

IT03 BAO Information Systems and Security Policy

Effective 1 Apr 2005

Last Revised 10 February 2009

Who Should Read This Policy

This policy applies to Business Affairs employees.

Background & Purpose

Business Affairs employees are granted access to sensitive student, employee and vendor information that is protected by federal, state and institutional regulations. Examples of sensitive information include; UO ID, SSN, bank account numbers, credit card numbers and other student information not explicitly defined as 'directory information'.

This policy was written to clarify employee responsibility for ensuring:

- The privacy and security of student, employee and vendor information.
- The integrity and security of BAO systems (desktops, network servers and printers), and
- The integrity of critical business information.

Policy

1. Student Records

- Employees will become familiar with the University of Oregon Student Records Policy, and in particular, the definition of 'directory information'.
<http://registrar.uoregon.edu/common/recrdprivpol/studentferpa.htm>

2. BAO Systems

- Employees will become familiar with the university's 'Acceptable Use of Computing Resources' guideline and operate university and BAO systems accordingly.
<http://cc.uoregon.edu/policy/index.html>

3. Passwords

- Employees will change user account passwords for desktop operating systems and servers every six months.
- Passwords shall contain a combination of at least eight numbers and letters
- Employees will not share their individual passwords (BANNER, Rhinos, Windows, Groupwise, VMS, Darkwing etc) or log others into systems using their individual passwords.

4. Storage, Transfer, and Disposal of Sensitive Customer Information

- Employees will not reveal the content of any record or report to anyone, except in the conduct of their work assignments.
- Employees will adopt practices that protect the confidentiality of paper records.

- Employees will use a secure method when disposing of sensitive paper records (shred or confidential recycle).
- Employees will work with the BAO Systems Administrator to ensure that any sensitive customer information placed on servers with shared access ('K drive' or 'common') resides in directories with access that is limited to employees with a legitimate business need.
- Employees will promptly delete sensitive customer information residing on desktop computers and servers once it has outlived its business purpose.
- Employees will use secure methods of electronic file transfer to share large quantities of sensitive customer information with colleagues or any quantity of highly sensitive information such as bank account and credit card numbers. Secure methods include secure file transfer, virtual private networks, PGP encrypted email or email attachments, and password protected email attachments.
- Employees will turn unwanted computer diskettes, magnetic tapes, hard drives etc. over to the BAO Systems Administrator who will securely dispose of all electronic media that may contain customer information.

5. Unattended Workstations

- Employees will use a password-protected screensaver to secure their workstation while away from their work area. When appropriate, employees will also lock their console or log off.
- Screensaver wait time shall be set to the minimum number of minutes that is practical, never exceeding 10 minutes.
- Employees will shut down and power off workstations at the end of each workday.

6. Workstation Maintenance

- The BAO Systems Administrator will ensure all workstations and server operating systems are updated, automate virus definition updates, and ensure that all workstations have appropriate operating system security settings and a spyware removal application installed.
- Employees will assist the BAO Systems Administrator in keeping their workstation secure, (change passwords as required, install operating system updates, update anti-virus definitions, perform daily virus scans, browse responsibly, report suspicious email and attachments, install approved personal software only).
- Employees will promptly report all system performance issues to the BAO Systems Administrator.

7. Desktop Software

- The BAO Systems Administrator will install all software.
- Employee requests for software will be evaluated based on; business need, system security, system performance, and licensing.
- Employee requests to install games will be denied.

8. Storage, Archiving and Recovery of Business Critical Information

- Employees will store all business critical information on file servers (H or K drive), where it can be backed up, rather than on desktop drives (C drive).
- The BAO Systems Administrator will back up server data on a nightly, weekly and monthly basis. Monthly media will be securely stored offsite.

9. Employee Termination/Resignation

- BAO Managers will work with the BAO Office Manager to complete the employee checklist when an employee terminates.
- The BAO Systems Administrator shall remove an employee's system privileges (desktop, file server, email server, etc.) whenever necessary, and always on their last day of work.
- The BAO Systems Administrator will make the former employee's email and data files available to the employee's supervisor/successor or delete them.

10. After Hours Building Access

- Employees that provide after hours building access to any person(s), shall take responsibility for the actions of said person(s).

Authority

The Director of Business Affairs has authority for administering this policy.

References

- The Gramm-Leach Bliley Act
<http://www.ftc.gov/privacy/glbact/>
- The Family Educational Rights and Privacy Act
<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- University of Oregon Student Records Policy
<http://registrar.uoregon.edu/common/recrdprivpol/studentferpa.htm>
- Acceptable Use of Computing Resources
<http://cc.uoregon.edu/policy/index.html>
- Oregon's Public Record Law ORS 192.800 - 192.810
<http://landru.leg.state.or.us/ors/192.html>
- Faculty Records Rule OAR 571-030-0010, and 0015
http://arcweb.sos.state.or.us/rules/OARS_500/OAR_571/571_030.html

Contacts

BAO Systems Administrator 6-2030

BAO Office Manager 6-4340

IT03 BAO Information Systems and Security Policy

Employee Certification

I have read, understand, and will comply with, the Business Affairs Information Systems and Security Policy.

_____ (printed name)

_____ (signature)

_____ (date)