Security Training for Users of Federal Student Aid Systems (Page 1 of 3)

The data contained in Federal Student Aid (FSA) systems is confidential and is protected by the Privacy Act of 1974 (as amended), and other applicable statutes and regulations. Protected information includes, but is not confined to, name, address, telephone number, Social Security number, date of birth, maiden name, and similar types of information that can be used to identify a specific person.
Access to FSA systems is granted to individuals whose specific job responsibilities include at least one of the following activities:

- Determining a specific student applicant's eligibility for Title IV student aid;
- Billing and collecting on a Title IV loan;
- Enforcing the terms of a Title IV loan;
- Billing and collecting on a Title IV grant overpayment;
- Submitting student enrollment information;
- Ensuring the accuracy of a financial aid or borrower record;
- Assisting with default aversion activities;
- Obtaining default rate information; and
- Obtaining Gainful Employment Information

Data contained within FSA systems may not be used for any other purpose, including the marketing of student loans or other products.

The information contained in the following pages will provide additional information on these requirements and your responsibilities as a user and/or a Primary Destination Point Administrator (PDPA) of FSA systems.

Protection of Data Contained within FSA Systems:

To comply with the rules and regulations regarding the Title IV aid programs, you may at times need to keep records of information that you have obtained from an FSA system.

- Any information retrieved from FSA systems may be shared only with individuals expressly authorized to receive this information.
- Data must not be "screen scraped" or accessed by automated tools and used in any other program.
- All printed materials are to be marked as Personally Identifiable Information (PII).
- All sensitive information existing in hard copy must be stored in a locked container in a limited or exclusive area, an access controlled electronic environment, or be under the physical control of an authorized individual.
- All inquiries on student/borrower data must be business related.
- Electronic files must be properly encrypted. The current encryption protocol is Advanced Encryption Standard (AES) 128-bit, in accordance with Federal Information Processing Standards (FIPS). Additional information can be located at: http://csrc.nist.gov/publications/fips/index.html
- Never save unencrypted information on an unsecured drive, including a computer's hard drive.
- Never access data unless a relationship exists with the student/borrower.
- Never leave computers logged on and unattended. Log off at the end of each session or use access control software (i.e., screen saver with password) during unattended use.
- Never email Privacy Act protected information except in an encrypted and password-protected attachment.
- Never provide a password in the same email as an encrypted document.
- Never view sensitive material while in a public place.

The penalty for knowingly disclosing information to unauthorized individuals or willfully violating security standards is a misdemeanor with a fine up to $5,000.

Be Aware: *You will be required to agree to conform to the Rules of Behavior for use of FSA systems and agree to abide by the Privacy Act of 1974 (as amended).*

Penalties for violating FSA security procedures are severe for both users and the organizations they represent.

- The sharing of User IDs and passwords is a violation of the Rules of Behavior and will result in the individual, and potentially the organization (and/or servicer), permanently losing access to FSA Systems.
- The User ID is assigned to an individual, not the organization.
- Only the individual to whom the User ID is assigned can use that User ID to access FSA systems online.
- Each individual is responsible for protecting his or her access, password, and the data in FSA systems.
- At no time should an individual be asked to provide their FSA system User ID and password to anyone.
- This includes the employee's supervisor or management.
- Individuals who are asked to provide their User ID and password to anyone must contact the Customer Service Center for the system in question immediately.
- An eligible organization that allows unauthorized access to an FSA system will be considered to have violated its responsibilities and places itself at risk of losing access to Departmental systems and data, and to possible loss of eligibility to participate in the Title IV student aid programs.
- All organizations must train employees on the importance of maintaining the privacy of student aid related data, and review its own policies, procedures, and agreements to ensure that it is in full compliance.

The next several sections cover general Security information, with which you may already be familiar. It is important that you review this information again for the benefit of you and your organization.

Personally Identifiable Information (PII)

PII is information that can be used to distinguish or trace someone's identity. It is any information about an individual maintained by an agency. PII includes, but is not limited to, education, financial transactions, medical history, criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, and any other personal information that is linked or linkable to an individual.

It can include information such as:

- Social Security Numbers;
- Age;
- Home and office phone numbers;
- Birthdays;
- Marital status and spouse names;
- Educational history;
- Medical history;
- Demographics;
- Biometric information; and
- Financial information.

These are often found on:

- Office personnel lists,
- Medical records,
- Rolodex cards, and
- Electronic-based address books or contact records.

Even if the individual pieces of information seem harmless, one or two pieces of information can be combined with other information to compromise someone's identity. For example, the Social Security

combined with other information to compromise someone's identity. For example, the Social Security Number, if associated or combined with other PII, can create a high risk to the identity protection of an individual.

In many FSA systems, PII is a subset of sensitive information. If you handle PII, you are the first line of defense in preventing the identity theft. It is your responsibility to protect any PII entrusted to you. In addition, you and your organization have the responsibility of protecting PII and mitigating the damage when PII is lost or stolen.

Sensitive Information

Sensitive Information can include, but is not limited to:

- Personnel,
- Financial,
- Payroll,
- Medical,
- Operational, and
- Privacy Act information.

During working hours, reasonable steps should be taken to minimize the risk of access to sensitive information by unauthorized personnel.

If contract building security is not provided, sensitive information must be stored in locked containers, desks, or cabinets. Follow your organization's policy for storing sensitive information.

Security Training for Users of Federal Student Aid Systems (Page 2 of 3)

Creating a Secure Password

Each organization has its own policy on passwords, but there are some general guidelines you should follow to protect the Government's information systems from being compromised. Using these guidelines at home keeps your home computer secure as well.

Password Do's:

- Do use a combination of:
  - Lower and upper case letters,
  - Numbers, and,
  - Special characters, such as the number sign or percent sign.
- Do change your password according to your organization's policy.
- Do create a complex, strong password, and protect its secrecy. This is critical for protecting Federal information and information systems, as well as for protecting your own personal information.

Password Don'ts:

- Do not use personal information, such as:
  - Birthdays, or
  - Names of:
    - Family members,
    - Friends,
    - Pets,
    - Favorite sports teams, or
    - Favorite bands.
- Do not use common phrases or words found in the dictionary, including foreign languages. Hackers even have a Klingon dictionary!
- Do not write down your password. Commit it to memory.
- Do not share your password with anyone, ever.

Example of Strong Password

MH1&MomPlus3131 is the best option as it contains:

- Upper case letters,
- Lower case letters,
- Numbers, and
- Special characters.

Unlocked Computer

If your agency has implemented Personal Identity Verification (PIV) cards, or smart cards:

- You must remove and take your PIV card with you when you leave your computer. Removing your PIV card will automatically lock your computer and ensure that no one can access your files or send files using your identity.
- Do not leave your PIV card unattended, even for a minute.

If your agency has not implemented PIV cards:

- Be sure to manually log off, or shut down your computer.
- When you leave for the day, be sure to log off your computer.
- Many organizations require you to restart your computer for overnight updates.
- Follow your organization's policy.

Spillage

Spillage includes the improper handling of sensitive information on a non-sensitive system, including the improper:

- Storage,
- Transmission, or
- Processing of information.

When storing sensitive information, including PII, prevent spillage by following these security tips:

- Encrypt data before storing.
- Store data only on a network that has been certified and accredited to store this type of information.
- Remember, some systems are strictly non-sensitive. Never transmit, store, or process sensitive data on a non-sensitive system.

Social Engineering

Social engineering is a collection of techniques intended to trick people into divulging private information. The social engineer attempts to use the information to gain unauthorized access to computer systems, or to commit fraud.

Social engineers use a variety of communication devices to contact their victims, including:

- Telephone surveys,
- E-mail messages,
- Websites,
- Text messaging,
- Automated phone calls, and
- In-person interviews.

Phishing

Phishing is one type of social engineering that uses e-mail or websites to trick you into disclosing personal, sensitive information, such as:

- Credit card numbers,
- Bank account information,
- Your Social Security Number, or
- Passwords.

The intention is to steal your identity (identity theft), run up bills or commit crimes in your name, or access your organization's computer systems. Phishing is a serious, high-tech scam.

How does it work?

Phishers try to deceive you by sending e-mails or pop-up messages that appear to be from:

- Your Government agency,
- Your Internet service provider (ISP),
- Your bank, or
- Some other legitimate business or organization.

The message might claim that you need to update or validate your account information. It might threaten some dire consequence if you do not respond. The message directs you to a web site that looks just like a legitimate organization's site, but it is not affiliated with the real organization in any way. The bogus site tricks

you into divulging your personal information. It may also install malicious code on your system.

Removable Media

Removable media includes:

- CDs,
- DVDs,
- Thumb drives,
- Flash drives, and
- External hard drives.

Removable media that contains sensitive information must be properly:

- Labeled,
- Stored,
- Encrypted, and, when discarded,
- Purged.

If the media contains PII or other sensitive data, including Government information not cleared for public release, the information must be encrypted. Contact your security POC for additional information on proper labeling of removable media.

Be careful how you discard of CDs or other removable media. A CD that is labeled as sensitive must be purged before it is discarded. Merely deleting sensitive data does not prevent it from being recovered. The most common purging method is using an approved software tool that repeatedly overwrites the entire media to completely destroy any recoverable remnants of the original information.

Anything that cannot be overwritten must be physically destroyed. For example, many shredders are designed to handle CDs and DVDs. Be aware that data can be recovered from media fragments as small as 1/100 of an inch. Your information security officer can help identify an appropriate data purging method based on the sensitivity of your information.

Please note, some agencies may severely restrict or prohibit the use of removable media, especially flash memory devices, such as thumb drives.

Security Training for Users of Federal Student Aid Systems (Page 3 of 3)

Mobile Computing Devices

Be extra vigilant when storing data on mobile computing devices, such as, PDAs, cell phones, laptops, and personal electronic devices, or PEDs. Because of their small size and portability, these devices are especially vulnerable to security risks.

All PDAs and other mobile computing devices connecting to Government systems must be in compliance with Federal policy. Please note that the Government considers laptop computers as mobile computing devices.

All laptops that store PII must be secured using a whole-disk encryption solution to protect the sensitive information stored on them.

All sensitive data must be encrypted in accordance with the data's sensitivity level. This includes all PII, such as:

- Social Security Numbers,
- Dates and places of birth,
- Mothers' maiden names, and
- Biometric records.

If a device is lost or stolen, immediately report the loss to your security POC.

If the PDA contains PII, you must also follow any other procedures your organization has implemented regarding the compromise of PII.

Please note that some agencies may severely restrict or prohibit the use of mobile computing devices.

Fax Machines

Before transmitting sensitive information over a fax machine:

- Ensure that the recipient is at the receiving end, ready to pick up the fax immediately.
- Use the correct cover sheet for the sensitivity of the information you are faxing.
- After sending the fax, contact the recipient to confirm receipt.

Never transmit sensitive information via an unsecured fax machine

E-Commerce and Cookies

A cookie is a text file that a web server puts on your hard drive. As you enter information at a website, the cookie saves the data, including which items you've placed into your "shopping cart," your user preferences, and your user name.

Though sometimes useful, enabling cookies can pose a security threat, the most serious being when a cookie "saves" unencrypted personal information, such as your credit card numbers or Social Security Number.

Cookies can also track your activities on the web; this also poses a security risk, and may lead to a potential

Cookies can also track your activities on the web, this also poses a security risk, and may lead to a potential invasion of your privacy.
Both in the office and at home, shop online wisely and follow these security tips:

- Use cookies with caution.
- If your organization does not configure your cookies setting, set your browser preferences to prompt you each time a website wants to store a cookie.
- Only accept cookies from reputable, trusted websites.
- Confirm that any e-commerce site conducts its business over an encrypted link before providing any personal information:
- An encrypted link is indicated by "h-t-t-p-s" in the URL name.
- Make sure that an icon is visible that indicates the encryption is actually functioning.
- Note that not all https sites are legitimate; you are still taking a risk by entering your information online.

Roles and Responsibilities

Additional Information for PDPAs:

If you have been identified as a PDPA for your organization, in addition to the information listed above you are responsible for:

- Enrolling the organization's users.
- Maintaining an accurate and current listing of your organization's active users.
- Deactivating users who are no longer employed or whose job no longer warrants access to FSA systems.
- Monitoring users' access for any unauthorized activity.
- Recertifying online access for your organization's users on an annual basis.
- Signing access applications that your servicer makes through www.fsawebenroll.ed.gov

You should never approve a user for access unless that person is an employee of the organization, school, or servicer to which the school has contracted to perform necessary functions. In addition, you must promptly deactivate any user who loses eligibility.

Additional Responsibilities for Guaranty Agency (GA), Federal Servicer, and Not-For-Profit Servicer (NFP) PDPAs

The PDPA of a GA, Federal Servicer, or NFP is responsible for activating and deactivating the appropriate number of individuals to perform:

- Online Loan Update
- Teacher Loan Forgiveness/Loan Discharge Update.

The agency is responsible for ensuring that the individuals who received update authority have been properly trained prior to receiving this access.

What if I am notified of a violation?

Activities on FSA systems are subject to monitoring, recording, and periodic audits to ensure that the resources are functioning properly and to protect against unauthorized use. Information obtained will be disclosed to appropriate third parties, including law enforcement personnel. Use of FSA computing resources implies consent by the user to such monitoring, recording, and auditing.

You may be notified by email of a potential violation by a user from your organization.

- Use the security monitoring reports to research the user's activities.
- If you determine that the user's online access must be terminated, use the www.fsawebenroll.ed.gov Web site to deactivate their online services. (For questions regarding FSAWebenroll, contact CPS/SAIG Customer Service at (800) 330-5947.)

For more serious potential violations, FSA will suspend the online ID and any other IDs associated with the user for the system(s) in question. You will be notified by email of the suspension.

- The email you receive will explain if the potential security violation occurred at the organization or another organization where the user has an online ID. If the violation occurred at your organization

another organization where the user has an online ID. If the violation occurred at your organization, use the security monitoring reports to investigate if the user violated security policies.

- If you determine that FSA security policies have been violated, deactivate the user's online services as described above.

If the PDPA determines that FSA security policies have not been violated, and there are extenuating circumstances which justified the perceived security violation, they must contact the Customer Service Center for the system in question.

☐ **I acknowledge that I have complied with the Department's guidance on information system security training. I acknowledge that I have taken the necessary training needed in order to have system access. I understand that failure to abide by the above rules and responsibilities may lead to disciplinary action.**