|  |  |  |
| --- | --- | --- |
| **Dimension** | **Key Factors** | |
| Security services and operations | * Individual with institution-wide information security responsibility and authority written in their job description, or equivalent. Note: This may be the CIO, CISO, CSO, or other. * Duties are sufficiently segregated to ensure unintentional or unauthorized modification of information is detected. * Individuals interacting with institutional systems receive information security awareness training. * Participation in local or national security groups (e.g., REN-ISAC, EDUCAUSE, InfraGard, etc.). * Incident-handling procedures include the definition of roles and responsibilities. * Incident response staff are aware of legal or compliance requirements surrounding evidence collection. | * Relationships with local law enforcement authorities. * Information security policy has been approved by institutional leadership. * Incident-handling procedures in place to report and respond to security events throughout the incident life cycle. * Incident handling procedures include the requirement to hold an after-incident review to determine the need for new controls to reduce the likelihood and impact of future incidents.   Assessment of security controls of contracted services with external entities (third parties) before granting access to sensitive institutional information assets. |
| Asset protection | * Monitor and promptly respond to patch releases, security bulletins, and vulnerability reports. * An Acceptable Use Policy defines misuse of institutional IT resources and data. * Maintain security configuration standards for information systems and applications. * Procedures and technologies in place to protect sensitive data from unauthorized access and tampering. * Data backup process is consistent with the availability requirements of our organization. * Data backup restore procedures routinely tested. | * Access control procedures to authorize and revoke access rights to information systems and physical assets. * Procedures to regularly review users' access to ensure only needed privileges are applied. * Authorization system that enforces time limits lockout on login failure and defaults to minimum privileges. * Methods to detect, quarantine, and eradicate known malicious code on information systems including workstations, servers, and mobile computing devices. |
| Systems review | * Process for identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of records containing sensitive information. * Vulnerability management strategy in place. * Process for routinely monitoring logs to detect unauthorized and anomalous activities. * Secure log data to prevent unauthorized access and tampering. | * Configuration-management process in place to ensure that changes to our critical information systems and applications are for valid business reasons and have received proper testing and authorization. * Complete independent security reviews at planned intervals and when significant changes to the environment occur. |
| Policies | * Usage guidance established for mobile computing devices (regardless of ownership) that store, process, or transmit institutional data. * Policies indicate when encryption should be used (e.g., at rest, in transit, with sensitive or confidential data, on certain types of devices, etc.). * Identification of critical information assets and the functions that rely on them. * Classification of data to indicate the appropriate levels of information security. * Standards for isolating sensitive data to protect it from unauthorized access and tampering. * Records management or data governance policy that addresses the life cycle of paper and electronic records. | |
| Business continuity | * Business continuity plan for information technology that has been reviewed and approved by senior staff or the board of trustees and that is periodically tested. | |