UF Restricted Data
Required Training

Kathy Bergsma
UF Information Security Manager
ufirt@ufl.edu
http://infosec.ufl.edu
Introduction to Restricted Data
What is Restricted Data?

Data, which if disclosed to unauthorized users, may have very significant adverse impact on an individual, a group or institution. Data protected by law and legal contracts.

- Credit card numbers
- Social security numbers
- Bank account and other financial numbers
- Drivers license numbers
- Medical records, account numbers and photos
- Student records such as grades, schedules and rosters

See [http://privacy.ufl.edu](http://privacy.ufl.edu) for a complete list.
Other Data Terms

Confidential Data
• Not a UF data classification, but a general term for data that should not be shared with those who are not authorized.

Private Data
• Not a UF data classification, but a general term for certain personal information that an individual has the right to control.

Sensitive Data
• Information that is not restricted and not public such as salaries, finance records and intellectual property.
Categories of Restricted Data

- Credit Cards
- SSNs, Drivers Licenses, Financial Accounts
- Health Records
- Student Records
Why Protect Restricted Data?

To preserve the privacy rights of those who share their personal information with us. It’s the law.

- Credit card industry standard (PCI DSS)
- Florida privacy Law
- Health record privacy (HIPAA)
- Student record privacy (FERPA)
Why Protect Restricted Data?

Direct costs
- Notifications
- Fines and Penalties

Indirect costs
- Reputation damage
  - Reduced enrollment
  - Reduced grant funding
  - Reduced donations
- Reduced productivity
Why Protect Restricted Data?

Individuals are accountable
  • Disciplinary action
  • Penalties
  • Law enforcement
Major Data Security Players
Major Data Security Players

UF Privacy Office
Major Data Security Players

- UF Privacy Office
- Information Security and Compliance
Major Data Security Players

- UF Privacy Office
- Information Security and Compliance
- Unit Administrators
Major Data Security Players

UF Privacy Office

You

Information Security and Compliance

Unit Administrators
Data Security Roles

**Users:** Anyone authorized to access, create, store or alter UF Restricted Data

**IT Professionals**
- Those who provide technical facilities and support services for UF Restricted Data

**Unit Administrators**
- Those with authority to direct action as needed to protect UF Restricted Data and to enforce UF and unit data security policies and procedures
Data Security Roles

Users: Sales clerks, Advisors, Faculty, Payroll clerks

IT Professionals
- Server managers
- Web content managers
- Workstation support

Unit Administrators
- Deans
- Directors
- Department Chairs
Who Authorizes Restricted Data?

- UF Controller
- Unit Administrators
- UF Privacy Office

Credit Cards
- Personally Identifiable Information

Student Records
- Health Records

- UF Privacy Office
Restricted Data Safeguards

Different types of Restricted Data have special safeguards, but some safeguards apply to all types.
Restricted Data Safeguards

RAPID SAM

Report unauthorized exposure
Restricted Data Safeguards

RAPID SAM

If in doubt, Ask
Restricted Data Safeguards

RAPID SAM

Get Permission
Restricted Data Safeguards

RAPID SAM

Login using unique Identification
Restricted Data Safeguards

RAPID SAM

Destroy data before Disposal
Restricted Data Safeguards

RAPID SAM

Confirm web site Security
Restricted Data Safeguards

RAPID SAM

Use only Approved software and systems
Restricted Data Safeguards

RAPID SAM

Minimize the amount and length of time
Avoid the following risks:

✓ Storing Restricted Data on workstations, portable devices or removable media.

✓ Sending Restricted Data in email or instant messages.

✓ Using Restricted Data on unapproved web sites.

✓ Removing Restricted Data from UF premises.
Approved Enterprise Systems

- UF Portal
  - Social Security Numbers
  - Financial account numbers
  - Drivers license numbers
  - Student records
  - Credit card data

- UF Course Management System
  - Student records

- UF ISIS
  - Social Security Numbers
  - Student records
Quick Review

What is Restricted Data?

A. [ ] All data concerning the design, manufacturing and use of atomic weapons

B. [ ] Data, which if disclosed to unauthorized users, may have very significant adverse impact on an individual, a group or institution

C. [ ] Data protected by law and legal contracts
Quick Review

Which of the following are Restricted Data?

A. Credit Cards
B. Salaries
C. SSNs
D. Staff ID
E. Student grades
Quick Review

Who are the major players in securing UF Restricted Data?

A. UF Privacy Office

B. DDD, managers and supervisors

C. Physical Plant

D. Information Security and Compliance

E. You
Quick Review

Which of the following are data security roles?

A. Users
B. Unit Administrators
C. Maintenance Workers
D. IT Professionals
Quick Review

Why do we protect Restricted Data?

A. ___________ To protect individual privacy rights

B. ___________ To obey the law

C. ___________ To protect the UF reputation

D. ___________ To avoid penalties and notification costs

E. ___________ To reduce productivity
Quick Review

Who authorizes the use of credit cards?

The UF Controller
Quick Review

Who authorizes the use of Social Security Numbers?

The UF Privacy Officer
Quick Review

Match the following safeguards with appropriate letter in **RAPID SAM**.

- **R** — Report exposures
- **A** — Destroy data before disposal
- **P** — Get permission
- **I** — If in doubt, ask
- **D** — Login using unique identification
- **S** — Use only approved software and systems
- **M** — Minimize the amount and length of time
- **A** — Confirm web site security
Credit Card Data
Credit Card Data

In addition to **RAPID SAM**...

- Use only authorized processing systems
- Never store credit card data
- Never send in email or instant messages
- Never download
- Never cut-and-paste
A UF ticket sales clerk processes credit card transactions from a desktop computer. Which of the following are acceptable uses of credit card data?

A. Storing credit card data on his desktop
B. Using credit card numbers in email
C. Entering on an approved web server
D. Archiving credit card data on CDs
Personally Identifiable Information
Personally Identifiable Information

Name together with one or more of the following:

• Social security number
• Drivers license number
• Financial account number in combination with any security code, access code, or password
Personally Identifiable Information

In addition to RAPID SAM…

Never store on desktop, laptop, CD, DVD or USB

Never send in email or instant messages
Professor Smith has been with UF for 30 years. Some of his older student records include SSNs. What is appropriate use of these records?

A. __________ Publish them on the web for easy access

B. __________ Store them on his laptop for access while traveling

C. __________ Purge SSNs from all records

D. __________ Move records to the UF course management system
Student Records
Student Records

- Personal identification number
- Financial aid, tuition, payments, account balances
- Grades, exam scores, or GPA
- Applications and admissions
- Disciplinary status
- Class rosters and schedules
- Evaluations, forms, essays, memos, or correspondence
- Other information to trace the student's identity
Student Records

In addition to **RAPID SAM**…

Don’t store on desktop, laptop, CD, DVD or USB drive

Don’t send in email or instant messages
Quick Review

Professor Johnson uses her laptop to maintain grades for his students. Which of the following are appropriate?

A. Get permission from the Department Chair
B. Use full disk encryption
C. Keep all records on her computer indefinitely
Health Records
Health Records

Any information that links an individual with their physical or mental health condition such as:

- Name of individual or relative
- Any address smaller than state
- Dates such as birth, admission, or discharge
- Telephone numbers
- Medical record numbers
- Account numbers
- Health plan beneficiary number
- Photographic or comparable images
Password Security
Password Security
Passwords are Like Underwear

- Longer is better
- Change them often
- Be mysterious
- Don’t leave them laying around
- Don’t share them with friends
Password Safeguards

**Don’t share it with ANYONE!**
- Not even family members
- Beware of phishing

**If you must write it down:**
- Don't include the word 'password'
- Don't include your logon id
- Disguise the password
- Protect it like a credit card
Phishing – Don’t Get Hooked

Learn to recognize phishing; they often...
• Try to build credibility by spoofing a real company or university
• Create false urgency for a quick response (account will be closed)
• Insist on a call to action (click a link or reply with information)

Use common sense when giving out personal information
• Be suspicious by default
• Check email for fake web links or fake web addresses
• Never give out account or personal information by email
• Remember, UF will never ask you for your password

Verify the information reported in the e-mail
• If in doubt, call customer support or the UF Helpdesk at 392-HELP
Password Security
Sample Passwords

Gator.Nation

NO

Gr82b@FlG8r

BETTER

***** WARNING *****

Don’t use this password!
Quick Review

Jane’s boyfriend doesn’t go to UF. While visiting Jane in Gainesville, he wants to connect his computer to UF wireless network. What should Jane do?

A. ____ Give him her GatorLink ID and password

B. ____ Ask him to use his cell phone to connect

C. ____ Direct him to public access wireless at nearest coffee shop
Quick Review

Mark just changed his GatorLink password. He used a complex password, but he’s afraid he’ll forget it. What should Mark do?

A. Keep the password under his keyboard until he has it memorized.

B. Disguise the password and keep it in his wallet.

C. Store it in an encrypted file on his password-protected PDA.
Quick Review

Salena gets an email from someone claiming to be a UF IT worker about a problem with her GatorLink account. He asks for her password to investigate. What should Salena do?

A. **thumbs down** Respond to the email with her password.

B. **thumbs down** Check the sender’s email address before responding with her password.

C. **thumbs up** Call the UF HelpDesk to validate.

D. **thumbs up** Delete the email.
Encryption
Encryption

What is encryption?
• A digital process that renders data unreadable by those who are not authorized.

What is file encryption?
• Individual files and/or folders are encrypted separately.

What is whole disk encryption?
• Every bit of available data on a computer hard drive is encrypted including web cache, memory swap space, recycle bin and hidden files. The user has no decision in what is to be encrypted.
Encryption

Why is it important?

• Encrypted content may be exempt from liability
• Encryption helps protect Restricted Data from unauthorized access
How do I encrypt my data?

WARNING!

If the encryption key is forgotten, lost or stolen, the data is unrecoverable.

Work with your local unit IT professional for encryption key management.
Encryption

How do I encrypt my data?

• See your local IT worker for assistance
• Use only approved methods

Example Methods

• File/Folder: NTFS, Truecrypt, PGP
• Application: Winzip, Adobe Acrobat, Microsoft Office
• Whole-disk: Bitlocker, Truecrypt, PGP-WDE
Encryption Requirements

<table>
<thead>
<tr>
<th></th>
<th>Credit Cards</th>
<th>PII</th>
<th>Health Data</th>
<th>Student Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>Required</td>
<td>Risk-based²</td>
<td>Risk-based</td>
<td>Risk-based</td>
</tr>
<tr>
<td>Workstation</td>
<td>Required</td>
<td>Risk-based</td>
<td>Risk-based</td>
<td>Risk-based</td>
</tr>
<tr>
<td>Portable devices</td>
<td>Not Allowed¹</td>
<td>Required</td>
<td>Required</td>
<td>Risk-based</td>
</tr>
<tr>
<td>Backups</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Risk-based</td>
</tr>
</tbody>
</table>

¹Storing credit card numbers on portable devices and media is not allowed.  
²The need to encrypt Restricted Data is based on a risk evaluation that considers other controls used to protect the data.
Encryption

How can I avoid encryption?

• Do not store any Restricted Data on portable devices or media.
• Use only enterprise services for storing Restricted Data.
• De-identify data before storing it
De-Identification

A code may be used to replace identifying information if…

- The code is not derived from or related to information about the individual
- The code is not used for any other purpose
- The code is not disclosed for any other purpose
- The mechanism for creating the code is not disclosed
Encryption

Transmission of Data

• See your local IT worker
• Some methods are transparent to user
• Use only approved methods
  • Virtual Private Network (VPN)
  • SSL or https
  • SSH and SCP
  • SFTP
What is a VPN?

A VPN (virtual private network) is used to encrypt communication to UF from an untrusted network such as home, travel or even the UF wireless network. See your local IT Worker or visit the Network Services website for more information.
Quick Review

Professor Stewart teaches Economics. Which of the following will protect student records?

A. __ Send student records in email.

B. __ Use the UF Course Management System to maintain student records.

C. __ Contact the IT staff for encryption support with whole disk encryption on her laptop.

D. __ Use the UF VPN when working from home or travel.
Workstation Security
Workstation Authorization

- Credit Cards
  - Never
- SSNs, Drivers Licenses, Financial Accounts
  - Rare
- Student Records
  - Only when Authorized
- Health Records
  - Only when Authorized
Workstation Security

In addition to **RAPID SAM**…

Use only computers maintained by UF IT workers

Position screen so that it’s not viewable to others

Lock the screen when unattended
Quick Review

A clerk in a UF medical clinic accesses patient data from her desktop computer. Which of the following safeguards are advisable?

A. When leaving the computer unattended, enable a password-protected screen saver.

B. Position the screen so that no one can see it.

C. Configure a short screen saver time-out.

D. Tape password to monitor to keep it handy.
Portable Devices and Removable Media
Portable Devices/Removable Media

What is a portable device?
- Laptop
- Tablet PC
- Personal digital assistant (PDA)
- Smart phone

What is removable media?
- CD
- DVD
- Universal serial bus (USB) drive
- Magnetic tape
- External hard drive
Portable Devices/Removable Media

What is the risk?

• Portable devices and removable media are easily lost or stolen
Portable Devices/Removable Media

- Never
- Rare
- Only when Authorized

Credit Cards
- SSNs, Drivers Licenses, Financial Accounts

Student Records
- Health Records

Financial Accounts
- Only when Authorized
Portable Device Safeguards

In addition to **RAPID SAM**...

- Use only approved devices maintained by professional IT Workers
- Get special permission to remove from campus
- Use whole disk encryption
- Don’t synchronize it with your home computer
- Protect it like a wallet or purse
Removable Media Safeguards

In addition to **RAPID SAM**…

- Use only approved media maintained by professional IT Workers
- Use encryption
- Store in a secure location with limited and audited access
- Get permission before removing from campus
- Protect like a wallet or purse in transit
Travel Safeguards

In addition to **RAPID SAM**…

…and the portable device safeguards

- Remove unnecessary Restricted Data
- Make a secure backup before you travel
- Use the VPN to communicate with UF from locations
- Consider remote data destruction software
- Consider device tracking software

*Remember that special permission is required to remove Restricted Data from campus.*
Quick Review

Dr. Adams stores student data on his laptop. What should he do to protect the data?

A. ______ Contact the IT group for support with whole disk encryption.

B. ______ Remove the data when it’s no longer needed.

C. ______ Share the laptop with trusted family members.

D. ______ Ensure the data is unrecoverable when the laptop is surveyed.
Quick Review

CDs are used by the Academic Advisor in the Math Department to archive student records. Which of the following are advised?

A. Encrypt the data on the CDs.
B. Keep the CDs at hands reach on her desk.
C. Shred the CDs when no longer needed.
D. Discontinue this process and use a secure backup service provided by a professional UF IT worker.
Quick Review

Professor Wolfe needs to take his laptop to Europe to conduct confidential research funded by NSF. What should Prof. Wolf do?

A. Install remote data destruction software.

A. Remove unnecessary data before he travels.

A. Make a backup before he travels.

A. Use the UF VPN to connect from Europe to UF.
Personally-Managed Computers
Personally-Managed Computers

All computers used with UF Restricted Data should be managed by skilled IT professionals. Even where special permission has been granted, personally-managed computers should be audited periodically by IT professionals.

- Users are less likely to understand safe computing practices
- User might lack the technical skills to adequately secure their computer
- Personally-managed computers are more likely to be shared with family, friends and other unauthorized users
Personally-Managed Computers

- Never
- Only when Authorized

Credit Cards
- Rare
- Only when Authorized
- SSNs, Drivers Licenses, Financial Accounts

Student Records
- Health Records
- Only when Authorized

- Health Records
- Only when Authorized

- Financial Accounts
- Drivers Licenses, SSNs
- Only when Authorized

- Student Records
- Credit Cards
- Never
- Only when Authorized
## Personally-Managed Computers

In addition to **RAPID SAM**…

- Use only approved computers
- Maintain current OS and software updates
- Maintain current antivirus protection
- Use strong passwords
- Use whole disk encryption
- Enable the firewall
- Encrypt and protect backups
Home Computing Safeguards

In addition to **RAPID SAM**…

…and the personally-managed computer safeguards

- Do not share the computer with family and friends
- Use the VPN to communicate with UF from home
- Secure backups

*Remember that special permission is required to remove Restricted Data from campus.*
Quick Review

A professor in Engineering processes student grades on a computer that he personally manages. What precautions should he take?

A. ____ He’s a professor, so he doesn’t need authorization.

B. ____ Minimize the number of records and length of time they are stored.

C. ____ Enable the firewall on his computer.

D. ____ Share his computer with his graduate students.
Quick Review

Professor Jones processes student grades on her home computer. How should she protect the data?

A. Use current anti-virus software.

B. Maintain current updates on all software.

C. Use strong passwords.

D. Remove the data promptly when no longer needed.

E. Share the computer with trusted family members.
Email and Instant Messaging Security
Email and IM Security

Why are email and IM bad ways to exchange Restricted Data?

• Email and Instant Messaging are usually sent unencrypted
• Data sent via email and IM can be easily forwarded to others
• Auto-completion features make it easy to send data to wrong people
Email Authorization

- Never
- Rare

Credit Cards

- SSNs, Drivers Licenses, Financial Accounts

Student Records

- Rare

Health Records

- Rare
Email Safeguards

In addition to **RAPID SAM**…

- Use only approved email software and methods
- Do not use commercial services such Google, Yahoo, or MSN
- Label Restricted Data and provide handling instructions
- Send only to approved email addresses, usually ufl.edu
- Minimize the number of recipients - **No Mailing Lists**
- Beware of auto-completion errors; double check the recipients
- Hidden columns in attached spreadsheet are still accessible
Instant Message Authorization

- Never
- Rare

Credit Cards

SSNs, Drivers Licenses, Financial Accounts

Student Records

Health Records

- Never
Instant Message Safeguards

In addition to **RAPID SAM**…

- Use only approved software and methods
- Do not use commercial services such Google, AOL, or MSN
- Label Restricted Data and provide handling instructions
- Send only to approved addresses ending in ufl.edu
- Minimize the number of recipients - **No Lists**
- Beware of auto-completion errors; double check recipients
Quick Review

The Academic Advisor in the botany department needs to send student records to the Registrar. What procedures should be followed?

A. **Get permission**

B. **Ensure the message is sent to an authorized recipient using the correct ufl.edu address.**

C. **In the body of the message, note that confidential data is included, the message should not be forwarded and it should be deleted promptly.**
Web Security
Web Security

Access Restricted Data only from approved websites. Be aware of the following:

• Confirm the site is secure (look for the "s" in httpS://)
• Do not access Restricted Data from sites that do not have a valid security certificate
• Be discerning - Hackers can create sites that mimic trusted sites, but can conceal malware in web ads, games, pictures, etc.
Web Security

Publishing Web Content

• Ensure data is available only to those who are authorized
• Do not publish Restricted Data to the web unless authorized to do so
• Only publish Restricted Data on approved UF websites

Be aware of the following:

• Access restrictions may not survive upgrades, reorganizations, etc.
• Spreadsheets are often used to store data on websites - note that "hiding" a column does not remove the data from the actual spreadsheet
Web Authorization

- Only when authorized

Credit Cards

SSNs, Drivers Licenses, Financial Accounts

Student Records

Health Records

- Only when authorized
Web Safeguards

In addition to **RAPID SAM**…

- Use only approved browser, configuration and methods
- Use only approved web sites
- Do not use features to remember or auto-complete passwords
- Look for the lock or https in the url
- Beware of phishing scams
Social Media Precautions

Do not reveal too much information about yourself

Beware of fake profiles designed to exploit your trust

Beware of links – they might...

• Send your information to a third party
• Spread malware
Web Example

Professor Huang wants to use the web to provide grades to her students. Which of the following is allowed?

A. Use the student’s UFID to identify their grade.
B. Use GatorLink accounts to authenticate student access.
C. Get permission.
D. Use the UF course management system.
Reuse and Disposal Security
Reuse and Disposal

In addition to **RAPID SAM**…

- Consult your local IT Worker for approved reuse and disposal methods.

- Render Restricted Data unreadable before media reuse or disposal. Protect it until this can be done.

- Maintain inventory of data that must be stored or transported prior to reuse or destruction
Disposal Methods

Hard drives
- Derik’s Boot and Nuke

Paper or cdroms
- Shredder

Disposal vendors
- UF Cintas contract
Copiers, Printers, and Fax Disposal

- Attach a warning label

"WARNING: Data scanned on this device is stored in persistent memory."
Copiers, Printers, and Fax Disposal

• Ensure that originals are removed
• Consult the manufacturer for sanitization procedures
• Ensure new contracts include security requirement
• If the vendor does not provide a facility to sanitize media, remove the hard drive and sanitize
• If a 3rd party removes device, get a certificate of destruction
Disposal Example

The Psychology department is disposing of several computers. Which of the following will help prevent confidential data leakage?

A. [____] The survey office will take care of it.
B. [____] Contact the IT group for support.
A. [____] Use a certified disposal contractor.
Information Security and Compliance

Kathy Bergsma, UF Information Security Manager
392-2061
ufirt@ufl.edu
http://infosec.ufl.edu/

Colleen Ebel, Health Science Center ISM
Phone: 273-7478
Non-urgent email: HSC-Security-L@Lists.ufl.edu
Urgent email: HSCIRT@ufl.edu
Web: https://security.health.ufl.edu/
UF Privacy Office

Susan Blair, Chief Privacy Officer
Office phone: 392-2094
Privacy Hotline: 866-876-4472
Email: privacy@ufl.edu
Web: http://privacy.ufl.edu/

Credit Cards
Renato Squindo
squindo@ufl.edu
392-9057
Unit Contacts

IFAS
Wayne Hyde, IFAS Unit ISM
Phone: 846-2565
Email: IFASIRT-L@lists.ifas.ufl.edu or abuse@ifas.ufl.edu

Other Units
http://net-services.ufl.edu/cgi-bin/subnet-form.cgi