The College of DuPage
Security Management Training

Developed by the IT department
What is this Security Management Training all about?
What is this Security Management Training all about?

- Understanding why we need Security Management training
What is this Security Management Training all about?

- Understanding why we need Security Management training
- Understanding what data is considered “sensitive” and requires protection
What is this Security Management Training all about?

- Understanding why we need Security Management training
- Understanding what data is considered “sensitive” and requires protection
- Understanding good/required practices for protecting sensitive data
What is this Security Management Training all about? - continued

- Understanding what is the allowable use of the college computer infrastructure, including your PC, telephone, and FAX.
What is this Security Management Training all about? - continued

- Understanding what is the allowable use of the college computer infrastructure, including your PC, telephone, and FAX.
- Knowing where to get help if you are unsure about any Security Management topic.
What is this Security Management Training all about? - continued

- Understanding what is the allowable use of the college computer infrastructure, including your PC, telephone, and FAX.
- Knowing where to get help if you are unsure about any Security Management topic.
- Being able to demonstrate that Security Management training has been periodically delivered and understood by all COD staff.
Why do we need to do Security Management training?
Why do we need to do Security Management training?

- Federal Regulations
Why do we need to do Security Management training?

- Federal Regulations
- State Regulations
Why do we need to do Security Management training?

- Federal Regulations
- State Regulations
- Industry Standards
Why do we need to do Security Management training?

- Federal Regulations
- State Regulations
- Industry Standards
- Industry Best Practices
Why do we need to do Security Management training?

- Federal Regulations
- State Regulations
- Industry Standards
- Industry Best Practices
- It is good Business!
What happens if the college does not do Security Management training?
What happens if the college does not do Security Management training?

- Audits
What happens if the college does not do Security Management training?

- Audits
- Failing an Audit
  - Fines
  - Lost Revenues
  - Limitations on how the college does business
Two Parts to Security Management
Two Parts to Security Management

- Protecting Data
Two Parts to Security Management

- Protecting Data
- Protecting the Computer Infrastructure – both from abuse and misuse
What Data is “Sensitive” and Needs Heightened Protection?
What Data is “Sensitive” and Needs Heightened Protection?

Here at the college of DuPage, personal information is defined as an individual’s **name** (last name and first name or initial), in combination with any of the following data:

- Social security number
- Student education records
- Driver’s license number or identification card number
- Financial account number, credit or debit card number with personal identification number such as an access code, security codes or password that would permit access to an individual’s financial account.
- Home address or e-mail address
- Medical or health information
- Date of birth
Where at the college does sensitive data exist?
Where at the college does sensitive data exist?

- Sensitive data exists in the following places (not meant to be an exhaustive list):
  - Student Educational Records
  - Tuition and fee payment records
  - Financial Aid / Student Loan applications
  - COD Foundation donor records
  - Human Resource records
  - Health and Special Services records
  - Health records from college clinical programs, e.g. Dental Hygiene
Where at the college does sensitive data exist?

- Sensitive data exists in the following places (not meant to be an exhaustive list):
  - Student Educational Records
  - Tuition and fee payment records
  - Financial Aid / Student Loan applications
  - COD Foundation donor records
  - Human Resource records
  - Health and Special Services records
  - Health records from college clinical programs, e.g. Dental Hygiene

- Protected/sensitive data and information includes both paper (hard-copy) and electronic records
Protecting Sensitive Data - Good Practices
Protecting Sensitive Data - Good Practices

- Provide physical security
Protecting Sensitive Data - Good Practices

- Provide physical security
- Maintain access control to those who “need to know”
Protecting Sensitive Data - Good Practices

- Provide physical security
- Maintain access control to those who “need to know”
- Use strong passwords & change them frequently
Protecting Sensitive Data - Good Practices

- Provide physical security
- Maintain access control to those who “need to know”
- Use strong passwords & change them frequently
- DO NOT open email (or attachments) from someone you do not know
Protecting Sensitive Data - Good Practices

- Provide physical security
- Maintain access control to those who “need to know”
- Use strong passwords & change them frequently
- DO NOT open email (or attachments) from someone you do not know
- Referring calls & (e)mail asking for sensitive data to trained personnel
Protecting Sensitive Data - Good Practices

- Provide physical security
- Maintain access control to those who “need to know”
- Use strong passwords & change them frequently
- DO NOT open email (or attachments) from someone you do not know
- Referring calls & (e)mail asking for sensitive data to trained personnel
- Shredding paper & erasing electronic files
Protecting Sensitive Data - Good Practices

- Provide physical security
- Maintain access control to those who “need to know”
- Use strong passwords & change them frequently
- DO NOT open email (or attachments) from someone you do not know
- Referring calls & (e)mail asking for sensitive data to trained personnel
- Shredding paper & erasing electronic files
- Limiting views (screens/paper) & never leave desk with sensitive data in view of a casual passer-by
Protecting Sensitive Data - Good Practices

- Provide physical security
- Maintain access control to those who “need to know”
- Use strong passwords & change them frequently
- DO NOT open email (or attachments) from someone you do not know
- Referring calls & (e)mail asking for sensitive data to trained personnel
- Shredding paper & erasing electronic files
- Limiting views (screens/paper) & never leave desk with sensitive data in view of a casual passer-by
- Erasing screens / using password activated screensavers
Protecting Sensitive Data - Good Practices

- Provide physical security
- Maintain access control to those who “need to know”
- Use strong passwords & change them frequently
- DO NOT open email (or attachments) from someone you do not know
- Referring calls & (e)mail asking for sensitive data to trained personnel
- Shredding paper & erasing electronic files
- Limiting views (screens/paper) & never leave desk with sensitive data in view of a casual passer-by
- Erasing screens / using password activated screensavers
- Report suspicious activity to supervisor or Public Safety, as appropriate
Protecting the College Computer Infrastructure (e.g., PC, telephone, FAX)
Protecting the College Computer Infrastructure (e.g., PC, telephone, FAX)

- Personal use is discouraged
Protecting the College Computer Infrastructure (e.g., PC, telephone, FAX)

- Personal use is discouraged
- Must support the college and its mission.
Protecting the College Computer Infrastructure (e.g., PC, telephone, FAX)

- Personal use is discouraged
- Must support the college and its mission.
- “Those who use College computer facilities must do so reasonably; i.e., comply with public law, all college policies and guidelines, and reasonable standards of professional and personal courtesy and conduct.” College Policy/Procedure 6114
Protecting the College Computer Infrastructure (e.g., PC, telephone, FAX)

- Personal use is discouraged
- Must support the college and its mission.
- “Those who use College computer facilities must do so reasonably; i.e., comply with public law, all college policies and guidelines, and reasonable standards of professional and personal courtesy and conduct.” College Policy/Procedure 6114
- Your job defines “allowable use”
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements or promotions
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements or promotions
- Obtain personal financial gain
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements or promotions
- Obtain personal financial gain
- Overload any technology capacities
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements or promotions
- Obtain personal financial gain
- Overload any technology capacities
- Violation of any other college policy
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements or promotions
- Obtain personal financial gain
- Overload any technology capacities
- Violation of any other college policy
- Do anything that is inconsistent with “Allowable Use”
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements or promotions
- Obtain personal financial gain
- Overload any technology capacities
- Violation of any other college policy
- Do anything that is inconsistent with “Allowable Use”
- Do anything with a false identity
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements or promotions
- Obtain personal financial gain
- Overload any technology capacities
- Violation of any other college policy
- Do anything that is inconsistent with “Allowable Use”
- Do anything with a false identity
- Interfere with the College electronic communications infrastructure
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements or promotions
- Obtain personal financial gain
- Overload any technology capacities
- Violation of any other college policy
- Do anything that is inconsistent with “Allowable Use”
- Do anything with a false identity
- Interfere with the College electronic communications infrastructure
- Incur costs to the college
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements or promotions
- Obtain personal financial gain
- Overload any technology capacities
- Violation of any other college policy
- Do anything that is inconsistent with “ Allowable Use”
- Do anything with a false identity
- Interfere with the College electronic communications infrastructure
- Incur costs to the college
- Compromise the college mission
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements or promotions
- Obtain personal financial gain
- Overload any technology capacities
- Violation of any other college policy
- Do anything that is inconsistent with “Allowable Use”
- Do anything with a false identity
- Interfere with the College electronic communications infrastructure
- Incur costs to the college
- Compromise the college mission
- Clash with the employee’s job duties
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements or promotions
- Obtain personal financial gain
- Overload any technology capacities
- Violation of any other college policy
- Do anything that is inconsistent with “Allowable Use”
- Do anything with a false identity
- Interfere with the College electronic communications infrastructure
- Incur costs to the college
- Compromise the college mission
- Clash with the employee’s job duties
- Send disruptive, destructive, or unproductive email
What are examples of NOT “allowable use” (e.g. PC, telephone, FAX)

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements or promotions
- Obtain personal financial gain
- Overload any technology capacities
- Violation of any other college policy
- Do anything that is inconsistent with “Allowable Use”
- Do anything with a false identity
- Interfere with the College electronic communications infrastructure
- Incur costs to the college
- Compromise the college mission
- Clash with the employee’s job duties
- Send disruptive, destructive, or unproductive email
- Misrepresent the college
Who is responsible for helping maintain the college-wide Security Management program?
Who is responsible for helping maintain the college-wide Security Management program?

YOU!
Where do I get help to understand anything about Security Management here at the college
Where do I get help to understand anything about Security Management here at the college

- Start with your supervisor
Where do I get help to understand anything about Security Management here at the college

- Start with your supervisor
- If you or your supervisor still need help, contact Keith Conlee, Chief Security Officer – IT, x3055, conlee@cod.edu
Demonstrating that Security Management Training has been delivered and understood

Please answer the following six (6) questions about the information that was just presented.
Q1: Along with a person’s first and last name what other data listed below would be considered sensitive data?

A. Credit Card number
B. Doctor’s physical exam report
C. Social Security Number
D. All of the above
Q2: True or False – Sensitive data only exists in electronic form?

A. True
B. False
Q3: Which of the following is not a good practice for protecting sensitive data in your work-area?

A. Selecting a “strong” password that is not easily guessable by strangers or people who know you.
B. Lock office and desk drawers containing sensitive data when away from work-area.
C. Erase electronic files and shred paper files containing sensitive data when no longer needed for college business.
D. Share passwords among co-workers because we all do the same work.
Q4: What item below would be considered allowable use of the college computer infrastructure?

A. Checking the betting odds on a sporting event and placing a bet.
B. Forwarding political materials to college employees about a candidate you support
C. Electronically discussing higher education trends and practices with peer colleagues at other educational related institutions.
D. Downloading a digital version of a movie for my family to watch over the weekend.
Q5: Which COD employees are responsible for making sure security initiatives to protect sensitive data and the computing infrastructure are carried out?

A. Only IT Security
B. Only Supervision
C. Only Public Safety
D. All COD Employees
Q6: If you are unsure about anything that has to do with Security Management for sensitive data or the College computer infrastructure, whom should you contact first?

A. IT Security
B. Human Resources
C. Public Safety
D. Your Supervisor / Management