UP09-002: Sensitive Data and Security Policy
Responsible Executive: Chief Information Officer (CIO)
Responsible Office: Office of the CIO
Related Policy: UP09-001 Information Technology Resources Policy
Approval/Effective Date(s):
Revision Date:
Scheduled Review Date:

I. POLICY STATEMENT

The ability to collect and process information for administrative and academic purposes is critical to the University's mission. Information collected and processed may include personal information regarding students, employees or alumni. Users operating or utilizing JCU computing resources are responsible for managing and maintaining the security of the data, computing resources and protected information, including Sensitive Data. Protecting such information is driven by a variety of considerations including legal, academic, financial, and other business requirements. This is especially true if Sensitive Data is being sent via e-mail. In this age of mobility, e-mail is often carried on unsecured mobile devices such as Blackberries.

Sensitive Data will not be collected, accessed, disclosed or transmitted except as provided by University policy and procedures, or as required by operation of law or court order.

All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of Sensitive Data from unauthorized generation, access, modification, disclosure, transmission, or destruction.

II. PURPOSE

JCU must protect Sensitive Data and comply with laws and other University policies regarding the protection and use of Sensitive Data. This Policy provides a framework in order to ensure the privacy and security of that data.

III. DEFINITIONS

Please refer to Definitions section of Information Technology Resources Policy, UP09-001.

A. Sensitive Data. Data designated as private or confidential by law or by the University as detailed in UP09-001, IV (E).

B. **Portable Storage Devices and Media**. Includes (but is not limited to):

- Portable computers-Laptops/ Notebooks
- MP3/4 or other media players
- Cameras and mobile phones/camera phones
- External Hard Drives
- Zip® disks or drives
- CDs/DVDs
- Floppy disks
- Tapes
- Internet hosted storage
- E-mail
- USB "sticks" (e.g., memory sticks/pens, USB flash drives, etc.)

C. Please refer to UP09-001, for all other definitions.

IV. POLICY ELABORATION

A. **Functional Unit Responsibility**. Functional unit heads are responsible for implementing appropriate managerial, operations, physical, and technical controls for access to, use of, transmission of, and disposal of data in compliance with this Policy. This requirement is especially important for those computing resources that support or host critical business functions or Sensitive Data.

B. **Sensitive Data**. Some examples of Sensitive Data include: social security numbers, driver license numbers, credit card or other financial account numbers, JCU ID numbers, protected health information, financial data, educational records, intellectual property or research records, donor profiles, or any information that could result in a material risk of identity theft, a violation of FERPA, HIPPA or GLBA, or otherwise harm the legitimate financial and reputational interests of the University if unauthorized access is permitted, whether intentionally or unintentionally.

C. **Secure Storage**. Secure storage is available on University provided network attached storage: (e.g., "O-drive"). All Sensitive Data is to be stored either on the network attached storage or within other authorized institutional enterprise system (e.g., Banner, Adirondack, etc.). Storage on a PC, either University owned or personal is not considered secure unless the hard drive is properly encrypted.

D. **Downloading and Transporting**. Sensitive Data may not be downloaded to or transported on any Portable Storage Device and Media. This applies to both on-campus and off-campus downloading and transportation. As noted in this Policy, secure network attached storage is provided for this purpose. Sensitive Data may be downloaded and/or transported only with prior written consent of the appropriate Vice President. This consent will only be granted on a temporary, case-by-case basis.

E. **Use of Media or Equipment**. Users are to access University information on University-owned media or equipment. All information stored on University owned equipment, including but not limited to PCs, servers, and network attached storage, is considered the property of the University.

Users are not to store, communicate, transport, or process University information on personally owned media, devices, or computers without prior written approval from the appropriate Vice President and the approval of the personal equipment by Information Technology Services (ITS).

Information on University owned portable devices such as flash drives, disks, or laptop computers must be stored in physically secure locations and must not to be transported without encrypting the data using University approved software and techniques.

F. Encryption. Software, policies, and procedures for encrypting Sensitive Data are currently being developed and deployed by the University. Due to the scope of this work and the changing nature of technology inventory, the deployment of encryption is an ongoing process.

G. Ohio Breach Notification Act. The Ohio Breach Notification Act requires prompt notification to individuals whose personal information has been exposed if the incident could lead to fraud or identity theft. Any loss of Sensitive Data, disclosure of Sensitive Data to unauthorized individuals or suspected misuse of Sensitive Data must be immediately reported to the Office of the CIO.

H. Breach of this Policy. Violation of this Policy will be viewed as a serious disciplinary offense and will be addressed through the appropriate Vice President and the Office of Human Resources. Violations of this Policy may lead to disciplinary action up to and including dismissal, expulsion, and/or legal action. Current Functional Unit practices or procedures shall be adapted to comply with this Policy.