West Virginia University
Information Technology Services
16-002 Sensitive Data Protection Policy

Effective: August 13th, 2016
Updated or Revised: August 13th, 2016
Next Scheduled Review: (every three years from the date of approval)
Contact: Chief Information Security Officer, Information Technology Services

Purpose

West Virginia University (WVU) recognizes that it collects and maintains confidential information relating to its students, employees, and associates. WVU also acknowledges that it makes and receives payments using credit cards. The University is committed to maintaining the privacy and confidentiality of an individual's Social Security Number (SSN) and credit card information in processing payments and transactions. This policy establishes the responsibilities of all WVU organizational units regarding the use, storage and protection of Social Security Numbers and credit card information.

Scope

This policy applies to all faculty, staff, students, organizational units and third parties working for and with WVU that have access to, collect, or use an individual's Social Security Number or credit card information.

Definitions

- Credit Card information –the credit card number, the card holder’s name, address, SSN, and any other PII that is stored on the credit card.

- WVU third party – an individual or an entity that has an affiliation with WVU (Examples: retirees, consultants, presenters, camp attendees, or vendors.)

- PII – Personally Identifiable Information.

- PCI-DSS – Payment Card Industry Data Security Standards are the standards developed by the major credit card issuers (Visa, MasterCard, American Express, Discover and JCB) on merchant responsibilities for processing credit card transactions.

- WVUID – an internally-generated number used to identify individuals associated with WVU.

- Electronic communications – communications that have been designated as not being secure, (Examples: email, public web sites, social media).

- Data Stewards – WVU executive officers or their designees who have planning and policy-level responsibilities for data in their functional areas, and have management responsibilities for recognized information systems.

- Information Systems – Computer systems used for academic, administrative and research operations.

- WVU IT Enterprise – all WVU-owned information technology assets.

- WVU IT asset - A server, computer, laptop, tablet or mobile device used to enter or access information from a WVU information system.

- University operations – operations designated as essential to the administrative needs of employees, and operations designated as essential to the academic needs of students.

Policy

The WVUID will act as the primary identifier used by WVU for all persons in its information systems and it will be used as the primary identifier by WVU for all persons in electronic communications. WVU will discontinue the use of SSN as the primary identifier in all instances except where required by Federal or State law. Faculty, staff, students, organizational units and WVU third parties will not solicit SSNs except when required by federal or state law.

To ensure the security of credit card transactions, WVU will follow the governance documents and compliance requirements as published in the PCI-DSS. WVU will not accept credit card numbers by email and will not store credit card numbers in WVU information systems except where required by federal or state law.

All WVU units and staff are expected to follow published procedures in maintaining the security and privacy of SSNs and credit card information. Units and staff are expected to follow procedures maintained by Information Technology Services and WVU designated data stewards for the collection, dissemination, and security of SSNs and credit card information. These procedures are posted on Information Security Services' site http://it.wvu.edu/security/governance.

Units or individuals responsible for breaching the privacy of another person by improperly obtaining, using or disclosing an SSN or credit card information are subject to discipline as explained in the applicable WVU HR Employee Relations and Student Life policies.

The following apply to all WVU organizational units:

1. Employees and students shall comply with the provisions of this policy as well as related institutional policies and procedures.

2. Employees and students shall not disclose the SSN of another person unless it is necessary for the continuance of University operations.

3. Employees and students shall not send credit card information by email, shall not knowingly accept credit card numbers by email, and will not store credit card numbers on any WVU-owned computer.

4. Employees and students may not seek out or use the SSN or credit card of another person for personal advantage.

5. Employees responsible for maintaining records containing SSNs and / or credit card information shall observe all University published policies and procedures to protect the confidentiality of such records.

6. Employees shall report promptly to their supervisors and to Information Security Services (Infosec@mail.wvu.edu) any inappropriate disclosure of an SSN or a credit card.

7. If SSNs or credit card information are inappropriately disclosed and individuals have been put at risk of identity theft or other harm, Information Security Services and the General Counsel's Office shall be notified within 24 hours of the discovery.

8. Employees and units shall identify and report to Information Security Services any current practice using SSNs or credit cards that is not essential to continuing University operations.

9. Employees and units shall report to Information Security Services improper storage of SSNs or credit cards (Example: when stored on a PC's desktop or on removable media).

To maintain compliance with the requirements of this policy the IT Directors for all WVU organizational units will coordinate with Information Security Services to install ID Finder on University owned computers used by employees. Specifics on remediating ID Finder results are explained in the Sensitive Data Protection procedure found at - http://it.wvu.edu/security/governance.

Enforcement

WVU's Chief Information Officer and Chief Information Security Officer will coordinate with identified data stewards on the implementation of this policy. Information Security Services will conduct regular scans of the WVU IT Enterprise to identify unsecured SSNs or the existence of credit card information.

Violation or non-compliance of this policy will be addressed in accordance with established WVU disciplinary policies and procedures, as issued and enforced by the appropriate authorities. Failure to comply with this or other related standards may result in disciplinary action up to and including termination of employment or studies.

Relevant Documents

Links

- Avoid Identity Theft: Protect Social Security Numbers; Social Security Administration Philadelphia Region, http://www.ssa.gov/phila/ProtectingSSNs.htm
- Defend Your Data http://it.wvu.edu.security/governance

Policies

- ITS Information Security: http://it.wvu.edu/security/governance
- WVU Human Resources: http://www.hr.wvu.edu/policies
- WVU ResNet Acceptable Use: http://www.resnet.wvu.edu/
- WVU Student Conduct Code: http://campuslife.wvu.edu/r/download/220286