Header

Policy Name and Number: **Sensitive Data and Cybersecurity Policy** (JCU-IT-POL-100)

Policy Developer: Information Technology Services

Original Date: December 20, 2019

Approval Date: December 20, 2019; October 18, 2022 (Interim); May 2, 2024

Contact Person for Website: Director of IT Security

Body

POLICY

The ability to collect and process information for administrative and academic purposes is critical to John Carroll University's ("the University's") mission. Information collected and processed may include personal information regarding students, employees, or alumni. Users utilizing University Information Technology ("IT") Resources or Data are responsible for managing and maintaining the security of the data, IT 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.

All employees of the University community have a responsibility to protect the confidentiality, integrity, and availability of Sensitive Data from unauthorized collection, access, modification, disclosure, transmission, or destruction by following the Procedures below.

PURPOSE

The University must protect Sensitive Data and comply with laws and other University policies regarding the protection and use of Sensitive Data. This Policy reflects the University's cybersecurity program and provides a framework in order to ensure the privacy and security of Sensitive Data.

SCOPE

This policy pertains to all employees of the University.

PROCEDURES

A. All employees are required to comply with the provisions of this policy related to the privacy and security of Sensitive Data that is retained by any University employee in the

scope of their job duties or maintained on University IT Resources. These requirements include the following:

1. Sensitive Data will not be collected, accessed, or disclosed except as provided by University policy and procedures, or as required by operation of law or court order. Sensitive Data may only be transmitted over approved communication channels that have been analyzed and approved by Information Technology Services ("ITS"). Approved communication channels are listed in the Information Classification Matrix.
2. If Sensitive Data is to be transmitted to or stored on third-party "cloud" storage providers, those providers must be approved by ITS. The primary approved cloud storage providers are outlined in the Information Classification Matrix.
3. Sensitive Data may only be stored locally or transported on University-owned and controlled devices unless approval is first obtained from the division leader of the employee's department.
    a. Employees are permitted to use smartphones (examples: iPhone, Android) and tablet computers (examples: iPad, Android) to access cloud-based data for job-related purposes, provided the official Google-provided or ITS-specified apps are utilized. Other phone apps are not permitted. Users accessing such data acknowledge that JCU will have the ability and right to remotely delete such data in the event of loss or theft, and such loss must be reported to JCU ITS immediately.
    b. All portable devices containing Sensitive Data must be encrypted (see section F below for more information on process). Examples include portable storage (like USB flash drives and hard drives or SD/MicroSD Cards), smartphones, tablets, and laptops.
4. High Value Sensitive Data has additional handling and storage requirements due to its increased risk profile. The Information Classification Matrix provides guidelines for the handling and storage of High Value Sensitive Data.
5. FAFSA Data has additional privacy and handling requirements per the Undergraduate Talent by Unlocking Resources for Education Act (FUTURE Act). These requirements are detailed in the SEFS Data Sharing Policy.

B. Department Responsibility: Department heads are responsible for implementing appropriate managerial, physical, technical, and operational 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 High Value Sensitive Data. Additionally, requests for large sets of High Value Sensitive Data (e.g., a list of W-2s, Social Security numbers, or other similar Sensitive Data) from University administrators through email or other electronic methods must be verified either in person or with a phone call from the requestor

before complying with the request. Additional guidelines for data storage, transmission, and use restrictions are outlined in the Information Classification Matrix and other ITS guidelines.

C. Information System Inventory: The purchase, distribution, useful life, replacement and disposal of University IT-related device and equipment assets must be documented and verified. The IT Department will verify critical assets within inventory on at least an annual basis. Unauthorized additions or removals of critical hardware or software must be reported as a Security incident. The University will maintain an inventory of University-owned devices, equipment and systems, reviewed at least annually, that includes, but is not limited to:

A. Inventory of critical hardware and software, identifying at a minimum, asset type, location, and specific identifier information (Serial Number, Model numbers, etc.)
B. A list of IT-related devices and equipment and personnel with access to each such device or equipment;
C. List of University-approved products that may be utilized in connection with the University's systems and networks.

D. Security Awareness and Training: The University's CIO, in conjunction with the Director of IT Security, will develop and maintain a multi-faceted security awareness program as well as a process to communicate security program information and requirements, security training and awareness materials, and other security items of interest. All employees will be required to participate in specified, mandatory training in the program. This training will be aligned with the requirements of the Gramm-Leach-Bliley Act including specific training for IT staff as their position requires.

E. Endpoint Protection: All University managed/provided and non-University managed/provided computer systems are required to have an enterprise grade next-generation security platform capable of deep learning, detection and response to malware, spyware, exploits, ransomware, and other unauthorized programs/software installed on the Endpoint.

F. Secure Storage: Secure storage is available on University Google Drive accounts with two-factor authentication ("2FA") in place. Accounts without 2FA are not considered Secure Storage. Secure storage is also available on University-provided network attached storage (e.g., "O-drive"). Sensitive Data is to be stored on Google Drive with 2FA, or on the network attached storage ("O-drive"), or within other authorized University enterprise systems as outlined in the Information Classification Matrix. Storage is prohibited on any personal or unsupported cloud-based service (e.g., DropBox, Box, OneDrive) and in Google Drive used via a non-University account. Google Drive used via the individual's University account protected by Google 2FA is

the primary service for cloud storage of University Sensitive Data. Please see the Information Classification Matrix for additional guidelines.

G. Downloading and Transporting: High Value Sensitive Data should only be downloaded to or transported via University-provided and encrypted Portable Storage Devices and Media, and only if required. This applies to both on-campus and off-campus downloading and transportation. As noted in this Policy, secure network attached storage (i.e. "O drive") is provided for this purpose. High Value Sensitive Data may be downloaded and/or transported by other means only with prior written consent of the appropriate Vice President. This consent will only be granted on a temporary, case-by-case basis.

H. Use of Media or Equipment: Users are to access University Data on University-owned or approved 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 unless otherwise specified in a separate policy, agreement, Faculty Handbook provision, or contract.

The University, department heads, and ITS reserve the right to restrict or prohibit Users' ability to store, communicate, transport, or process University information on personally-owned media, devices, or computers.

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

I. Encryption: Software for encrypting Sensitive Data is available from ITS. Due to the scope of this work and the changing nature of technology inventory and the evolution of security risks, the acquisition and deployment of appropriate encryption technology is an ongoing process. Employees are required to encrypt Sensitive Data. Department heads are required to ensure employees are advised of the obligation to encrypt data appropriately in accordance with this Policy and the related Information Classification Matrix. Contact the ITS Service Desk or visit the ITS Encryption website for assistance in choosing and implementing an appropriate encryption mechanism.

J. Backup and Recovery: JCU IT maintains copies of business-critical data for recovery purposes for specified periods of time. The University maintains a Records Retention Policy that contains specific backup and recovery capabilities for business-critical data. For additional detail of specific backup and recovery retention periods, reference the Records Retention Policy. Backup data is encrypted and stored offsite with an internet

cloud-hosted service. Restoration testing will be performed no less than annually on the backup data.

K. Data Retention and Destruction: JCU has a Records Retention Policy to ensure that the University's records are being managed, maintained, and disposed/destroyed in a secure manner and that complies with all of the legal requirements regarding records retention. For additional information and details refer to the Records Retention Policy.

L. Device Disposal: JCU stores information on computer hard drives, server/file shares, within applications, and other forms of electronic media. As new equipment is obtained and older equipment/media reaches end of life, information stored on retiring equipment and media must be properly destroyed and otherwise made unreadable to protect the University, our users, and customers. Reference the Procedures for Sensitive Data Destruction for proper asset disposition procedures.

M. Security Authorization Process: JCU manages the security state of University systems through a security authorization process that follows the least privileged access model and designates individuals to fulfill specific roles and responsibilities within the JCU risk management process. The security authorization process is fully integrated and is followed University-wide as part of the risk management process.

N. Computer Administrator/Root/Privileged Access: JCU manages the security state of University systems through a security authorization process that follows the least privileged access model and by default, all John Carroll University employees are assigned standard access level rights on University-provided computers. Temporary access can be granted via the Service Desk; all other requests are approved by the CIO.

O. Privileged Account Segmentation: Persistent IT Administrator privileges, when required, will be approved by the CIO and will only be granted to a dedicated account that is separate from that IT Administrator's standard/employee (everyday use) account.

P. Penetration Testing and Asset-based Risk Assessment: The Chief Information Officer (CIO) and/or Director of IT Security are responsible for ensuring:

A. Penetration testing is performed against JCU managed IT resources no less than annually. For non-managed IT resources, the CIO or Director of IT Security/CISO shall ensure the appropriate requirements are contained in the Third-Party contracts.

B. All issues identified as a result of the penetration testing are appropriately remediated.

C. The penetration testing and remediation are appropriately documented, and risks are communicated to University senior leadership and, if requested, the Board of Directors.

D. Third-Party Vendor Assessment: All third-party vendors who provide, store, or manipulate sensitive data are subject to cybersecurity review before their product is

acquired in accordance with the University Purchasing Policy. Each vendor must be reviewed annually to ensure continued compliance.

Q. Regulatory & Non-Regulatory Compliance: JCU addresses information security issues in the development, implementation, and documentation to protect University's critical systems and Sensitive Data in accordance with applicable local, state, and federal laws, as well as non-regulatory requirements that a University is contractually bound to address. JCU leverages internal and external guidance on new or updated local, state, or federal laws and non-regulatory requirements on a regular basis.

R. Ohio Breach Notification Act: The Ohio Breach Notification Act requires prompt notification to individuals whose personal information has been subject to unauthorized access that compromises the security or confidentiality of the data and where there is a material risk that the access could result in 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.

S. Breach of this Policy: Violation of this policy will result in notification to the appropriate Vice President and will be grounds for corrective action under the appropriate University policies. Violations of this Policy may lead to corrective action up to and including termination, other appropriate discipline, and/or legal action. Current department practices or procedures must be adapted to comply with this Policy.

DEFINITIONS

A. Data: All information that is used by or belongs to the University, or that is processed, stored, posted, maintained, transmitted, copied on, or copied from University IT Resources.

B. Sensitive Data: Data designated as private or confidential by law or by the University. Sensitive Data includes, but is not limited to, employment records, medical records, student education records, personal financial records (or other sensitive personally identifiable information), protected research Data, trade secrets, classified government information, proprietary information of the University, or any Data that could harm the legitimate financial and reputational interests of the University if unauthorized access is permitted, whether intentionally or unintentionally.

Examples of Sensitive Data include: JCU ID numbers; protected health information; financial data; educational records; intellectual property records; protected research records; donor profiles; or any information that could result in a material risk of identity theft, a violation of the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), or the

Gramm-Leach-Bliley Act (GLBA), or otherwise harm the legitimate financial and reputational interests of the University if unauthorized access is permitted, whether intentionally or unintentionally. Sensitive Data shall not include records that by law must be made available to the general public.

C. High Value Sensitive Data: A sub-category of Sensitive Data that includes data that is particularly sensitive; has additional legal compliance requirements; or is a high volume aggregation of other Sensitive Data. Some examples of High Value Sensitive Data include social security numbers; driver license numbers; credit card, banking or other financial account numbers; and W-2 information. Data can be classified as High Value Sensitive Data by the Information Classification Matrix (See attachments), or the Chief Information Officer (CIO) or their designee.

D. FAFSA Data: Data provided to the institution via the Free Application for Federal Student Aid (FAFSA ®). This type of data has additional legal requirements regarding its security.

E. Portable Storage Devices and Media include (but are not limited to) the following:

- smartphones and smart watches (iPhone, Android),
- tablet computers (iPad, Android, Surface),
- portable computers (Laptops, Notebooks, Chromebooks, Netbooks),
- portable storage (USB Flash Drives and Hard Disks, SD/MicroSD Cards, Compact Flash),
- media players (iPod, MP3/MP4 players),
- digital cameras, and
- physical storage media (CD, DVD, tape).

F. Internet and "Cloud" Storage includes (but is not limited to) the following:

- email;
- websites, web hosting providers;
- remote storage solutions (Google Drive, Dropbox, Box, OneDrive, iCloud);
- messaging services (SMS texts, Hangouts, iMessage); and
- cloud software and database products that store University Data externally.

CROSS REFERENCES

A. University Policies, including but not limited to

1. Records Retention Policy
2. SEFS Data Sharing Policy
3. University Purchasing Policy

B. Laws, including but limited to

1. The Ohio Breach Notification Act

2. Fostering Undergraduate Talent by Unlocking Resources for Education Act (FUTURE Act)

The policy and its accompanying documents are to be reviewed every year. If a policy has expired, the policy shall nonetheless remain in effect until it is updated and approved.