CAMPUS TECHNOLOGY 2007

Confidential Data Handling Blueprint

Personal Blueprint Worksheet

Step 1: Create a security risk-aware culture that includes an information security risk management program

Sub-step	Existing Efforts	To-Do
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		

Step 2: Define institutional data types

Sub-step	Existing Efforts	To-Do
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		

Step 3: Clarify responsibilities and accountability for safeguarding confidential/sensitive data

Sub-step	Existing Efforts	To-Do
3.1 Data stewardship roles and responsibilities		
3.2 Legally binding third party agreements that assign responsibility for secure data handling		

Step 4: Reduce access to confidential/sensitive data not absolutely essential to institutional processes

Sub-step	Existing Efforts	To-Do
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		
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		

Step 5: Establish and implement stricter controls for safeguarding confidential/sensitive data

Sub-step	Existing Efforts	To-Do
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		
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		

Step 6: Provide awareness and training

Sub-step	Existing Efforts	To-Do
6.1 Make confidential/sensitive data handlers aware of privacy and security requirements		
6.2 Require acknowledgment 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 Clearly communicate how to safeguard data so that collaboration mechanisms such as e-mail have strengths and limitations in terms of access control		

Step 7: Verify compliance routinely with your policies and procedures

Sub-step	Existing Efforts	To-Do
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		
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		