploitation of a vulnerability in DNS server software. This is an insidious attack, and not easily detected.
  - Shoulder Surfing - looking over someone’s shoulder to get information.

THREATS – PROTECTION AGAINST THREATS

- Malicious Software/Programs:
    - Keep Antivirus and Anti-Spyware Software installed and up-to-date.
    - Don’t visit questionable websites.
    - Don’t click on links sent in email unless from a trusted source (and even then, be wary).
    - Report excessively slow computer, or unintended links and images popping up on your screen.
- Theft of Data and/or Equipment:
    - Secure all equipment and data storage media.
    - Lock screen/terminal when not in use or unattended.
    - Encrypt and guard sensitive data in transit (email/FTP) and at rest (storage).

THREATS – PROTECTION AGAINST THREATS (CONTINUED)

- Social Engineering:
  - Phishing:
    - Never give out personally identifiable information in an email or to a web site that has a link in an email without validating it with the legitimate source.
    - Never give out your password or PIN to anyone.
    - Do not open email with attachments or enclosures if they are from unknown sources. Do not reply to the email, and do not type or paste any information into the email.
    - Do not click on any links contained within the email from any unknown source.
    - Get more information by visiting the Federal Trade Commission’s website.

THREATS – PROTECTION AGAINST THREATS (CONTINUED 2)

- Social Engineering:
    - Pharming:
        - Use anti-virus software, anti-spyware, and firewall software (all from trusted, legitimate sources).
        - Ensure that your web-browser is kept up to date and security patches are applied.
        - Look for website privacy policies. Avoid doing business with any site that does not post its privacy policy.
        - Limit the number of websites and amount of personal information you share on the Internet.
        - Look for misspelled words and bad formatting.
        - If a password is needed, enter an incorrect password first and see what happens.
        - Use only a reputable Internet Service Provider.

THREATS – POINTS TO REMEMBER

Points to Remember!

- The Department of Education DOES NOT solicit Privacy Act protected information through emails, nor directs you to websites through emails that then solicit Privacy Act protected information.
- No one at the Department of Education, including the FMS Help Desk, will ever ask you for your password. Never disclose your password or PIN to anyone.
- FMS users who receive email requests from unknown sources for sensitive student data should immediately report such incidents to the FMS Information System Security Officer (ISSO).

FMS SECURITY POINTS OF CONTACT

- FMS Help Desk
  - Phone: 1-800-433-7327, Option 1
  - Email: FMS.Operations@ed.gov

- FMS Information System Security Officers
  - Clinton Swart
    - Email: Clinton.Swart@ed.gov
  - Alonzo Posey
    - Email: Alonzo.Posey@ed.gov

REVIEW

- **Report Suspected Incidents and Threats**
  - If you suspect that your FMS password, or FMS data has been stolen or compromised, contact the FMS ISSO immediately.
  - Immediately report all security incidents, compromise, potential indicators of insider threat or suspected compromise, and potential threats and vulnerabilities involving computing resources to designated FMS computer security.
- **Abide by the Rules of Behavior**
- **Observe User Responsibilities**
- **Protect Sensitive and Privacy Act Data**
- **Beware of Threats**
- **Renew your FMS Access Annually**
- **Notify the FMS Help Desk or the FMS ISSO if you no longer require system access**

ACKNOWLEDGEMENT OF TRAINING

- FMS access will not be granted or renewed until a completed and signed training acknowledgement form is received after the completion of training.
- Please insert your name where '[insert name]' is in the below paragraph. Insert the date you reviewed the training presentation where '[insert date]' is located. Then, cut-and-paste the following paragraph into an email:

I,[insert name], hereby certify that I have received, reviewed, and understand the General Information Security Awareness Training for FMS, based on the standards set forth in NIST Special Publication 800-16, as presented. This training is mandatory and fulfills the requirement set forth in OMB Circular A-130, Appendix III. The individual named above received this training on [insert date].

- *If sending via e-mail from your registered email account, FMS will consider you to have "signed" this form electronically. Submit completed form via email to: FMS.OPERATIONS@ed.gov.