multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

- Information Technology Department is the individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of the University and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.
- Unit is a college, department, school, program, research center, business service center, or other operating component of the University.
- A patch

- Gramm-Leach-Bliley ACT (GLBA) Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance to explain their information-sharing practices to their customers and to safeguard sensitive data.
- Functional Lead - Technical lead point person for a department. Responsibilities include coordination of upgrades, delegating access, and system issues. Acts as a liaison to ITD.
- The Family Educational Rights and Privacy Act (FERPA) a Federal law that protects the privacy of student education records.
- Information Owner - is a person responsible for the management and fitness of information elements (also known as critical data elements) - both the content and metadata.
- Backup is saving or copying information onto digital storage media.
- Restore is performed to return data that has been lost, stolen, or damaged to its original condition or to move data to a new location.
- Recovery Point Objective (RPO) is the maximum acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs.
- Recovery Time Objective (RTO) is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels. The RTO defines the point in time after a failure or disaster at which the consequences of the interruption become unacceptable.
- Electronically stored information (ESI) is the general term for any electronic information stored on any medium (i.e. hard drive, back-up tapes, CDs, DVDs, flash drives, external drives, and any other form of electronic media capable of storing data) that can be retrieved and examined.
- Archive is defined as the saving of old or unused files on off-line mass storage media for the purpose of releasing on-line storage space.
- Disaster Recovery is a combination of the policies, process and procedures related to preparing for recovery of technology infrastructure critical to CSU operations after a natural or human induced event. Disaster recovery focuses on the restoring technology systems that support business functions that fail in the event of a disaster.
- Bring Your Own Device (BYOD) refers to employees who bring their personal devices to work, whether laptop, smartphone, or tablet, in order to interface to the corporate network.

Responsibility

The Personal Device Security Policy for CSU applies to all active members of the University-Related Persons / Employees / Staff, Associates / Contractors or 3rd parties, and Students who use a University supplied personal device to access University Information Resources.

Personnel found to have violated any provision of this policy may be subject to sanctions up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties.

References

- NIST CSF: ID.AM-1, ID.RA-1, PR.AC-1, PR.AC-3, PR.AC-7
- The Illinois State Auditing Act (30 ILCS 5/3-2.4)

Version History

Version	Modified Date	Next Review	Approved Date	Approved By	Comments
1.0	11/3/2022	11/1/2023	11/6/2022	Donna Hart	
			11/1/2023	Donna Hart	