

Customer Information Security Program Procedures and Protocols

(A) Risk Identification and Assessment

- (1) The Information Security Program Coordinator (ISPC) shall work with all relevant areas of the University to identify potential and actual risks to security and privacy of customer information, as defined in university rule 3359-11-10.4.
 - (a) Each College, School, and department head, or his or her designee, will conduct a data security review annually or as deemed to be necessary, with guidance from the ISPC and the Information Technology Security Officer (ITSO).
 - (b) Vice Presidents, or their designees, will be asked annually to identify any employees in their respective areas that work with customer information. Vice presidents, or their designees, will notify the ISPC when new employees who work with customer information are hired.
 - (c) The ISPC shall conduct a review of procedures, incidents and responses annually or as deemed to be necessary, and may publish all relevant materials except in those cases where publication may lead to breaches of security or privacy of customer information or any other information protected by federal, state or local law. Publication of these materials is for the purpose of educating the University community on information security and privacy issues.
 - (d) The ISPC will consult with the ITSO in order to assess university procedures and responses as compared with those generally practiced in higher education.
- (2) In order to protect the security and integrity of the University network and its data, Network and Communication Services will develop and maintain a complete registry of all computers attached to the University network. This registry may include, where deemed to be relevant, IP addresses or subnet, MAC address, physical location, operating system, intended use (server, personal computer, lab machine, dorm machine, etc.), the person, persons or department primarily responsible for the machine, and whether the machine has or has special access to any customer information.
- (3) The Director of Hardware Operations and Operating Systems is responsible for assuring that patches for university operating systems or software environments are reasonably up to date, and will keep records of patching activity. The Director of Hardware Operations and Operating Systems will review procedures for patches to operating systems and

software as it deems necessary, and keep current on potential threats to the network and its data. Risk assessments will be updated annually or as deemed to be necessary by the Network and Communication Services Network Engineer.

- (4) The ITSO has primary responsibility for identifying internal and external risks to customer information on university hardware. The ITSO, working in conjunction with the relevant University offices, will conduct regular risk assessments, including but not limited to the categories listed by university rule 3359-11-10.4 and the Gramm-Leach-Bliley Safeguards Rule.
 - (5) The Enterprise Applications Services Security Administrator, working in cooperation with relevant University departments, will develop and maintain data listings of those persons or offices responsible for each covered data field in relevant software systems (financial, student administration, development, etc.) The Enterprise Applications Services Security Administrator and the relevant departments will conduct ongoing audits of activity, and will report any significant questionable activities to the ISPC, ITSO or others as deemed to be necessary.
 - (6) The ISPC, together with the Director of Student Financials, will work with the relevant offices (Student Financials, Financial Aid, Human Resources, and the Registrar among others) to develop and maintain a registry of those members of the University community who have access to customer information. The ISPC, in cooperation with the Director of Student Financials and Human Resources, will work to keep this registry rigorously up to date.
 - (7) The ITSO will assess the physical security of all servers and terminals that contain or have access to customer information. The ISPC, in conjunction with the ITSO, will work with other relevant areas of the University to develop guidelines for the physical security of any covered servers in locations outside the central server area. The ISPC, in conjunction with the ITSO, will conduct a survey of other physical security risks, including the storage of covered paper records in non-secure environments, and other procedures that may expose the University to risks annually or as otherwise deemed necessary.
 - (8) The ISPC will periodically review the University's disaster recovery program and data-retention policies and present a report to the Vice Presidents.
- (B) Physical record security safeguards.

- (1) Departments that receive credit card information and forward it to the Cashier's Office for processing write the relevant credit card information on a paper credit card transaction form, which is transmitted to the Cashier's Office by a member of The University of Akron Police Department (UAPD). Under no circumstances does such an office retain a copy of the credit card information.
 - (2) Offices that maintain customer information take the following security precautions:
 - (a) Cash receipts and cash receipt processing are conducted in glass enclosed rooms;
 - (b) Current customer information is secured in locked filing cabinets in offices that are secured at night;
 - (c) Retention files containing customer information are maintained in a secured, non-public area with limited access;
 - (d) Customer information that exceeds the University's retention capabilities is destroyed by shredding;
 - (e) All staff are encouraged and reminded to sign off their computers when leaving the immediate area or to use screen savers that require password deactivation;
 - (f) Student employees working in affected offices are only provided limited access sufficient to perform their job responsibilities;
 - (g) All computers are turned to face University employees rather than customers to avoid inadvertent or unauthorized screen viewing;
 - (h) Non-students who pay student invoices receive modified receipts that do not display student identification or social security numbers; and
 - (i) The Cashier's, Accounts Receivable, and Financial Offices are non-student contact offices and members of the public must be invited into these offices. Members of the public are only invited to the conference office area or lobby in these offices.
- (C) Network security safeguards.
- (1) Vulnerability scans.
 - (a) Network and Communication Services Network Engineer

- (i) Scans servers accessible from the public Internet for vulnerabilities on a quarterly basis and as deemed to be necessary. The contact person responsible for any server that is determined to be exploitable is notified of and instructed on how to correct the vulnerability.
 - (ii) Scans all other machines on the network (lab, desktop, dorm, etc.) for vulnerabilities twice per year or as deemed to be necessary. The contact person responsible for any machine that is determined to be exploitable is notified of and instructed on how to correct the vulnerability.
- (2) Firewall security practices.
 - (a) The Network and Communication Services Network Engineer
 - (i) Maintains a record of services that make services available to the public Internet and adjusts the firewall rules accordingly;
 - (ii) Will develop and implement a system for automatically monitoring firewall logs on a routine basis. Until an automated firewall log-monitoring system is in place, the Network and Communication Services Network Engineer regularly monitors the firewall logs.
 - (b) All incoming traffic to machines that make services available to the public Internet will be blocked, except for that which is explicitly permitted. All traffic associated with known or suspected vulnerabilities, exploits, or backdoors is blocked.
- (3) Security related news.
 - (a) The Network and Communication Services Network Engineer frequently reviews security related news sources and maintains a familiarity with new exploits and vulnerabilities, as well as current events and trends in the security field. To accomplish this, the Network and Communication Services Network Engineer reviews information provided through the SANS Institute, including but not limited to that included in SANS NewsBites, SANS Critical Vulnerability Analysis and Security Alert Consensus.
- (4) Security awareness practices.

- (a) The Network and Communication Services Network Engineer maintains a security mailing list, which is be used to inform information technology staff across the campus of security issues and to provide them with additional information resources.
- (5) Miscellaneous network security safeguards.
 - (a) The Network and Communication Services Network Engineer
 - (i) Monitors network traffic that is deemed to be suspicious and examines it for exploit signatures, protocol header anomalies and other signs of malevolent activity;
 - (ii) Installs and maintains hardware as necessary to provide heightened security for customer information;
 - (iii) Maintains the university's intrusion detection hardware as necessary to provide heightened security for customer information; and
 - (iv) Researches, develops and deploys new network security applications as the need or opportunity arises.
- (D) Software security safeguards.
 - (1) Access control.
 - (a) University employees or students who require access to customer information to perform their duties, must submit a form request to the Enterprise Applications Services Security Administrator.
 - (i) Form requests for user access to customer information must be approved by the employee or student's supervisor and the data owner (record custodian) before the employee or student requesting access to customer information are granted access.
 - (b) The Enterprise Applications Services Security Administrator audits PeopleSoft security, with the assistance of the appropriate data owners, by reviewing a list of users with access to customer information and their security level annually or as deemed to be necessary. The Enterprise Applications Services Security Administrator adjusts users' security levels as necessary based upon the results of this audit.
 - (2) Physical security safeguards related to software security.

- (a) Hardcopies of security documents are kept in a secure area in the computer center.
 - (b) Old security and access request forms and reports are shredded in the computer center by the Inventory Control Officer.
 - (3) Encryption safeguards.
 - (a) Web payments are encrypted in transit.
 - (b) Credit card numbers stored in PeopleSoft are be encrypted.
- (E) Miscellaneous security safeguards.
 - (1) If appropriate, relevant offices of the University, in cooperation with Human Resources, will determine whether more extensive background or reference checks or other forms of confirmation are prudent in the hiring process for certain new employees, and implement such procedures if merited.
 - (2) Each department that handles or maintains customer information implements those precautions it deems to be necessary and appropriate to protect customer information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.
- (F) Employee Management and Training.
 - (1) Human Resources will check the references of new employees working in areas that regularly work with customer information.
 - (2) The Manager of Software Training Services, in coordination with Human Resources and any appropriate individuals in affected departments, will train individuals who have access to customer information on the importance of the confidentiality of customer information, educational records, and other types of protected data and information. Individuals will also receive training in the proper use of computer information, passwords, procedures and protocols implemented to prevent individuals from providing confidential information to unauthorized individuals.
- (G) Selection of Appropriate Service Providers.
 - (1) Service providers that will maintain or regularly access customer information shall be evaluated by the ITSO or his/her designee, in

conjunction with appropriate individuals from the university, prior to selection to determine their ability to safeguard customer information.

- (2) Contracts with service providers that will maintain or regularly access customer information may include the following provisions:
 - (a) An explicit acknowledgment that the contract allows the service provider access to customer information;
 - (b) A specific definition or description of the customer information being provided to the service provider;
 - (c) A stipulation that the service provider will hold customer information in strict confidence and will only access the information for the explicit business purpose of the contract;
 - (d) An assurance that the service provider will protect the customer information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information;
 - (e) A provision providing for the return or destruction of all customer information the service provider receives during the course of the contract upon completion or termination of the contract;
 - (f) An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitle The University of Akron to terminate the contract without penalty;
 - (g) An agreement that the service provider will indemnify and hold the University harmless from any damages resulting from the contract's confidentiality conditions; and
 - (i) A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.