West Virginia State University

Customer Information Security Guidelines

These information security guidelines describe West Virginia State University's ongoing efforts to secure information related to students and others who provide certain sensitive information to the University. The University is required by law, specifically the federal Gramm Leach Bliley Act ("GLBA") and its accompanying Safeguards rule, the Federal Trade Commission's "Red Flags" rule, the Family Educational Rights and Privacy Act ("FERPA"), the Health Insurance Portability and Accountability Act ("HIPAA"), and the West Virginia Consumer Credit and Protection Act to:

- maintain, monitor, and test this plan;
- designate a security officer to coordinate the safeguarding of customer information;
- identify and assess risks to customer information;
- evaluate, improve, and implement safeguards to protect customer information;
- identify and respond to red flags concerning potential identity theft; and
- notify individuals of data breaches under circumstances established by law.

These guidelines also make good business sense, as they help assure the University's "customers" that the university is taking adequate steps to protect their information and to minimize loss in the event of a security breach. These guidelines also serve to deter and respond to an increasingly common crime nationwide identity theft.

Scope

These security guidelines protect customer information University-wide in any office, college, school, division, department, or responsibility center that is significantly engaged in financial activities. When in doubt as to whether a school, department, responsibility center, or office is 'significantly engaged' in financial activities, the unit should err on the side of applicability.

"Customer information" means any paper or electronic record containing non-public personal information about an individual that the University, or its affiliates, handle and maintain. Customer information includes any personally identifiable information provided by students or others in order to obtain a financial product or service from the University such as loan applications, credit card numbers, account histories, and related consumer information. It also includes data found in accounts where the University provides services and defers payment (essentially extending credit) such as in a deferred tuition payment plan or ticket payment plan.

University Unit Responsibilities

A. Securing Information

Units must immediately and continually assess the safeguards they have in place to protect not only customer information, but all confidential University data. Heads of units should appoint a trusted and knowledgeable employee to oversee their individual safeguarding programs. Specific safeguarding practices that units must assess, and if necessary, implement, include:

1. Maintaining physical security by locking rooms and file cabinets where customer and sensitive information is stored. Ensuring windows are locked and using safes when practicable for especially sensitive data such as credit card information, checks, and currency;
2. Maintaining adequate key control and limiting access to sensitive areas to those individuals with appropriate clearance who require access to those areas as a result of their job;
3. Using strong passwords and either frequently changing passwords or adopting multi-factor authentication when accessing automated systems that process sensitive information and requiring identification before processing in-person transactions;
4. Using firewalls and encrypting information when feasible and using authentication and passwords when creating new accounts;
5. Minimizing the storage of customer information on mobile devices, and, in situations where it is unavoidable, ensuring that mobile devices are adequately protected, e.g., physical security, use of encryption; icloud storage;
6. Referring calls and mail requesting customer information to those individuals who have been trained in safeguarding information;
7. Shredding and erasing customer information when no longer needed in accordance with unit and University policy and the law;
8. Encouraging employees to report suspicious activity to supervisors and law enforcement authorities;
9. Ensuring that agreements with third-party contractors contain safeguarding provisions and monitoring those agreements to oversee compliance;
10. Discouraging the use of social security numbers and using social security numbers only in accordance with university Policy on social security numbers;
11. Notification of new hires / position changes
12. Marketing/Media
13. Control media in transport
14. Prohibit portable devices that have no owner
15. Alternate work sites, e.g., work from home

B. Training

Units should ensure that all new and existing employees who are involved in activities covered under these guidelines receive safeguarding and red flags training.

1. A written agreement containing the employee's signature, and attesting to the fact that he or she received training, is aware of University and Unit information policies and guidelines, and is aware of the importance the University places on safeguarding information, is suggested. New users to Banner must receive the Introduction to Banner training, and user training increases for additional data access authority.
2. Training should, at a minimum, encompass the areas covered by this document.

C. Monitoring and Detection

Units must continually assess what types of information are received, stored and distributed and assess the vulnerabilities of their systems. Assistance is available in assessing the efficacy of their existing safeguards and in proposing improvements. The University Police Department ("UPD"), are available to discuss physical security issues and can provide a security analysis for your unit. Units should also identify particular red flags that may indicate that identify theft is afoot. These include:

1. Receipt of alerts from consumer reporting agencies such as a credit freeze or notice that certain accounts may be susceptible to fraud;
2. Receipt of suspicious documents containing forged signatures or apparent alterations or an identification card with a photograph that does not resemble the owner of the account;
3. Receipt of suspicious personal identifying information such as a Banner A-number that does not match the student, or information that matches somebody else's education records, or submitting a lack of required personal information after further request;
4. Unusual use of or other suspicious activity related to a customer or prospective customer account, such as a suspicious application, suspicious change of direct deposit information, a recurring payment made to a student despite the student's not registering for courses, or refunds at unusual times, a pattern of dropping courses, etc.;
5. Receipt of notices from victims, law enforcement agencies, or others such as University administrators that an individual's information has been breached.

D. Managing Systems Failures and Handling Red Flags

1. The University acknowledges that no system is flawless. Nevertheless, immediate steps should be taken to correct any security breach. Units must immediately report significant failures of their safeguarding system to the UPD, if the problem involves computer security, and to the Designated Information Security Officer. Affected customers may also need to be notified by University officials after the unit consults with the Designated Information Security Officer, UPD, and the Office of General Counsel about the necessity of notification and the proper notification procedures. Examples of significant failures would include a successful hacking effort that results in the loss of unencrypted personal data as defined by West Virginia state law, a burglary, or impersonations leading to the defrauding of customers.
2. Steps that units may take to respond to red flags it has detected or prevent a potential loss of data include: conducting an investigation, removing data from a network, monitoring accounts for evidence of identity theft, closing or re-designating accounts, refusing to open new accounts, contacting the customer after consultation with the above University officials, changing passwords, and further enhancing physical or computer security after consultation with UPD.

E. No Third-Party Rights

While these guidelines are intended to promote the security of information, they do not create any consumer, customer, or other third-party rights or remedies, or establish or increase any standards of care that would otherwise not be applicable.

University Policies and Guidelines That Protect Customer Information

The following policies and guidelines supplement and help to create a comprehensive information security plan. Referral and adherence to these documents is imperative to overall protection of customer information. The following documents are incorporated by reference into the plan.

1. University Board of Governors Policy 52 governs "Information Technology (IT) Security Policy." This policy establishes guidelines and responsibilities for WVSU employees regarding information security and the protection of university information resources. It can be found at: http://wvstateu.edu/wvsu/media/About/p52.pdf
2. University Board of Governors Policy 53 governs the "Responsible Use of University Computing Resources." It can be found at: http://wvstateu.edu/wvsu/media/About/p53.pdf
3. University Board of Governors Policy 63 governs the university's "Record Retention Policy," and provides guidelines for the retention of business records at WVSU based on a schedule of documents available on the university's website. The policy can be found at: https://www.wvstateu.edu/wvsu/media/President/BOG-Policy-63-Record-Retention_Final_with_link.pdf, and the schedule at: http://www.wvstateu.edu/wvsu/media/President/SJDOCS-7925278-v1-General_Retention_Schedule.pdf
4. The University's Registrar maintains the university's Policy on the Family Educational Rights and Privacy Act ("FERPA") and how it applies to students' accounts as part of the Student Handbook, which can be found at: https://www.wvstateu.edu/getattachment/Current-Students/Student-Handbook/WVSU-Student-Handbook-Student-Code-of-Conduct-for-WEB.pdf
   FERPA Training is also conducted upon departmental request and each term through the Registrar's Office
5. University policy delineates the requirements and implementation of the Health Insurance Portability and Accountability Act ("HIPAA"). This policy bolsters patient privacy in regard to health care and payment for health care.
6. The University's Employee Handbook emphasizes the protection and confidentiality of university proprietary information. The Handbook is located at: https://www.wvstateu.edu/getattachment/About/Administration/Human-Resources/Employee-Handbook-2013-14.pdf
7. The University's Faculty (and Part-time Faculty Handbook) is located at: https://www.wvstateu.edu/getattachment/Faculty-Staff/Faculty-Resources/2018-19-WVSU-Faculty-Handbook.pdf

Designated Information Security Officer

The Designated Information Security Officer is appointed by the President and is responsible for coordinating the safeguarding of customer information throughout the University. Per the requirements of the Red Flags Rule, the Designated Information Security Officer shall report the adherence to these guidelines, their effectiveness, serious incidents falling under it, related issues with third-part service providers, and any suggested material changes annually.