UF Office of Information Security and Compliance
UNIVERSITY of FLORIDA

Cyber Safeguards for UF Restricted Data

Kathy Bergsma

UF Information Security Manager

3/2/2010

This introductory data security course will explain the dos and don'ts of using UF Restricted Data on computers. You will learn when to use encryption, proper methods for disposal, and what to do in the event of a Restricted Data exposure. Important contacts regarding Restricted Data will be presented and technical resources for data protection will be discussed.

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 for a complete list.

Categories of Restricted Data

- Credit card data
- Personally identifiable information
    - Social security numbers
    - Drivers license numbers
    - Bank and other financial account numbers
- Student records
- Medical records

Other Data Terminology

- 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.

Why Do We 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
- Student record privacy (FERPA)
- Health record privacy (HIPAA)

Direct costs

- Notifications
- Fines and Penalties

Indirect costs

- Reputation damage
- Reduced enrollment
- Reduced grant funding
- Reduced donations
- Reduced productivity

Why Do We Protect Restricted Data?

Individuals are accountable

- Disciplinary action
- Penalties
- Law enforcement

Major Players

- UF Privacy Office
- UF Office of Information Security and Compliance
- Unit Administrators
- **You**

Data Security Roles

- 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
    - Deans
    - Directors
    - Department Chairs
- IT Workers: Those who provide technical facilities and support services for UF Restricted Data
    - Server managers
    - Web content managers
    - Workstation support
- Users: Anyone authorized to access, create, store or alter UF Restricted Data
    - Sales clerks
    - Advisors
    - Faculty
    - Payroll clerk

Who Authorizes Restricted Data?

- Credit Cards ⇒ UF Controller
- Personally Identifiable Information ⇒ UF Privacy Office
- Student Records ⇒ Unit Administrators
- Medical Records ⇒ UF Privacy Office

Restricted Data Safeguards

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

Try this memory to cue… *RAPID SAM*

R *Report* unauthorized exposure

A If in doubt, *Ask*

P Get *Permission*

I Login using unique *Identificaiton*

D Destroy data before *Disposal*

S Confirm web site *Security*

A Use only *Approved* software and systems

M *Minimize* the amount of data and the 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 non-ufl.edu web sites.
- Removing Restricted Data from UF premises without authorization.

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
  - Student records
  - Social security numbers

Credit Card Data

In addition to *RAPID SAM*…

- Use only authorized credit card processing systems
- Never store credit card data outside of the authorized system
- Never send credit card data in email or instant messages
- Never download credit card data
- Never cut or paste credit card data

Personally Identifiable Information

Name together with one or more of the following:

- Social security number
- Driver license number
- Financial account number in combination with any security code, access code, or password.

In addition to *RAPID SAM*…

- Never store on desktop, laptop, CD, DVD or USB
- Never send in email or instant messages

Student Records

- Name of the student's parent or other family member
- Address of student's family
- Personal identifier, such as the student's social security number
- A list of personal characteristics that would make the student's identity easily traceable
- Disciplinary status
- Financial – aid, tuition, payments, account balances
- Grades, exam scores, or GPA (grade point average)
- Class rosters
- Applications and admissions information
- Schedules
- Evaluations, forms, essays, memos, or correspondence to and about the student
- Birth date
- Gender
- Citizenship
- Marital status
- Religion

In addition to *RAPID SAM*…

- Do not store on desktop, laptop, CD, DVD or USB without special permission
- Do not send in email or instant messages without special permission

Medical 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
- Electronic mail address
- Social security numbers
- Medical record numbers
- Account numbers
- Health plan beneficiary number
- Full face photographic images and any comparable images
- *Any other unique identifying number, characteristic, or code*

Password Safeguards

- ✓ Password composition
  - Long, sometimes called passphrases
  - Complex
  - Difficult to guess
  - Easy to remember
- ✓ Password protection
  - Don’t share with ANYONE, EVER!
    - Not even family members
    - Beware of “social engineering”
  - If you must write it down to remember it:
    - Don't write the word 'password' on the note
    - Don't write your logon id on the same note
    - 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

Encryption

What is Encryption?
Encryption is a digital process that renders data unreadable by those who are not authorized.

- File encryption is when individual files and/or folders are encrypted separately.
- Whole disk encryption is when very 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.

Why Use Encryption?

- Encrypted content may be exempt from liability
- Encryption helps secure Restricted Data from unauthorized access

WARNING: Don't try encryption without professional support. If the encryption key is forgotten, lost or stolen, the data is unrecoverable. Always see your local IT Worker for support with encryption key management.

Methods for Encrypting Stored Data

- See your local IT Worker
- Use only approved encryption methods
- The following are examples, but they might not be approved in your unit
    - File/Folder: NTFS, Truecrypt, PGP
    - Application: Winzip, Adobe Acrobat, Microsoft Office
    - Whole-disk: Bitlocker, Truecrypt, PGP-WDE

When Is Encryption Required?

	Credit Cards	PII	Medical Records	Student Records
Servers	Required	Risk-based[2]	Risk-based	Risk-based
Desktops	Required	Risk-based	Risk-based	Risk-based
Portable Devices and Media	NA[1]	Required	Required	Risk-based
Backups	Required	Required	Required	Risk-based

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

How can I avoid the need to use 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 of Restricted Data

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

Methods for Encrypting Data for Transmission

- See your local IT Worker
- Some methods are transparent to user
- Use only approved methods
    - Virtual Private Network (VPN)
    - SSL or https
    - SSH, 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 web site for more information at http://net-services.ufl.edu/provided_services/vpn/

Workstation Safeguards

Can I store Restricted Data on my workstation?

- Credit Card Data: Never
- Personally Identifiable Information: Requires special permission and should be rare
- Student Records: Requires authorization
- Medical Records: Requires authorization

Avoid storing Restricted Data on your workstation. When the business need outweighs the risk and special permission is granted, remember *RAPID SAM* and…

- Use only approved computers maintained by UF IT workers
- Position screen so that it's not viewable to others
- Lock the screen when unattended

Portable Devices and 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

What is the risk of storing Restricted Data on portable devices or removable media?

- They are easily lost or stolen

Can I store Restricted Data on my portable device or removable media?

- Credit Card Data: Never
- Personally Identifiable Information: Requires special permission and should be rare
- Student Records: Requires authorization
- Medical Records: Requires authorization

Portable Device Safeguards

Avoid storing Restricted Data on portable devices. When the business need outweighs the risk and special permission is granted, remember *RAPID SAM* and…

- Use only approved devices maintained by professional IT Workers
- Get special permission to remove Restricted Data from campus
- Use whole disk encryption
- Don't synchronize portable devices with your home computer
- Protect portable devices and removable media like a wallet or purse

Removable Media Safeguards

Avoid storing Restricted Data on removable media. When the business need outweighs the risk and special permission is granted, remember *RAPID SAM* and…

- Use only approved media maintained by professional IT Workers
- Get special permission to remove Restricted Data from campus
- Use encryption
- Store it in a secure location with limited and audited access
- Protect portable devices and removable media like a wallet or purse

Travel Safeguards

Avoid traveling with Restricted Data. When the business need outweighs the risk and special permission is granted, remember the safeguards for portable devices and removable media, remember *RAPID SAM* and…

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

Personally Managed Computer Safeguards

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.

Why should we avoid storing Restricted Data on personally managed computers?

- 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

Can I store Restricted Data on my personally managed computer?

- Credit Card Data: Never
- Personally Identifiable Information: Requires special permission and should be very rare
- Student Records: Requires authorization
- Medical Records: Requires authorization

Avoid storing Restricted Data on personally managed computers. When the business need outweighs the risk and special permission is granted, remember *RAPID SAM* and…

- 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

Avoid using Restricted Data on your home computer. When the business need outweighs the risk and special permission is granted, remember the safeguards for personally managed computers, remember *RAPID SAM* and…

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

Email and Instant Messaging (IM)

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 Safeguards

Can I send Restricted Data in email?

- Credit Card Data: Never
- Personally Identifiable Information: Requires special permission and should be rare
- Student Records: Requires special permission and should be rare
- Medical Records: Requires special permission and should be rare

Avoid sending Restricted Data in email. When the business need outweighs the risk and special permission is granted, remember *RAPID SAM* and…

- 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 such as those ending in ufl.edu
- Minimize the number of recipients - ***No Mailing Lists***
- Beware of auto-completion errors; double check the recipients
- Spreadsheets are often used to store data on websites - note that hidden columns are still accessible

Instant Messaging Safeguards

Can I send Restricted Data in instant messages?

- Credit Card Data: Never
- Personally Identifiable Information: Never
- Student Records: Requires special permission and should be rare
- Medical Records: Never

Avoid sending Restricted Data in instant messages. When the business need outweighs the risk and special permission is granted, remember *RAPID SAM* and…

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

Web Safeguards

Access Restricted Data only on 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.

Publishing Restricted Data only on approved websites. Be aware of the following:

- 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 to approved UF websites

Be aware that…

- Access restrictions may not survive upgrades, reorganizations, etc.
- Spreadsheets are often used to store data on websites - note that hidden columns are still accessible

Can I use Restricted Data on the web?

- Credit Card Data: Requires authorization
- Personally Identifiable Information: Requires authorization
- Student Records: Requires authorization
- Medical Records: Requires authorization

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 http**S** 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

Disposal Safeguards

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
- Vendors: Cintas

Copiers, Scanners, Printers and Fax Machines

- 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

References

For copies of the slides, handouts, policies, products and other references, see http://infosec.ufl.edu/restricted-data

Contacts

Information Security and Compliance

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

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

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
Phone: 392-9057
squindo@ufl.edu

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