Policy Title: **Information Security**

Policy Number: PS 445

Purpose of Policy: Bellevue University (the "University") and our employees have the responsibility for securing the information contained within our Electronic Systems and Equipment (as defined in PS 402) to a reasonable and economically feasible degree against fraudulent activities and unauthorized access to private information stored within these systems. This responsibility includes maintaining strong user passwords, careful use and management of personal information, and the appropriate disposal of confidential information once the business need for the information has been completed.

Applies to: All Users (as defined in PS 402)

Policy Statement:

1. What follows constitutes a policy of information security for all Users of the University's Electronic Systems and Equipment. The information resources list addressed in this document are intended to cover all aspects of information security for all Electronic Systems and Equipment used at the University. The lack of a specific mention for a particular system does not exclude that system from the intent of the security practices defined in this document. Users who violate this policy will have their access privileges to the Electronic Systems and Equipment removed pending an investigation of the alleged violation(s). Violations of this policy may result in immediate corrective action, which can include termination of employment, permanent suspension from the University, or both.

2. By using any Electronic Systems and Equipment owned or provided by the University, the User is acknowledging the acceptance of this policy and the specific restrictions and warnings contained herein. Furthermore, the User understands that all information stored on any device owned, leased, or contracted for use by the University is confidential property of the University and should be treated as such. Access to all information residing on any of the University's Electronic Systems and Equipment is stored for the sole purpose of conducting the academic or business purposes of the University and is available to authorized Users as needed. The use of any business system information which does not further the academic or business purposes of the University is strictly prohibited.

3. Current University Electronic Systems and Equipment include Campus Solutions, BRUIN Portal, Blackboard, Salesforce, O365, ADP, Business Intelligence systems and Oracle Financials. This policy includes any Electronic Systems and Equipment currently in use or implemented in the future, and also includes all information or data located on any of the protected network servers or any other University owned location that is dedicated to storing information required to effectively meet the academic or business needs of the University.

4. System Configuration: No User will install any unapproved software or cause any unapproved software to be installed onto any Electronic Systems and Equipment. No User will tamper with or attempt to reconfigure any application installed on any Electronic Systems and Equipment. Helper toolbars installed on Internet browser are not authorized. All Users are required to immediately accept any updates that are applied to their machine through the University's Microsoft or the anti-virus software update programs and complete the required restart as instructed by the installation wizard.

5. No User of any computer within the University network shall access any site associated with the distribution or creation of any application that poses a threat to the University's network or information security. A partial list of application classes that fall into this category include all classes of Mal-Ware included but not limited to the following application classes: Hijackers, bulk e-mailers, P2P file sharing, worms, Trojan-horse, spy-ware, or key-loggers.

6. Privately owned computing equipment is forbidden from being connected to the University's internal (i.e. wired) network. Wireless guest connection points are available campus wide in conference rooms and other areas where Internet access is required by privately owned computer equipment of Users.

7. All information stored on one or more of the Electronic Systems and Equipment should not be released without signed authorization from the individual for whom it pertains or as allowed by the laws in place at the time. At no time should personal information be released to anyone in an unsecured manner or without the appropriate signed authorization.

8. High-risk information like credit card account numbers or Social Security Numbers will not be printed or released on any public document or through any unsecured medium like e-mail. Furthermore, credit card security codes will not be stored on any University Electronic Systems and Equipment.

9. All personnel who work with confidential information are responsible for ensuring that it is secured and safe from unauthorized access. Additionally, anytime the confidential information is no longer needed for an authorized academic or business use, the User using the information is responsible for seeing that it is disposed of in an approved manner subject to PS 999 (Records Retention).

10. Approved methods for the disposal of confidential information include the following:

    a. Paper documents cross cut shredding is required.

    b. Computer media shredding for media like CD, DVD or floppy disk.

c. Computer media like backup tapes or video tapes must be shredded or destroyed by magnetic exposure or fire, where applicable.

11. All personnel who work with confidential information and become aware of a security issue are required to report the issue immediately upon identifying the problem to one of the Incident Response Team ("IRT") members and ITS. Members of the IRT include the Vice President of Administration, Vice President of Information Technology.

a. **Immediately notify a member of the IRT if you discover a security incident or suspect a breach in the University's information security controls.** The University maintains various forms of monitoring and surveillance to detect security incidents, but you may be the first to become aware of a problem. Early detection and response can mitigate damages and minimize further risk to the University.

b. Security Incident Examples. Security incidents vary widely and include physical and technical issues. Some examples of security incidents that you should report include, but are not limited to:

i. Loss or suspected compromise of User credentials or physical access devices (including passwords, keys, badges, smart cards, or other means of identification and authentication);

ii. Suspected malware infections, including viruses, Trojans, spyware, worms, or any anomalous reports or messages from anti-virus software or personal firewalls;

iii. Loss or theft of any device that contains University information (other than Public Information), including computers, laptops, tablet computers, smartphones, USB drives, disks, or other storage media;

iv. Suspected entry (hacking) into the University's Electronic Systems or Equipment by unauthorized persons;

v. Any breach or suspected breach of Confidential or Highly Confidential Information;

vi. Any attempt by any person to obtain passwords or other Confidential or Highly Confidential Information in person or by phone, email, or other means (sometimes called social engineering, or in the case of email, phishing); and

vii. Any other any situation that appears to violate this Policy or otherwise create undue risks to the University's information assets.

c. If Users become aware of a compromised computer or other device, such User should:

i. Immediately deactivate (unplug) any network connections, but do not power down the equipment because valuable information regarding the incident may be lost if the device is turned off; and

ii. Immediately notify a member of the ITR.

12. Breach Notification. Applicable law may require the University to report security incidents that result in the exposure or loss of certain kinds of information to various authorities, affected individuals or organizations whose data was compromised, or both. Breaches of Highly Confidential Information (and especially personal information) are the most likely to carry these obligations. The ITR's incident response plan includes a step to review all incidents for any required breach notifications. Coordinate all external notifications with Chris Hay-Merchant Director of Communications and the ITR. Do not act on your own or make any external notifications without prior guidance and authorization

---

Supporting Documentation:	Employee Handbook, PS 401 (Management of E-Mail), PS 402 (Electronic Systems and Equipment), PS 450 (Operational and Network Security), PS 618 (Password Policy)
Keywords:	information security, computer, network, information technology, IT, information systems, software
Responsible Office:	Information Technology Services (ITS)
Contact Information:	Information Technology Services 402-557-7200
Approved by:	Dr. Mary Hawkins
Effective Date:	January 1, 2021
Review Cycle and Dates:	This policy statement supersedes previous versions of PS 445, dated January 31, 2018 and February 1, 2006.

APPROVED:

/signed/________________________________ 1/1/2021_____________
Dr. Mary Hawkins, Bellevue University President Date