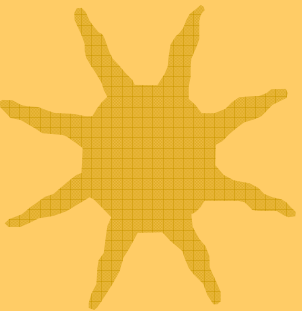
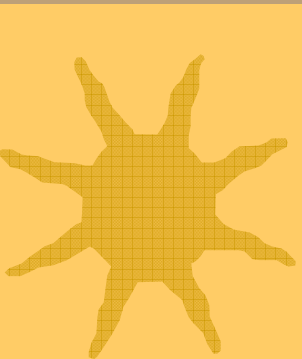


# *Developing A Comprehensive Approach To Handling Confidential/Sensitive Data*

---



*Darlene Quackenbush*  
*IT Planning & Information Security Officer*  
*James Madison University*

*Shirley Payne*  
*Director, Security Coordination & Policy*  
*University of Virginia*

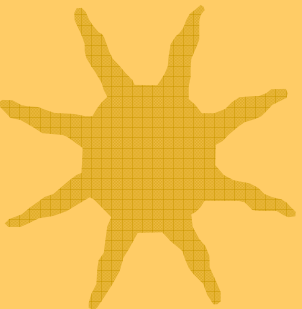
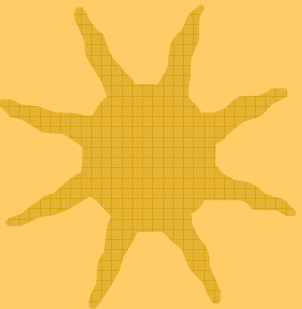
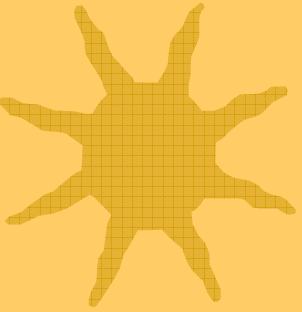
*Association of Collegiate Computing Services Conference, April 18, 2007*



# *Agenda*

---

- The Gathering Storm
  - Problem defined
  - Challenges ahead
- A Ray of Sunshine
  - EDUCAUSE Data Handling Blueprint
  - JMU and UVA Strategies
- Discussion





# *Rain Drops Keep Falling On My Head...*

---

- *February 7, 2007. Nine backup computer tapes sent out in late December for conversion to microfiche were not returned, Johns Hopkins announced. The tapes contained personal information on university employees and Johns Hopkins Hospital patients. Johns Hopkins believes it is very likely that the tapes were inadvertently destroyed.*



# *Rain Drops Keep Falling On My Head...*

---

- *December 21, 2006.* **MSU SUFFERS DATA MISHAP.** Officials from Mississippi State University (MSU) have notified approximately 2,400 students and employees that their confidential information was mistakenly made available on a public Web site.

# *Rain Drops Keep Falling On My Head...*

---

- *December 12, 2006. **UCLA Probes Computer Security Breach.** Officials at the University of California Los Angeles alerted about 800,000 current and former students, faculty and staff on Tuesday that their names and certain personal information were exposed after a hacker broke into a campus computer system.*

# *Just How Stormy Is It?*

---

- 1.9 billion electronic records reported exposed from 1980 to 2006
- Rate is increasing. Current rate is 672 records every 5 minutes!
- Higher Education accounts for one-third of all incidents, although <1% of total lost records.

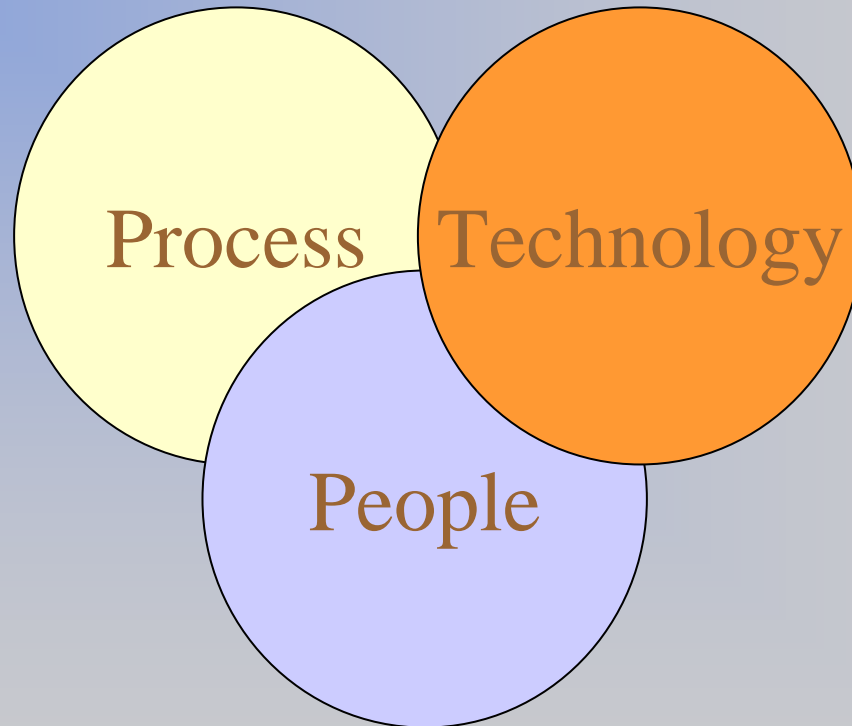
# *Consequences*

---

- Strategic, e.g. loss of intellectual property
- Financial, e.g. regulation penalties, cost of notifications
- Legal, e.g. lawsuits
- Operational, e.g. critical system downtime
- Reputational, e.g. loss of trust

# *Security Relies On...*

---



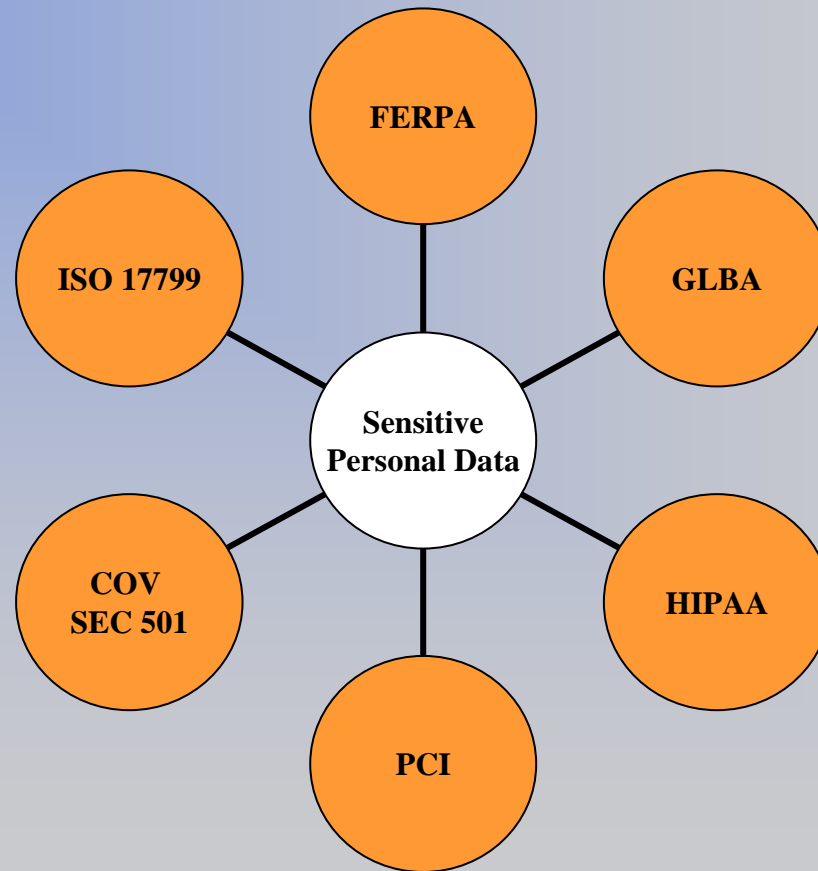
# *Why Is Security So Hard?*

---

- Cultural issues
- Lack of awareness
- No technical silver bullet
- Determined opponents & commercial value of data
- Absence and enforcement of policies

# *And if that weren't enough...COMPLIANCE*

---





# *A Ray of Sunshine – A comprehensive approach*

---

## EDUCAUSE Confidential Data Handling Blueprint

### Purpose

- To provide a list of key strategies to follow for stopping the leakage of confidential/sensitive data.
- To provide a toolkit that constructs resources pertaining to confidential/sensitive data handling.

<https://wiki.internet2.edu/confluence/display/secguide/Confidential+Data+Handling+Blueprint>

# *A Comprehensive Approach*

---

- Step 1: Create a security risk-aware culture that includes an information security risk management program
- Step 2: Define institutional data types
- Step 3: Clarify responsibilities and accountability for safeguarding confidential/sensitive data
- Step 4: Reduce access to confidential/sensitive data not absolutely essential to institutional processes
- Step 5: Establish and implement stricter controls for safeguarding confidential/sensitive data
- Step 6: Provide awareness and training
- Step 7: Verify compliance routinely with your policies and procedures



# *Illustrating Its Use*

---

- JMU sensitive data workgroup
- UVA sensitive data handling initiative



# *EDUCAUSE Blueprint Step 1*

---

1. Create security risk-aware culture that includes an information security risk management program
  - 1.1 Institution-wide security risk management program
  - 1.2 Roles and responsibilities defined for overall information security at the central and distributed level
  - 1.3 Executive leadership support in the form of policies and governance actions

# *EDUCAUSE Blueprint Step 2*

---

## 2. Define institutional data types

- 2.1 Compliance with applicable federal and state laws and regulations - as well as contractual obligations - related to privacy and security of data held by the institution (also consider applicable international laws)
- 2.2 Data classification schema developed with input from legal counsel and data stewards
- 2.3 Data classification schema assigned to institutional data to the extent possible or necessary

# *EDUCAUSE Blueprint Step 3*

---

3. Clarify responsibilities and accountability for safeguarding data
  - 3.1 Data stewardship roles and responsibilities
  - 3.2 Legally binding third party agreements that assign responsibility for secure data handling

# *EDUCAUSE Blueprint Step 4*

---

4. Reduce access to data not absolutely essential to institutional processes
  - 4.1 Data collection processes (including forms) should request only the minimum necessary confidential/sensitive information
  - 4.2 Application outputs (e.g., queries, hard copy reports, etc.) should provide only the minimum necessary confidential/sensitive information
  - 4.3 Inventory and review access to existing confidential/sensitive data on servers, desktops, and mobile devices

# *EDUCAUSE Blueprint Step 4 - continued*

---

4. Reduce access to data not absolutely essential to institutional processes
  - 4.4 Eliminate unnecessary confidential/sensitive data on servers, desktops, and mobile devices
  - 4.5 Eliminate dependence on SSNs as primary identifiers and as a form of authentication\*

\*Note: SSNs may need to be used for certain things (e.g., student employees, student financial aid, etc.) and we recommend that schools limit the use of SSNs to necessary processes only.

# *EDUCAUSE Blueprint Step 5*

---

5. Establish and implement stricter controls for safeguarding data
  - 5.1 Inventory and review/remediate security of devices
  - 5.2 Configuration standards for applications, servers, desktops, and mobile devices
  - 5.3 Network level protections
  - 5.4 Encryption strategies for data in transit and at rest



# *EDUCAUSE Blueprint Step 5 - continued*

---

5. Establish and implement stricter controls for safeguarding data
  - 5.5 Policies regarding confidential/sensitive data on mobile devices and home computers and for data archival/storage
  - 5.6 Identity management and resource provisioning processes
  - 5.7 Secure disposal of equipment and data
  - 5.8 Consider background checks on individuals handling confidential/sensitive data

# *EDUCAUSE Blueprint Step 6*

---

## 6. Provide awareness and training

- 6.1 Make confidential/sensitive data handlers aware of privacy and security requirements
- 6.2 Require acknowledgement by data users of their responsibility for safeguarding such data
- 6.3 Enhance general privacy and security awareness programs to specifically address safeguarding confidential/sensitive data
- 6.4 Collaboration mechanisms such as e-mail have strengths and limitations in terms of access control, which must be clearly communicated and understood so that the data will be safe-guarded



# *EDUCAUSE Blueprint Step 6 -- Resource*

---

**EDUCAUSE Security Awareness & Training Resources**

**<https://wiki.internet2.edu/confluence/display/secguide/Awareness+and+Training>**

# *EDUCAUSE Blueprint Step 7*

---

7. Verify compliance routinely with your policies and procedures
  - 7.1 Routinely test network-connected devices and services for weaknesses in operating systems, applications, and encryption
  - 7.2 Routinely scan servers, desktops, mobile devices, and networks containing confidential/sensitive data to verify compliance
  - 7.3 Routinely audit access privileges
  - 7.4 Procurement procedures and contract language to ensure proper data handling is maintained

# *EDUCAUSE Blueprint Step 7 - continued*

---

7. Verify compliance routinely with your policies and procedures
  - 7.5 System development methodologies that prevent new data handling problems from being introduced into the environment
  - 7.6 Utilize audit function within the institution to verify compliance
  - 7.7 Incident response policies and procedures
  - 7.8 Conduct regular meetings with stakeholders such as data stewards, legal counsel, compliance officers, public safety, public relations, and IT groups to review institutional risk and compliance and to revise existing policies and procedures as needed



# *EDUCAUSE Blueprint Step 7 - Resources*

---

Virginia Alliance for Secure Computing & Networking  
<http://vascan.org>

Information Security Governance Assessment Tool for Higher Education  
<http://www.educause.edu/ir/library/pdf/SEC0421.pdf>



# *Recommendations*

---

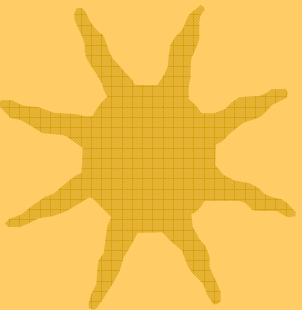
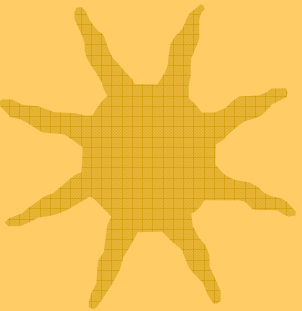
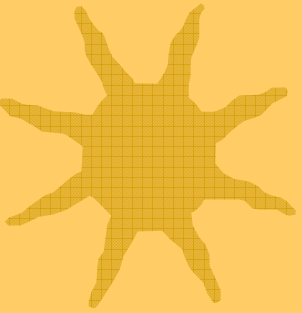
- Think broadly and get started
- Prioritize based on risk
- Find your allies
- Coordinate all needed work to ensure consistent solutions
- Communicate status widely



# *Discussion*

---

- What are your concerns about confidential/sensitive data handling?
- What solutions are being applied at your institutions?
- **QUESTIONS**





*Feel free to contact us...*

---

**Darlene Quackenbush – [quackedh@jmu.edu](mailto:quackedh@jmu.edu)**

**Shirley Payne – [payne@virginia.edu](mailto:payne@virginia.edu)**

