



COMMONWEALTH UNIVERSITY OF PENNSYLVANIA

Confidential Protected Data Storage Policy

Policy Number: PRP XXXX

Commonwealth University of Pennsylvania

Approved by University Senate, [Date of Approval]

Approved by the IT Subcommittee, [Date of Approval]

Responsible Office: University Office of Technology

1. Purpose

Although a large portion of Commonwealth University data is available to the public, some data have restrictions due to privacy protections mandated by federal, state, or local regulations and laws, ethical considerations, and proprietary worth. To comply with these mandates and protect the university community, Commonwealth University has the right and obligation to protect the confidentiality, integrity, and availability of data under its purview.

2. Scope

This policy applies to all faculty, staff, and administrators to protect employee data and ensure compliance with state and federal law.

3. Definitions, Roles and Responsibilities

3.1. Definitions

Confidential Protected Data – Data containing social security number, tax ID number, driver license number, passport number, financial account info, any type of username and/or password, and medical or health information.

3.2. Roles and Responsibilities

3.2.1. The Office of Information Technology oversees University approved data storage.



COMMONWEALTH UNIVERSITY OF PENNSYLVANIA

4. Policy

- 4.1.1 All Confidential Protected Data will only be stored in university owned systems approved by the IT department. For general use, Confidential Protected Data should only be stored if absolutely necessary. University-owned file servers, and approved cloud storage locations, are the only approved general use locations for Confidential Protected Data. The use of Artificial Intelligence is restricted to university owned and approved systems only.
- 4.1.2 Any modifications to the Confidential Protected Data Storage Policy must be granted via written approval from the IT Security department.

5. Procedures, Standards, and Guidelines

- 5.1 Students and employees have the option of saving data on multiple devices. University-owned servers and approved cloud storage locations are monitored by university personnel and provide users the most secure option for retaining Confidential Protected Data.

6 Compliance and Enforcement

- 6.1 Users are strongly encouraged to use University-owned and approved data storage options.

7. Additional Information

7.2 Supporting Documents

- 7.2.1 N/A

7.2.2 History

- 7.2.3 Established by the IT Subcommittee of the University Senate – 06/20/2024

7.2.4 Related Policies

- 7.2.5 N/A

7.2.6 Contacts for Additional Information and Reporting

[Office of Technology, Commonwealth University, Attn: Edward Keller,
ekeller@commonwealthu.edu, 570.389.3919]