IT03 BA Information Systems and Security Policy

Effective 1 Apr 2005 **Last Revised** Feb 2017

Who Should Read This Policy

This policy applies to Business Affairs employees.

Background & Purpose

Business Affairs (BA) employees have access to sensitive student, employee and financial data that is protected by federal, state and institutional regulations. Sensitive data includes; SSN, customer bank account number, credit card number, driver's license number, home address and telephone number, payroll benefits, other information exempt from disclosure under Oregon's public records law, billing charges and payments, and other student educational and health records.

All Business Affairs employees share responsibility for safeguarding sensitive data and maintaining the integrity of university systems (PC's laptops, servers, copiers and printers).

Policy

1. Student Records

- Employees will become familiar with the University of Oregon Student Records Policy, and in particular, the definition of 'directory information'.

2. BA Systems

- Employees will become familiar with the university's Acceptable Use of Computing Resources policy and operate university and BA systems accordingly.

3. Passwords

- Employees will change user account passwords for university systems when required.
- Employees will use strong passwords where practical.
- Employees will not share their individual passwords or log into systems for others.

4. Protecting Sensitive Data

- Employees will not reveal the content of any record or report, except with other university officials in the conduct of their work assignments.
- Employees will adopt practices that protect the confidentiality of paper records and dispose of records containing sensitive information at the end of the retention period using confidential recycle.

- Employees will avoid storing sensitive data on desktop computer hard drives, university laptop computers, and portable media (USB drives, CD, smart phones), which are prone to malfunction, theft and loss.
- Employees will not use Banner or process sensitive data on personal home computers. A university issued and maintained computer with encrypted hard drive should be requested if work from home is authorized. Use of DuckWeb and Outlook Web Access on personal home computers and smart phones is permitted.
- Employees will work with BA System Administrators to ensure sensitive information on file shares (K drive) resides in directories with access limited to employees with a legitimate business need.
- Employees will delete electronic files containing sensitive information from file and mail servers at the end of its retention period.
- Employees will use secure methods of electronic file transfer to share sensitive information including Secure File Transfer Protocol (SFTP), Virtual Private Networks (VPN), encrypted email or password protected email attachments.
- Employees will return unwanted computer media; diskettes, magnetic tapes, hard drives, USB drives, etc. to BA System Administrators who will securely dispose of all electronic media that may contain customer information.
- Employees will refer outside requests for public records to the Office of Public Records.

5. Unattended Workstations

- Employees will use a password-protected screensaver to secure their workstation while away from their work area. Employees will also lock their console.
- Screensaver wait time shall be set to 10 minutes or less.
- Employees will shut down and power off workstations at the end of each workday.

6. Workstation Maintenance

- BA System Administrators will ensure all computer operating systems are properly configured; patched and updated, anti-virus programs installed, configured and operating.
- Employees will assist BAO System Administrators in keeping their workstations secure by allowing operating system and antivirus updates to occur.
- Employees will browse responsibly and report system error messages and performance issues immediately.
- Employees will inspect all link addresses in email before clicking, and verify the source of any attachment before opening. Phishing related to university systems should be forwarded to phishing@uoregon.edu.

7. Desktop Software

- Employees will not be granted administrative rights on university computers.
- BA System Administrators will procure and install all software.
- Software will only be installed if:
    - There is legitimate business need,

- The software will not impair system security or performance, and
- Business Affairs has appropriate licensing.

8. File Storage

- Employees will store business critical information on file shares (H or K drives), where it can be backed up, rather than on desktop drives (C drive).
- Information Systems will back up server data on a nightly, weekly and monthly basis. Information Systems also stores monthly backups offsite.

9. Employee Termination/Resignation

- Managers will work with the BA Office Manager to complete the employee checklist when an employee terminates.
- Systems Administrators shall remove an employee's system privileges (MS Active Directory, file server, email server, etc.) on the last day of work.
- The BA System Administrators will make the former employee's email and data files available to the employee's supervisor.

10. Visitors

- Employees who provide after hours building access to any person(s), shall take responsibility for the actions of said person(s).
- Employees will greet visitors to Business Affairs and offer assistance.

Authority

The Associate Vice President (AVP) of Business Affairs has authority for administering this policy.

References

- University of Oregon Student Records Policy
  http://policies.uoregon.edu/vol-3-administration-student-affairs/ch-5-student-records/student-records

- Acceptable Use of Computing Resources
  http://it.uoregon.edu/acceptable-use-policy

- Oregon's Public Record Exempt from Disclosure ORS 192.501-505
  http://www.oregonlaws.org/ors/192.501

- Faculty Records Policy
  https://policies.uoregon.edu/faculty-records-policy

Contacts

BA Systems Administrator 6-2030, 6-1102
BA Office Manager 6-4340

IT03 BA 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)