ROGER WILLIAMS UNIVERSITY
Data Storage Policy

Purpose

Roger Williams University is committed to protecting its data. Data Storage environments including Cloud Storage are useful in many ways. However, there are inherent risks relative to security, copyright, privacy, and data retention. Unlike data stored on premise, when documents are saved in Cloud Storage environments, the University must identify the appropriate administrative and access controls for the stored data. This policy notes best practices and applies to all University employees and affiliates that store the University Data classifications outlined in this policy.

Scope

This policy applies to all persons accessing University data on premise and/or using 3rd party services capable of storing or transmitting protected or sensitive electronic data that are owned or leased by Roger Williams University, all consultants or agents of the University and any parties who are contractually bound to handle data produced by and in accordance with University contractual agreements and obligations.

Compliance with Legal and Regulatory Requirements

The University has many federal laws that it must follow, these include the Family Educational Rights and Privacy Act of 1974 (FERPA), and RI General Laws 11-49.3 (Identify Theft Protection Act) and 5-37.3 (Confidentiality of Health Care Communications and Information Act).

Definitions

Data Classifications:

Protected Data - Under state law, Personally Identifiable Information means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name and the data elements are not encrypted or are in hard copy, paper format-

- Social security number
- Driver's license number, state identification card number, or tribal identification number
- Account number, credit, or debit card number, with or without any required security code, access code, password, or personal identification number, that would permit access to an individual's financial account
- Medical or health insurance information
- E-mail address with any required security code, access code, security Q&A, or password that would permit access to an individual's personal, medical, insurance, or financial account.

Sensitive Data – Data not meant for public distribution but not classified as Protected Data (i.e. internal policies, internal memos, Intranet information)

Public Data – Data meant for public distribution (i.e. external website, public relations materials, etc.)

Storage Classifications:

Cloud Storage – Cloud infrastructure provisioned for open use by the general public (i.e. Dropbox, Microsoft OneDrive - Personal, Google Docs - Personal, etc.)

University System on Premise– Private on premise Infrastructure provisioned for the exclusive use of Roger Williams University (i.e. Network Drives, Student Information System, Finance System, HR System etc.)

University System Cloud-based– Cloud Infrastructure provisioned for the exclusive use of Roger Williams University (i.e. RWU Microsoft O365, RWU Learning Management System, RWU Google etc.)

Local Storage – Personal or Roger Williams University devices not connected to a network controlled infrastructure (i.e. USB drives, laptops, desktop computers, etc.)

Policy Guidelines: The following guidelines note the permitted and prohibited storage systems for the data classifications outlined in this policy

Data Classification	Cloud Storage	University System on Premise	University System Cloud-based	Local Storage
Protected Data	Prohibited	Permitted	Permitted with Encryption	Prohibited
Sensitive	Prohibited	Permitted	Permitted with Encryption	Prohibited
Public	Permitted	Permitted	Permitted	Permitted

All Roger Williams University employees and affiliates looking to provision Cloud Storage services for work-related activities should consult with the Information Technology Department before doing so in order to ensure appropriate data security measures are taken.

Cross Policy References: Records Retention Policy [Retention Schedule], Written Information Security Program [Data Destruction Methods]