IT04 Policy for Securing Customer Bank Account Information

Effective 1 July 2009 **Last Revised** June 2016

Who Should Read This Policy

University employees and agents entrusted with access to, and therefore, responsibility for, safeguarding customer bank account information.

Background & Purpose

Bank information is defined as personal identifying information (PII) by the State of Oregon and is subject to Oregon's Identity Theft Protection Act. Bank information is classified 'Sensitive' in the university Data Classification policy and is subject to the minimum security procedures for devices with sensitive data.

It is important that university employees and agents of the university take appropriate measures to safeguard sensitive customer information, including bank account numbers.

NACHA, the Electronic Payments Association, has adopted security standards for Automated Clearinghouse (ACH) transactions. Failure to comply with NACHA rules may result in financial loss, fines, suspension of ACH processing privileges, and/or damage to the reputation of the university.

Customer bank information is collected and processed by the university in several ways, for example:

1. Bank information is collected from employees, students and vendors using paper forms and the university's secure web portal DuckWeb.
2. Customer bank information is securely stored in the university's Banner enterprise system.
3. The Business Affairs Office (BAO) originates direct deposit files for employee payroll and reimbursement, student refunds and vendor payments which are processed by the university's bank on the national ACH network.
4. BAO employees process returned check transactions using third party banking systems.
5. The university's online student billing and payment vendor collects student bank information when they elect to pay tuition and fees by electronic check (echeck). This vendor originates ACH files and ACH return files on the university's behalf. This policy provides guidelines for safeguarding customer bank account information.

The purpose of this policy is to set out specific standards for the treatment of customer bank information by university employees.

Policy

The AVP Business Affairs/Controller is the steward of customer bank information and is responsible for,

a) Ensuring university compliance with state law and NACHA rules regarding the security of customer bank information.

b) Maintaining and enforcing related policies and procedures.

c) Authorizing all bank deposit activities at the University of Oregon.

d) Authorizing all university employees or agents who will collect or process customer bank information.

e) Conducting an annual risk assessment of practices for handling of customer bank information.

Customer bank account information must be treated in accordance with the following standards:

a) Publish and disseminate written unit operating procedures for handling and protection of customer bank information.
b) Do not store electronic files containing customer bank account information on the university network without a business reason and without meeting the Minimum Security Procedures for Devices with Sensitive Information (see university Data Classification policy below).
c) Do not send or receive bank account information using email. Use secure electronic file transfer methods such as secure file transfer protocol (SFTP) or a virtual private network (VPN).
d) Delete direct deposit/ACH files from the university network immediately after they have been securely transferred for processing.
e) Strictly limit access to paper and electronic records containing bank account information based on job function and business need. Where practical, limit access to full time professional staff. Access to customer bank account information must be authorized in writing by the employee's manager (for example using a system access form or position description).
f) Physically secure paper records containing bank account/ACH information in locked cabinets or offices with adequate key control. Mark these records as 'Confidential'. Strictly control the distribution of these records.
g) Inventory paper records and electronic media containing bank account information every six months to identify loss or theft of items.
h) Securely dispose of paper and electronic records containing bank account information when they are no longer required for business, legal or regulatory purposes and in

accordance with the university records retention policy. Paper records should be placed in confidential recycling when past their retention period. Electronic media should be destroyed beyond recovery.

i) If you access host systems containing bank account information using a wireless network connection, ensure that the network uses strong encryption for authentication and transmission.

j) Units must perform background checks on potential employees who will have access to customer bank account information.

k) Train new employees who will have access to customer bank account information so that they are aware of this policy and their responsibility for safeguarding this sensitive information.

l) In the event of a data breach involving customer bank information the university will execute its Data Security Incident Response Plan.

Authority

The university Vice President for Finance and Administration has authority for administering this policy and has delegated its implementation to the AVP Business Affairs/Controller.

References

- Oregon Identity Theft Protection Act
  http://www.cbs.state.or.us/dfcs/id_theft.html
- UO Data Classification Policy
  https://policies.uoregon.edu/vol-4-finance-administration-infrastructure/ch-6-information-technology/data-classification
- NACHA
  http://www.nacha.org/
- UO Records Retention Schedule
  http://libweb.uoregon.edu/records/schedule/sections.html
- Criminal Background Checks
  http://policies.uoregon.edu/criminal-background-checks-0
- Data Security Incident Response
  http://policies.uoregon.edu/vol-4-finance-administration-infrastructure/ch-6-information-technology/data-security-incident

Contact

Business Affairs Office 346-6249