Information Security Policy

Policy Number: PRP 2510

Commonwealth University of Pennsylvania

Approved by University Senate, [Date of Approval]

Revised 6/20/24 by the IT Subcommittee

Responsible Office: University Office of Technology

1. Purpose

The Information Security Policy acknowledges the need to protect the confidentiality, integrity, and availability of Commonwealth University data and the systems that store, process, or transmit it.

2. Scope

This policy applies to all faculty, staff, vendors, and other university affiliates who are authorized to access university data.

3. Definitions, Roles and Responsibilities

3.1. **Definitions**

3.1.1. **University Data:** University data is defined as any data that is owned or licensed by the university.

3.1.2. **Vendors:** Vendor is defined as any third party that has been contracted by the university to provide services related to storing, processing, or transmitting university data as part of those services.

3.2. **Roles and Responsibilities**

3.2.1. Faculty, staff, students, affiliates, auxiliaries, and vendors who have access to Commonwealth University data and its data storage and transmission systems must be aware of their obligation to protect university data. Systems must be protected from unauthorized access and use as well. Therefore, it is necessary to have appropriate local policies and procedures in place, as well as formal contracts with vendors that ensure the protection of all university data. Only vendors who have current contracts with

Commonwealth University may be utilized to store university data in consultation with the Information Technology Senate Subcommittee. The University's Office of Technology maintains a list of vendors with whom the university has formal data storage contracts.

4. Policy

Throughout its lifecycle, all university data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved by the University's Office of Technology and maintained by the Information Security Officer, given the level of sensitivity, value, and criticality that the data has to the University. Any university information system that stores, processes, or transmits university data shall also be secured in a manner that is considered reasonable and appropriate, as defined in documentation approved by the University's Office of Technology. All documentation for university data and information systems can be found in the Information Security Guidelines in Support of Information Security Policy. Individuals who are authorized to access university data shall adhere to the appropriate roles and responsibilities, as defined in documentation approved by the University's Office of Technology and maintained by the Information Security Officer.

5. Procedures, Standards, and Guidelines

5.1 Exceptions to this Policy must be approved by the Office of Technology, in consultation with the Executive Staff and the Information Technology Senate Subcommittee, and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

6 Compliance and Enforcement

6.1 Every University policy will undergo a regular review on a five-year cycle, with approximately 20% of the total policies inventory being reviewed each year.

6.2 All policy reviews will be conducted by the responsible Senate Committee to assure that the policy remains relevant and aligns with applicable federal and state laws and regulations, PASSHE Board of Governors policies, and other University policies, procedures, standards, or guidelines.

6.3 Violations of this policy may result in suspension or loss of the violator's use privileges, with respect to university data and university owned information systems. Additional administrative sanctions may apply up to and including termination of employment (for personnel) or cancellation of contracted services (for vendors). Criminal or civil prosecution under local, state, or federal laws may also apply.

7. Additional Information

7.1. **Supporting Documents**

7.2. N/A

7.3. **History**

7.4. Originally Issued General Administrative Committee, 2/23/2016

7.5. Effective Date – 4/20/2016 by University Forum

7.6. Revised - 6/20/24 by the IT Subcommittee

7.7. Next Review Date - 6/20/29

7.8. **Related Policies**

7.9. N/A

7.10. **Contacts for Additional Information and Reporting**

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