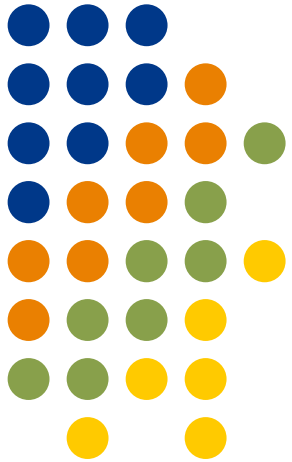
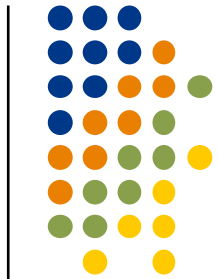
Cyber Safeguards for UF Restricted Data

Kathy Bergsma
UF Information Security Manager
ufirt@ufl.edu
http://infosec.ufl.edu/

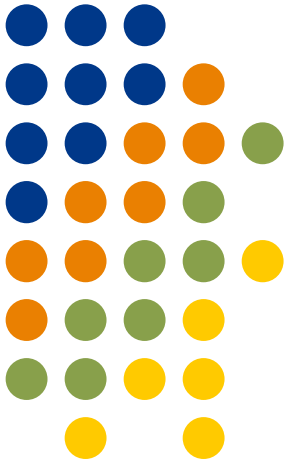


What is Restricted Data?

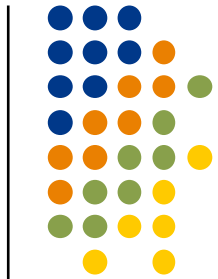


What type of Restricted Data do you use?

Introduction to Restricted Data



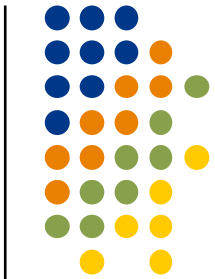
What is Restricted Data?



Terminology

- Restricted data
- Private data
- Confidential data
- Sensitive data

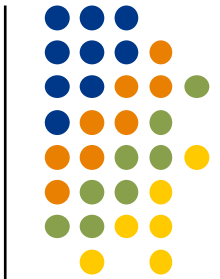
What is Restricted Data?



Major Players

- UF Privacy Office
- UF Office of Information Security and Compliance
- UF Health Science Center
- **You**

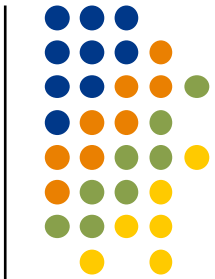
What is Restricted Data?



Four main categories of Restricted Data

- PCI: Payment Card Information
- PII: Personally Identifiable Information
- PER: Private Education Records
- PHI: Protected Health Information

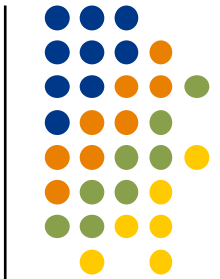
Examples of Restricted Data



See http://privacy.ufl.edu/ for a complete list.

- Social security number
- Credit card number
- Bank account and other financial numbers
- Drivers license number
- Medical records, account numbers, and photos
- Grades
- Schedules and rosters

Why Protect Restricted Data?



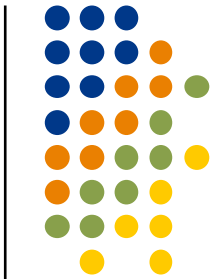
Legal:

- Court cases
- Notifications
- Penalties

Reputation:

- Registration
- Grant funding
- Donations

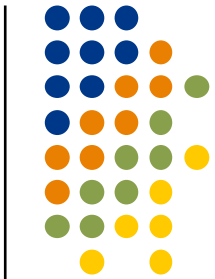
Why Protect Restricted Data?



Users are accountable

- Disciplinary action
- Penalties
- Law enforcement

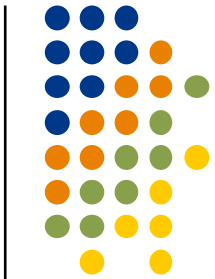
Restricted Data Safeguards



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.

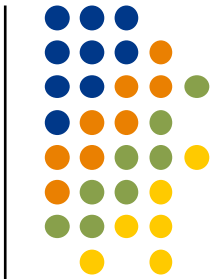
Restricted Data Safeguards



If in doubt, or if the need outweighs the risk:

- ✓Get permission
- ✓Use only approved systems
- ✓Authenticate to access
- ✓Minimize the amount of data
- ✓Minimize the length of time
- ✓Don’t use the official copy
- ✓Don’t use the only copy
- ✓Report exposure to UF Privacy Office

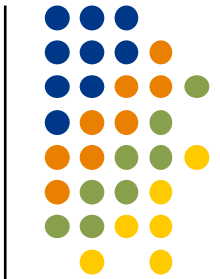
Restricted Data Safeguards



If in doubt or if need outweighs risk:

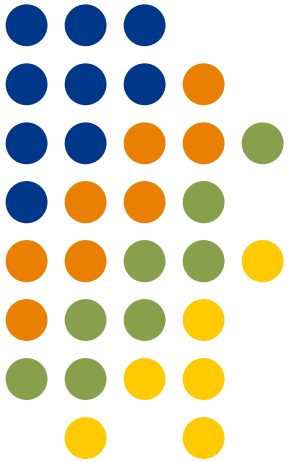
- ✓Use appropriate loss and theft protection
  - Report exposed Restricted Data to Privacy Office
  - Report exposed sensitive data to supervisor or DDD
- ✓Encrypt for storage and transmission
- ✓Render unreadable before reuse or disposal.

Additional Safeguards

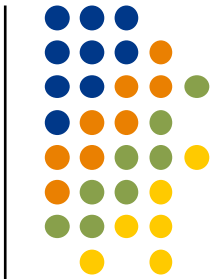


- Other concerns if you use Restricted Data
  - Copy and paste
  - Cache
  - Recycle Bin and deleted files
- Safeguards
  - Encryption
  - Secure reuse and disposal

PCI: Payment Card Information



PCI: Payment Card Information



Credit card account number alone or with any of the following:

- Cardholder name
- Service code
- Expiration date

PCI Safeguards

- ✓ Authorization from UF Controller must be documented.
- ✓ Use PCI data only on authorized computers maintained by UF professional IT workers.
- ✓ Never use PCI data outside the confines of the authorized credit card processing system.
- ✓ On the web, look for the lock or https in the url. 

PCI Safeguards

- ✓ Never store PCI data on a desktop, laptop, CD, DVD, thumb drive or **anywhere**.
- ✓ Never use PCI data in email or instant messages.
- ✓ Never download PCI data.
- ✓ Never cut & paste PCI data.

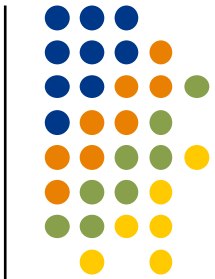
More Information About PCI

UF Privacy Office Financial Information
http://privacy.ufl.edu/financial.html

UF e-Commerce Policy
http://www.it.ufl.edu/policies/documents/E-commerce%20policy.pdf

UF cyber safeguards for PCI data
http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-limitations-pci.pdf

PCI Example



A UF ticket sales clerk processes credit card transactions from a desktop computer. Which of the following are acceptable uses of credit card numbers?

A.__ Storing credit card numbers on the desktop.

B.__ Using credit card numbers in email.

C.__ Entering credit card numbers on a UF secure web server.

PCI Example

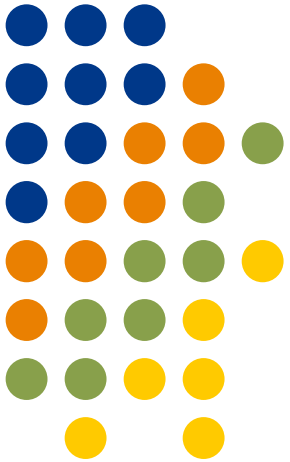
A UF ticket sales clerk processes credit card transactions from a desktop computer. Which of the following are acceptable uses of credit card numbers?

A. 👎 Storing credit card numbers on the desktop.

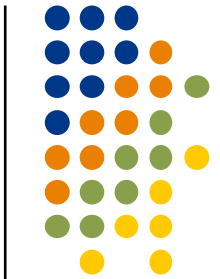
B. 👎 Using credit card numbers in email.

C. 👍 Entering credit card numbers on a UF secure web server.

PII: Personally Identifiable Information



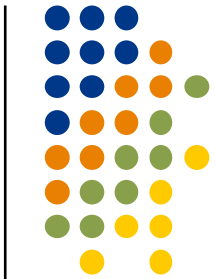
PII:
Personally Identifiable Information



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

PII Safeguards



- ✓ Privacy Office and DDD authorization must be documented.
- ✓ Use PII data only on authorized computers maintained by UF IT workers.
- ✓ PII data should not be stored on a desktop, laptop, CD, DVD, or thumb drive. Where necessary:
  - Obtain special permission
  - Use full disk encryption
  - Physically secure it

PII Safeguards

- ✓ Avoid using PII data in email or instant messages, especially to addresses that don't end in ufl.edu.
- ✓ On the web, look for the lock or https in the url. 

More Information About PII

UF cyber safeguards for PII data

http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-limitations-pii.pdf

PII Example

Professor Smith has been with UF for 20 years. Some of his older student records include SSNs. What is appropriate use of these records?

A.___ Publish the records on his UF web site for easy access.

B.___ Store them on his laptop so he can access them when he travels.

C.___ Purge SSNs from all his records.

D.___ Only store records on a secure UF server, minimizing retention to Florida statutes.

PII Example

Professor Smith has been with UF for 20 years. Some of his older student records include SSNs. What is appropriate use of these records?

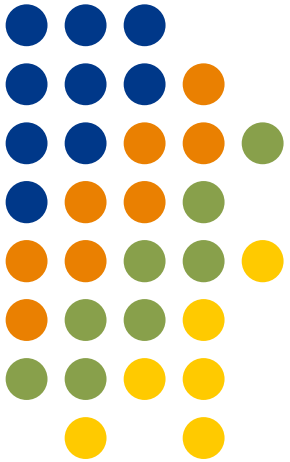
A. 👎 Publish the records on his UF web site for easy access.

B. 👎 Store them on his laptop so he can access them when he travels.

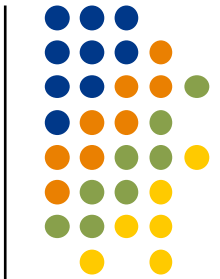
C. 👍 Purge SSNs from all his records.

D. 👍 Only store records on a secure UF server, minimizing retention to Florida statutes.

PER: Private Educational Record



PER: Private Educational Record



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

PER Safeguards

- ✓ DDD authorization must be documented.
- ✓ Use PER data only on authorized computers maintained by UF IT workers.
- ✓ PER data should not be stored on a desktop, laptop, CD, DVD, thumb drive. Where necessary, get special permission and use full-disk encryption.
- ✓ Avoid using PER data in email or instant messages, especially to addresses that don't end in ufl.edu.
- ✓ On the web, look for https in the url or the lock.

More Information about PER

FERPA training from the UF Privacy Office
http://privacy.ufl.edu/training/FERPA/

FERPA information from the UF Registrar
http://www.registrar.ufl.edu/ferpahub.html

UF cyber safeguards for PER data
http://www.it.ufl.edu/policies/security/drafts.html

PER Example

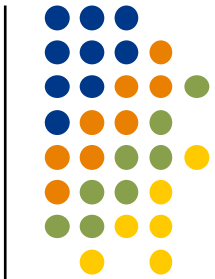
Professor Johnson uses his laptop to maintain grades for his students. Which of the following are appropriate?

A.__ Get permission from the Department Chair first.

B.__ Use full disk encryption.

C.__ Maintain the files on his computer until he retires.

PER Example



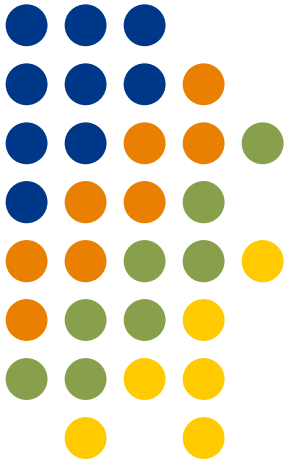
Professor Johnson uses his laptop to maintain grades for his students. Which of the following are appropriate?

A.  Get permission from the Department Chair first.

B.  Use full disk encryption.

C.  Maintain the files on his computer until he retires.

PHI: Protected Health Information



PHI: Protected Health Information

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
- Social security numbers
- Medical record numbers
- Account numbers
- Health plan beneficiary number
- Photographic or comparable images

PHI Safeguards

- ✓ DDD authorization must be documented.
- ✓ Unique identifier required for authentication.
- ✓ Encryption required for transmission and storage on laptops, PDAs and removable media.
- ✓ PHI usage in email must be authorized by the UF Privacy Office, sent only to ufl.edu addresses, and should be extremely rare.

PHI Safeguards

- ✓ Never transmit PHI by instant message.
- ✓ Workstations used with PHI must have a password protected screensaver with a short timeout.
- ✓ Do not remove from campus without DDD authorization.
- ✓ PHI must be disposed of securely.

More Information on PHI

Health Science Center security training
https://www.security.ufl.edu/staff/training.shtml

Privacy Office HIPAA training
http://privacy.ufl.edu/training/

Electronic Media Secure Disposal
https://www.security.health.ufl.edu/disposal

PHI Example

Dr. Roberts sometimes processes patient data on his PDA. What precautions should he take?

A.__ Lock his PDA when not in use.

B.__ Protect his PDA with a strong password.

C.__ Sync his PDA with his home computer.

D.__ Use UF wireless to send patient data from his PDA.

PHI Example

Dr. Roberts sometimes processes patient data on his PDA. What precautions should he take?

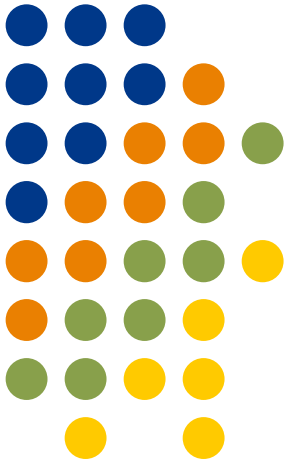
A.  Lock his PDA when not in use.

B.  Protect his PDA with a strong password.

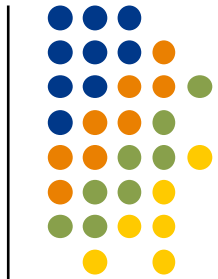
C.  Sync his PDA with his home computer.

D.  Use UF wireless to send patient data from his PDA.

Password Security



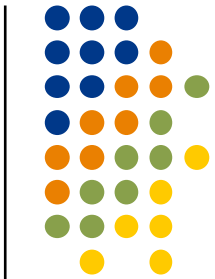
Password Safeguards



Password composition

- ✓ Long
- ✓ Complex
- ✓ Easy to remember

Passwords are Like Underwear



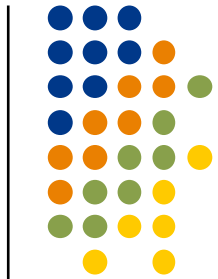
- ✓ Longer is better
- ✓ Change them often
- ✓ Be mysterious
- ✓ Don’t leave them laying around
- ✓ Don’t share them with friends

Password Safeguards

Password protection

- ✓ Don’t share with ANYONE, EVER!
  - Not even family members
  - Beware of “social engineering”
- ✓ If you must write it down:
  - Don't write the word 'password' on the note
  - Don't write your logon id on the same note
  - Disguise the password
  - Protect it like a credit card

Sample Passwords



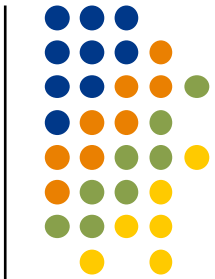
`Gator.Nation`

NO

`Gr82b@FlG8r`

BETTER

Sample Passwords



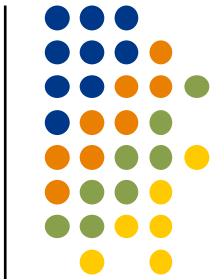
`JaneJohn`

NO

`nh0J.3n@J`

BETTER

Sample Passwords



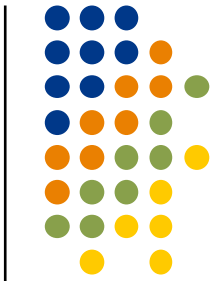
`Sept1101`

NO

`MLK121Ih@vedr3m`

BETTER

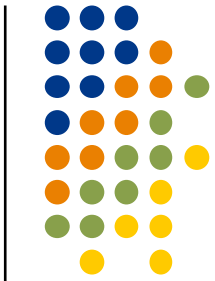
Sample Passwords



"Experience teaches you to recognize a mistake when you make it again."

Etu2r@mwymia

Password Example



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

A.___ Give him her GatorLink ID.

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

C.___ Direct him to public access wireless downtown or at local businesses.

Password Example

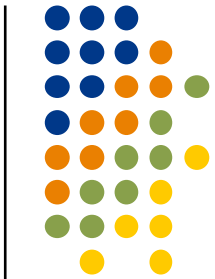
Jane's boyfriend doesn't go to UF. While visiting her in Gainesville, he wants to connect his computer to UF wireless network. What should Jane do?

A.  Give him her GatorLink ID.

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

C.  Direct him to public access wireless downtown or at local businesses.

Password Example



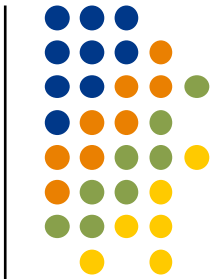
Mark just changed his GatorLink password. He used a complex password, but he's afraid he'll forget it. What should Mark do?

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.

Password Example



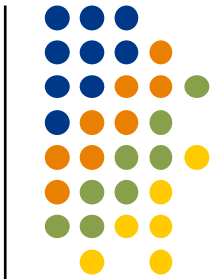
Mark just changed his GatorLink password. He used a complex password, but he's afraid he'll forget it. What should Mark do?

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.

Social Engineering Example



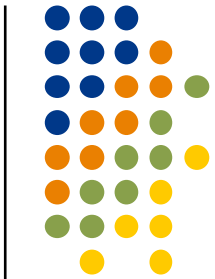
Sue gets a call from someone claiming to be a UF IT worker. He says that there's a problem with her GatorLink account and he needs her password to investigate. What should Sue do?

A.__ Give the caller her password.

B.__ Check caller ID. If it's a UF number, the give the caller her password.

C.__ Note the caller ID and report the call to her supervisor.

Social Engineering Example



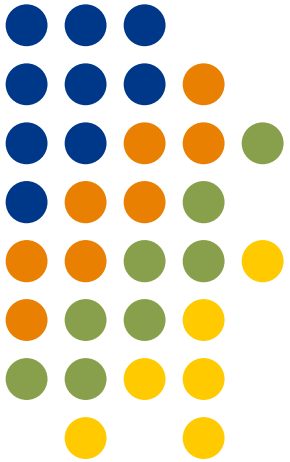
Sue gets a call from someone claiming to be a UF IT worker. He says that there's a problem with her GatorLink account and he needs her password to investigate. What should Sue do?

A. 👎 Give the caller her password.

B. 👎 Check caller ID. If it's a UF number, the give the caller her password.

C. 👍 Note the caller ID and report the call to her supervisor.

Encryption



Encryption

Storage

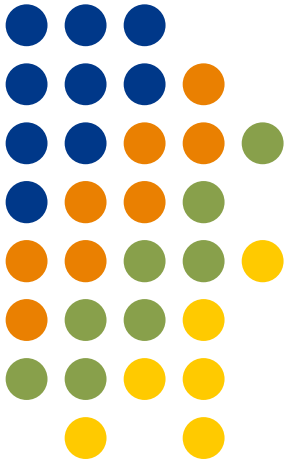
- ✓Encrypted content may be exempt from liability.
- ✓See your local IT worker for assistance.
- ✓Use method approved by Unit ISM.
  - File/Folder: NTFS, Truecrypt, PGP
  - Application: Winzip, Adobe Acrobat
  - Whole-disk: Bitlocker, Truecrypt, PGP-WDE

Encryption

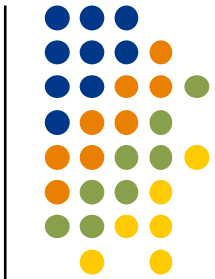
Transmission

- ✓Some methods are transparent to user.
- ✓Use method approved by Unit ISM.
  - Virtual Private Network (VPN)
  - SSL or https
  - SSH and SCP
  - SFTP
- ✓See your local IT worker.

Workstation Security



Workstation Safeguards



Can I store Restricted Data on my workstation?

- PCI: No
- PII: Requires special authorization and should be rare
- PER: Requires authorization
- PHI: Requires authorization

Workstation Safeguards

Avoid storing Restricted Data on your workstation

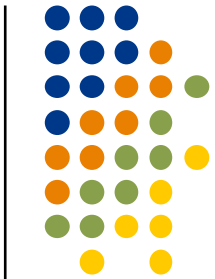
- ✓DDD authorization must be documented
- ✓Use computers maintained by UF IT workers and approved by Unit ISM
- ✓Position screen so it's not viewable to others
- ✓Lock the screen when unattended
  - ✓Automatically lock after a short time, maybe 5-15 min.
  - ✓Require a password to re-enter
- ✓Report exposed data to the Privacy Office

Workstation Safeguards

Avoid storing Restricted Data on your workstation.

- ✓Minimize the amount of data stored
- ✓Minimize the length of time it's stored
- ✓Use encryption
- ✓Maintain secure backups
- ✓Render unreadable before reuse or disposal

Workstation Example



A clerk in a UF medical clinic uses patient data from his 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.

Workstation Example

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

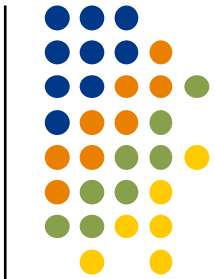
A.  When leaving the computer unattended, enable a password-protected screen saver.

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

C.  Configure a short screen saver time-out.

D.  Tape password to monitor so it's handy.

Workstation Example



A Payroll Clerk copies payroll data to his workstation to produce reports for his boss. What procedures should he follow?

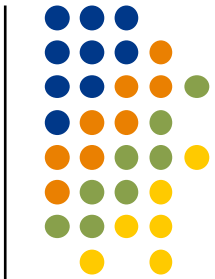
A.___ Obtain permission.

B.___ Minimize the amount of data on the workstation.

C.___ Encrypt the data.

D.___ Remove the data promptly when not needed.

Workstation Example



A Payroll Clerk copies payroll data to his workstation to produce reports for his boss. What procedures should he follow?

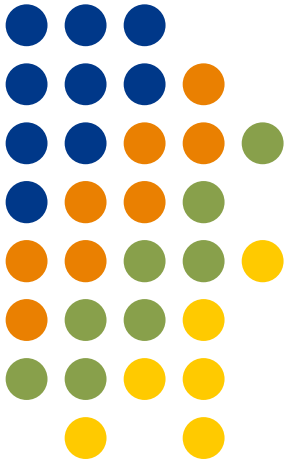
A. 👍 Obtain permission.

B. 👍 Minimize the amount of data on the workstation.

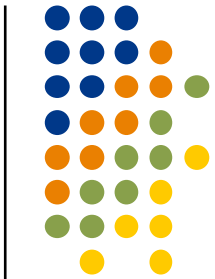
C. 👍 Encrypt the data.

D. 👍 Remove the data promptly when not needed.

Personally-Managed Computers



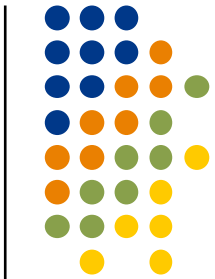
Personally-Managed Computer Safeguards



Can I store Restricted Data on my personally-managed computer?

- PCI: No
- PII: Requires authorization
- PER: Requires authorization
- PHI: Requires authorization

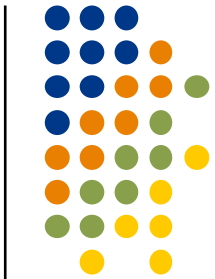
Personally-Managed Computer Safeguards



Avoid storing Restricted Data on personally-managed computers.

- ✓DDD authorization must be documented
- ✓DDD authorization required to remove from campus
- ✓Get device approval from the Unit ISM
- ✓Minimize the amount of data stored
- ✓Minimize the length of time it's stored
- ✓Use strong passwords

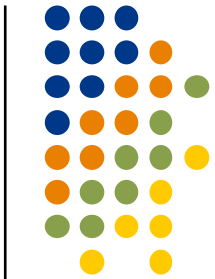
Personally-Managed Computer Safeguards



Avoid storing Restricted Data on personally-managed computers.

- ✓Maintain current software updates
- ✓Maintain current anti-virus updates
- ✓Use a firewall
- ✓Use whole-disk encryption
- ✓Maintain secure backups
- ✓Report exposed data immediately to UF Privacy Office
- ✓Render unreadable upon reuse or disposal

Personally-Managed Computer Example



A professor in Engineering manages his own computer. He needs to process student grades on his computer. What precautions should take?

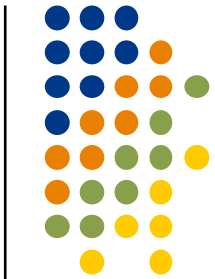
A.___ He's a professor, so he doesn't need authorization.

B.___ Minimize the amount of grades and length of time it's stored.

C.___ Firewall his computer.

D.___ Let graduate students use his computer.

Personally-Managed Computer Example



A professor in Engineering manages his own computer. He needs to process student grades on his computer. What precautions should take?

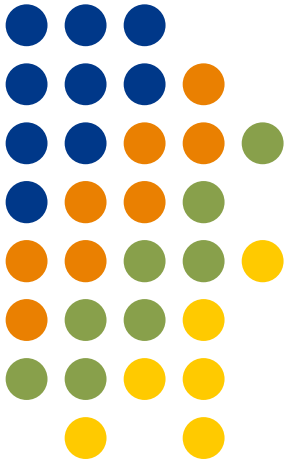
A. 👎 He's a professor, so he doesn't need authorization.

B. 👍 Minimize the amount of grades and length of time it's stored.

C. 👍 Firewall his computer.

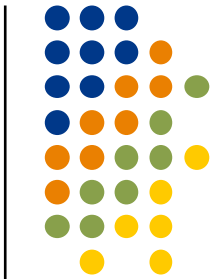
D. 👎 Let graduate students use his computer.

Portable Devices and Removable Media



Portable Device Safeguards

Laptops, PDAs, cell phones

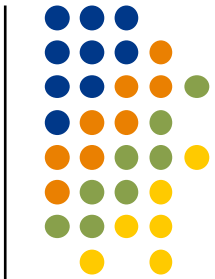


Can I store Restricted Data on my laptop or PDA?

- PCI: No
- PII: No
- PER: Requires authorization
- PHI: Requires authorization

Portable Device Safeguards

Laptops, PDAs, cell phones

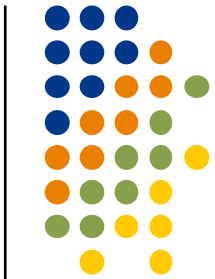


Avoid storing Restricted Data on portable devices

- ✓DDD authorization must be documented
- ✓DDD authorization required to remove from campus
- ✓Use devices maintained by UF IT workers and approved by the Unit ISM
- ✓Use whole-disk encryption
- ✓Maintain secure backups

Portable Device Safeguards

Laptops, PDAs, cell phones

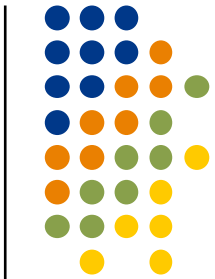


Avoid storing Restricted Data on portable devices.

- ✓Minimize the amount of data stored
- ✓Minimize the length of time it's stored
- ✓Don't synchronize with home computer
- ✓Protect device as you would a wallet or purse
- ✓Report lost devices to the UF Privacy Office
- ✓Render unreadable upon reuse or disposal

Removable Media Safeguards

CDs, DVDs, USB drives, external hard drives, floppy disks, backup tapes

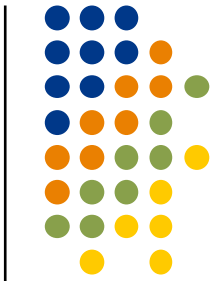


Can I store Restricted Data on removable media?

- PCI: No
- PII: Requires special authorization and should be rare
- PER: Requires authorization
- PHI: Requires authorization

Removable Media Safeguards

CDs, DVDs, USB drives, external hard drives, floppy disks, backup tapes

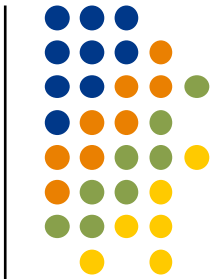


Avoid storing Restricted Data on removable media.

- ✓DDD authorization must be documented
- ✓DDD authorization required to remove from campus
- ✓Use media maintained by UF IT workers and approved by the Unit ISM
- ✓Use encryption
- ✓Maintain secure backups

Removable Media Safeguards

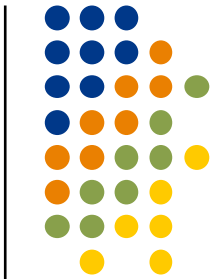
CDs, DVDs, USB drives, external hard drives, floppy disks, backup tapes



Avoid storing Restricted Data on removable media.

- ✓Minimize the amount of data stored
- ✓Minimize the length of time it's stored
- ✓Protect media as you would a wallet or purse
- ✓Report lost media immediately to UF Privacy Office
- ✓Render unreadable upon reuse or disposal

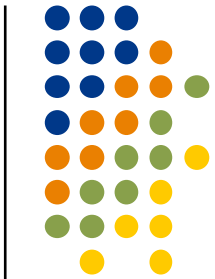
Home and Travel Safeguards



Can I store Restricted Data on my home or travel computer?

- PCI: No
- PII: Requires special authorization and should be rare
- PER: Requires authorization
- PHI: Requires authorization

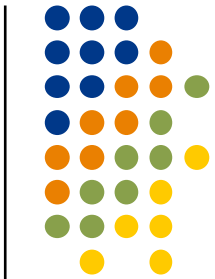
Home and Travel Safeguards



Avoid using Restricted Data at home or when traveling:

- ✓DDD authorization must be documented
- ✓DDD authorization required to remove from campus
- ✓Use whole-disk encryption
- ✓Make a backup before you travel
- ✓Use the UF VPN to connect with UF servers

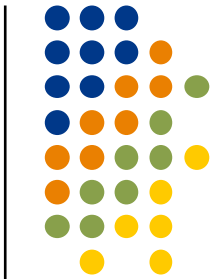
Home and Travel Safeguards



Avoid using Restricted Data at home or when traveling:

- ✓Use strong passwords
- ✓Maintain current anti-virus and updates
- ✓Minimize amount of data and length of time
- ✓Protect portable devices and media like a wallet
- ✓Consider remote data destruction software
- ✓Consider device tracking software

Portable Device Example



Dr. Adams uses patient data on his laptop. What should he do to protect the data?

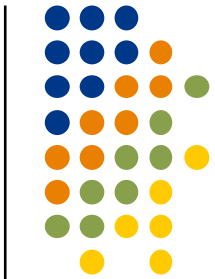
A.___ Encrypt the entire hard drive.

B.___ Remove the data when it's no longer needed.

C.___ Install remote data destruction and tracking software in case of lose or theft.

D.___ Ensure the data is unrecoverable when the laptop is surveyed.

Portable Device Example



Dr. Adams uses patient data on his laptop. What should he do to protect the data?

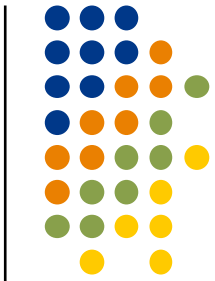
A.  Encrypt the entire hard drive.

B.  Remove the data when it's no longer needed.

C.  Install remote data destruction and tracking software in case of loss or theft.

D.  Ensure the data is unrecoverable when the laptop is surveyed.

Removable Media Example



CDs are used by the Academic Advisor in the Math Department to archive student records.

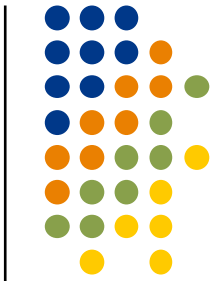
A.__ Encrypt the data on the CDs.

B.__ Store the CDs in a locked cabinet.

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.

Removable Media Example



CDs are used by the Academic Advisor in the Math Department to archive student records.

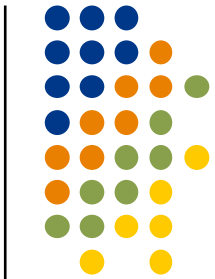
A. 👍 Encrypt the data on the CDs.

B. 👍 Store the CDs in a locked cabinet.

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.

Home Example



Professor Jones processes student grades on his home computer. How should he protect the data?

A.___ Use current anti-virus software.

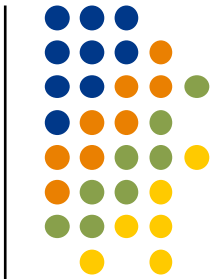
B.___ Maintain current updates.

C.___ Encrypt the data.

D.___ Remove the data promptly when no longer needed.

E.___ Share the computer with trusted family members.

Home Example



Professor Jones processes student grades on his home computer. How should he protect the data?

A.  Use current anti-virus software.

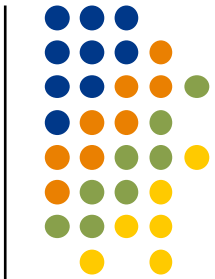
B.  Maintain current updates.

C.  Encrypt the data.

D.  Remove the data promptly when no longer needed.

E.  Share the computer with trusted family members.

Travel Example



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

A.___ Use whole-disk encryption.

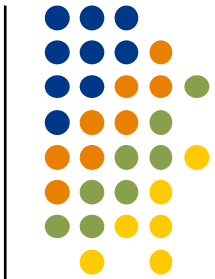
B.___ Remove unnecessary data.

C.___ Make a backup before he travels.

D.___ Use the UF VPN to communicate from Europe to UF.

E.___ Use a strong password on his laptop.

Travel Example



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

A. 👍 Use whole-disk encryption.

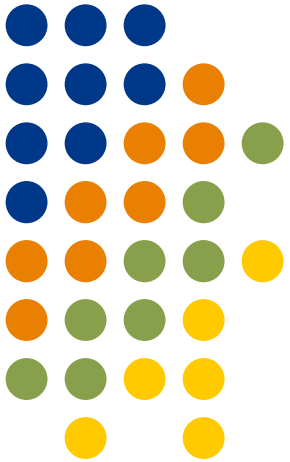
B. 👍 Remove unnecessary data.

C. 👍 Make a backup before he travels.

D. 👍 Use the UF VPN to communicate from Europe to UF.

E. 👍 Use a strong password on his laptop.

Email, Web and Instant Messaging Security

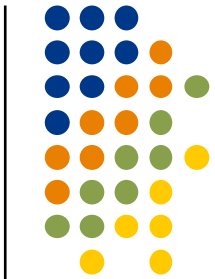


Email Safeguards

Can I send Restricted Data in email?

- PCI: No
- PII: Requires special authorization and should be rare
- PER: Requires special authorization and should be rare
- PHI: Requires special authorization and should be rare

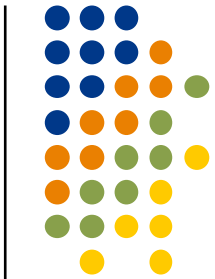
Email Safeguards



Avoid sending Restricted Data in email

- ✓ DDD authorization must be documented
- ✓ Use email software and methods approved by the Unit ISM
- ✓ In the email body, identify as Restricted Data and provide handling instructions

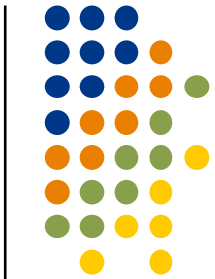
Email Safeguards



Avoid sending Restricted Data in email

- ✓ Minimize the amount of data sent
- ✓ Minimize the number of recipients; no lists
- ✓ Send only to email addresses ending in ufl.edu
- ✓ Double-check the recipient list. Beware of auto-completion features

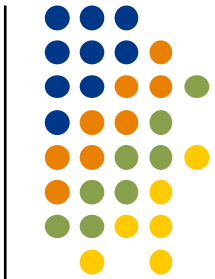
Instant Messaging Safeguards



Can I send Restricted Data in instant messages?

- PCI: No
- PII: No
- PER: Requires special authorization and should be rare
- PHI: No

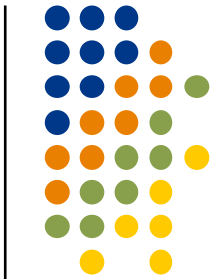
Instant Messaging Safeguards



Avoid sending Restricted Data via any IM.

- ✓DDD authorization must be documented
- ✓Do not use Restricted Data with commercial instant messaging services such AOL, Yahoo, or MSN
- ✓Do not use IM to send and receive attached files
- ✓Use software and methods approved by Unit ISM

Instant Messaging Safeguards



Avoid sending Restricted Data via any IM.

- ✓In the message, identify as Restricted Data and provide handling instructions
- ✓Minimize the amount of data
- ✓Minimize the number of recipients
- ✓Send only to IM addresses ending in ufl.edu
- ✓Double-check the recipient list

Web Safeguards

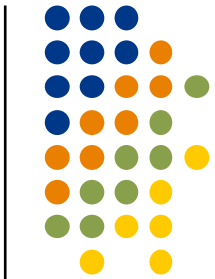
Can I use Restricted Data on the web?

- PCI: Requires authorization
- PII: Requires authorization
- PER: Requires authorization
- PHI: Requires authorization

Web Safeguards

- ✓ Beware of phishing scams. Never follow links in email or instant messages
- ✓ Use browser, configuration and methods approved by Unit ISM
- ✓ Use Restricted Data only with approved UF web sites
- ✓ Do not use features to remember or auto-complete passwords
- ✓ Look for the lock or https in the url 

Email Example



The Registrar's office needs to send email to Academic Advising listing student admission data. What procedures should be followed?

A.__ Obtain permission from the Registrar.

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.

Email Example

The Registrar's office needs to send email to Academic Advising listing student admission data. What procedures should be followed?

A. 👍 Obtain permission from the Registrar.

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.

Instant Messaging Example

Jane keeps in touch with her friend in accounting via AOL instant messenger. What should Jane know about instant messaging?

A.___ Never use AOL for official UF business.

B.___ Authorization must be documented before sending Restricted Data via instant message.

C.___ Avoid sending Restricted Data via any instant messaging service.

Instant Messaging Example

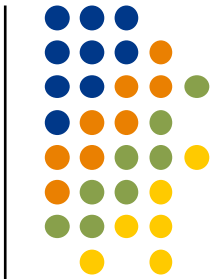
Jane keeps in touch with her friend in accounting via AOL instant messenger. What should Jane know about instant messaging?

A.  Never use AOL for official UF business.

B.  Avoid sending Restricted Data via any instant messaging service.

C.  Authorization must be documented before sending Restricted Data via instant message.

Web Example



Professor Carter puts grades on his web site for his students. Which of the following is allowed?

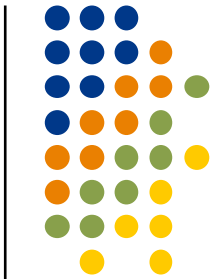
A.___ Use the student's name to identify their grade.

B.___ Limit access to the ufl.edu network.

C.___ Require authentication to access their grades.

D.___ Remove the data when the semester ends.

Web Example



Professor Carter puts grades on his web site for his students. Which of the following is allowed?

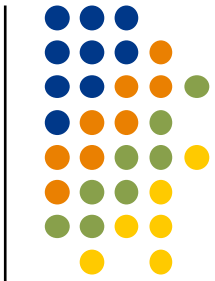
A. 👎 Use the student's name to identify their grade.

B. 👍 Limit access to the ufl.edu network.

C. 👍 Require authentication to access their grades.

D. 👍 Remove the data when the semester ends.

Phishing Example



The Academic Advisor gets an email from her bank about a problem with her account. A link is provided to the bank's web site. Which of following are appropriate?

A.___ Follow the link to fix the account problem.

B.___ Call her bank to inquire about the problem.

C.___ Go to the bank's web site using a Google link.

D.___ Go to the bank's web site using a bookmark.

E.___ Delete the email.

Phishing Example

The Academic Advisor gets an email from her bank about a problem with her account. A link is provided to the bank's web site. Which of following are appropriate?

A.  Follow the link to fix the account problem.

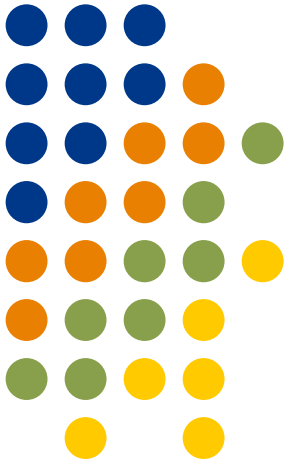
B.  Call her bank to inquire about the problem.

C.  Go to the bank's web site using a Google link.

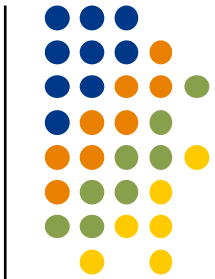
D.  Go to the bank's web site using a bookmark.

E.  Delete the email.

Reuse and Disposal Security

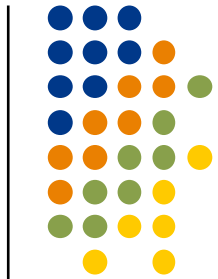


Disposal Safeguards



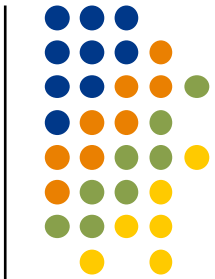
- ✓ Consult your local IT Worker for approved reuse and disposal methods
- ✓ Render Restricted Data unreadable before media reuse or disposal. Protect it until this can be done
- ✓ Maintain inventory of data that must be stored or transported prior to reuse or destruction
- ✓ Use only UF-approved reuse and disposal methods

Disposal Tools



- ✓ Hard drives
  - ✓ Derik's Boot and Nuke 3 pass overwrite
  - ✓ Others: http://www.fa.ufl.edu/am/destroy-data.asp
- ✓ Paper or cdroms
  - ✓ Shredder
- ✓ Disposal vendors
  - ✓ UF Cintas contract

Disposal Example



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

A.___ Leave it to the survey office.

B.___ Contact your Unit Information Security Manager for instructions.

C.___ A three-pass over-write of the hard drive.

D.___ Use a certified disposal contractor.

Disposal Example

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

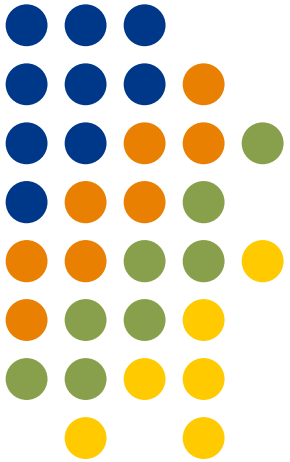
A.  Leave it to the survey office.

B.  Contact your Unit Information Security Manager for instructions.

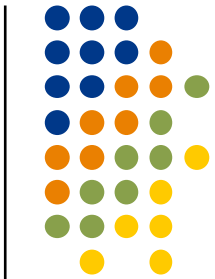
C.  A three-pass over-write of the hard drive.

D.  Use a certified disposal contractor.

IT Data Security Contacts



UF Incident Response Team



Kathy Bergsma

UF Information Security Manager

392-2061

ufirt@ufl.edu

http://infosec.ufl.edu/

UF Privacy Office

Susan Blair, Chief Privacy Officer

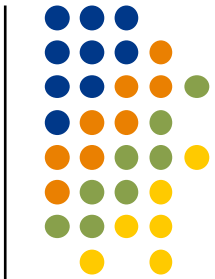
Office phone: 392-2094

Privacy Hotline: 866-876-4472

Email: privacy@ufl.edu

Web: http://privacy.ufl.edu/

Unit Contacts



Health Science Center

Colleen Ebel, HSC 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/

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