3.9. The institution implements, enhances, and secures its technology resources to support and sustain educational services and operational functions. The institution clearly communicates requirements for the safe and appropriate use of technology to students and employees and employs effective protocols for network and data security.

Review Criteria:
• The institution aligns technology planning, implementation, and maintenance with the institutional mission and goals.
• The institution's technology infrastructure is appropriate to support educational services and operations.
• The institution clearly communicates guidelines/rules for appropriate use of its technologies to all users.
• The institution's networks are secure and data is protected.
• The institution regularly evaluates its technology infrastructure (including network security) to ensure ongoing effectiveness in supporting educational services and operations.

Possible Sources of Evidence Could Include:
• Technology plans, educational master plans, or program reviews addressing technology needs
• Documentation of procedures for incidents of security threats and corresponding resolutions
• Publications containing acceptable use policies or guidelines (employee handbooks, student handbooks, Board policies, etc.)

3.10. The institution has appropriate strategies for risk management and has policies and procedures in place to implement contingency plans in the event of financial, environmental, or technological emergencies and other unforeseen circumstances.

Review Criteria:
• The institution has policies and procedures in place that will mitigate emergencies and unforeseen occurrences that would significantly impact availability of its resources.
• The institution has sufficient insurance to cover its needs. If the institution is self-funded in any insurance categories, it has sufficient reserves to handle financial emergencies.
• The institution routinely reviews and updates their insurance coverages.
• The institution has protocols for back-up and recovery of sensitive data systems, including student and employee information systems.

Possible Sources of Evidence Could Include:
• Policies or procedures for risk management
• Records of self-insurance for health benefits, workers compensation, and unemployment
• Contingency plans for financial, environmental, technological, and other emergencies