Policy: **Sensitive Data and Security**	Policy No: **T1.1**
Policy Developer(s): **Human Resources**	Original Date: December 20, 2019
Last Review Date: NA	Approval Date: December 20, 2019

Contact Person for Website: Director of IT Security

I. 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 computing resources or Data 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.

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.

II. 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.

III. SCOPE: This policy pertains to all employees of the University.

IV. 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 communications channels that have been analyzed and approved by Information Technology Services ("ITS"). Approved communication channels are listed in the Information Classification Matrix.

2. Sensitive Data may only be transmitted to or stored on ITS-approved third-party "cloud" storage providers. 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.

B. Department Responsibility: Department 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 High Value Sensitive Data. Specifically, 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. Secure Storage: Secure storage is available on University-provided network attached storage: (e.g., "O-drive"). Secure storage is also available on University Google Drive accounts with two-factor authentication ("2FA") in place. Accounts without 2FA are not considered Secure Storage. Sensitive Data is to be stored either on the network attached storage ("O-drive"), on Google Drive with 2FA, 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); 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.

D. 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.

E. 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 to be transported without encrypting the data using University-approved software and techniques.

F. 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.

G. 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.

H. 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.

I. 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.

V. DEFINITIONS: terms used within or relating to this policy.

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. 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).

E. 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.

VI. CROSS REFERENCES:

A. University Policies, including but not limited to
1. Information Technology Resources Policy
2. Corrective Action Policy

B. Laws, including but limited to
1. The Ohio Breach Notification Act

This policy will next be reviewed five years from the approval date/date of last review.

VII. ATTACHMENT: Information Classification Matrix

Information Classification Matrix

Appendix to Sensitive Data and Security Policy

John Carroll University has adopted this information classification matrix to support the management and protection of information, including electronic data.

- Department heads are responsible for assigning classifications to data & information assets according to the standard categories presented below.
- When reasonable, Data Classification information should be clearly indicated.
- All JCU personnel shall be guided by the Data Classification in their security-related handling of data & information.

For information regarding violations and enforcement, please refer to the Sensitive Data and Security Policy [link] section labeled "Breach of this Policy."

All data & information in use at JCU falls into one of the Data Classifications in the following table. These categories are presented in order of increasing sensitivity:

Data Classification	**Description**	**Examples**	**Storage / Processing Guidelines**
Public Data	Data that may be made available to the general public as appropriate.	Directory information[1], marketing materials, JCU website, data that does not contain personally identifiable information when all data stewards agree that it may be made available to the general public.	Data may be stored or processed using any JCU-provided mechanism, including email, removable media, and the official JCU website, as well as personal devices. The mechanism should be tailored to the desired level of public access and control.
Sensitive Data	Data that is not classified as High Value Sensitive Data, but which is classified by the unit Manager, JCU ITS, or institution as proprietary based on internal procedures or legal requirements.	Budgets, Salary information, JCU financial information, JCU planning information, routine Student Records, business or purchase agreements involving JCU, Financial Account/Loan, Transcript, or Disciplinary Records; Admission files.	Data may be stored or processed on JCU-provided PCs, tablets, or smartphones. Data may be viewed for job related purposes through approved apps (including the official Google G-suite apps) but not stored on personally owned devices without JCU ITS or department head approval.

[1] This is a technical term, defined in relation to FERPA. Information on the University's directory information is available on the Registrar's FERPA page.

Data Classification	**Description**	**Examples**	**Storage / Processing Guidelines**
High Value Sensitive Data	Data that contains legally protected personally identifiable information, data requiring higher levels of security under government privacy regulations, data designated as needing special protections by any voluntary industry standards or best practices that JCU chooses to follow.	Sensitive or large-scale aggregate data protected by FERPA. Other data requiring additional protection under the GLBA or PCI DSS, Social Security numbers, ACH (electronic payment) information, government identification numbers, protected health information, Additional Data may be designated as high value by JCU ITS or your area VP.	Data may not be stored or processed by third party entities except via contracted vendors approved for High Value Sensitive data or when required by law. Where storage or transmission is required by law, data must be encrypted prior to transmission. Data generally may be stored on JCU ITS provided file shares (O:\ , H:\ drives), and JCU ITS provided services (consistent with guidelines for use of said services) such as OnBase, Canvas, Google Suite with two-factor authentication, and ITS-provided encrypted removable media. Care must be taken to limit access to authorized individuals. Unencrypted Data may be emailed only with express permission of a Vice President. PCI DSS data may not be stored outside of a PCI-compliant network.

Commonly used Approved Cloud Vendors:

For Sensitive Data (but not High Value Sensitive Data):

- JCU.edu Google G-suite Applications
- Canvas
- Adirondack
- PeopleAdmin
- GivePulse

For Sensitive Data or High Value Sensitive Data:

- Slate
- OnBase
- GiveCampus

It is not appropriate to store Sensitive Data or High Value Sensitive Data by any mechanism not defined here and/or approved by ITS. If you have a question regarding any particular Data security issue, Data storage application, or Vendor, then please contact the Director of IT Security at x1614 or the JCU ITS Service Desk (formerly Helpdesk) at x3005.

FAQ/Helpful Links:

As this policy develops and ITS creates new resources to help employees better secure University Data, then this section will be updated with answers to frequently asked questions and informational resources that are helpful to Employees.