Information Security Management Models

Taaj Scholar Academy- Business Continuity Plan

CYB-535

Grand Canyon University

August 14th, 2024

Company Description

Taaj Scholar Academy is an educational institution committed to delivering high-quality academic programs and fostering an enriching learning environment for students. With advanced technology and innovative teaching methods, our goal is to support and empower both students and faculty in achieving educational excellence.

Mission Statement

The mission of Taaj Scholar Academy is to provide exceptional educational experience through innovative learning solutions and supportive technology infrastructure, and empowering students and faculty by delivering reliable and secure educational resources, ensuring that academic activities continue seamlessly even in the face of unforeseen disruptions.

Web Applications

Taaj Scholar Academy utilizes a range of web applications to support educational activities, including online learning platforms, grade management systems, and communication tools. These applications are essential for facilitating remote learning, managing academic records, and enabling effective interaction between students and faculty.

Servers

Our IT department comes fully loaded with robust servers for web applications, critical data storage, and ensure reliable access to educational resources. These servers are managed to provide high availability and performance, supporting the day-to-day operations of the Academy.

Departments

When it comes to handling various aspects of technology management, the Academy's IT department is structured in areas such as network administration, user support and application support.

Routers and Switches

Routers and switches are integral components of our network infrastructure, because it directs data traffic between devices and ensures efficient communication across the Academy's network.

Remote Access

Solutions are provided to support remote learning and flexible working arrangements. Authorized users can connect to the Academy’s network to access resources from outside the campus through VPNs and secure portals.

Wireless Communication

Students and faculties will have reliable access to the network within the campus through our wireless communication systems. Robust Wi-Fi solutions is deployed to support a high density of users and ensure consistent connectivity.

Firewalls

To prevent unauthorized access and potential cyber threats, firewalls are employed to protect the Academy’s network. Incoming and outgoing traffic are filtered based on security rules, which helps to safeguard our IT infrastructure from malicious activities.

Demilitarized Zone (DMZ)

At Taaj Scholar Academy the DMZ is a network segment that separates our internal network from external networks. It hosts public-facing services such as our website and email servers and an extra layer of security to protect sensitive internal systems is added.

The NIST Cybersecurity Framework (CSF) is voluntary guidance, based on existing standards, guidelines, and practices to help organizations better manage and reduce cybersecurity risk (NIST, n.d.). Therefore, to integrate the framework security activities into Taaj Scholar Academy, our approach will consist of assessing and mapping of current and existing controls and customizing and tailoring the framework to address needs and risk associated with educational institutes.

Phishing attacks, ransomware, data breaches and insider threats are common risks and dominant threat to information security. These forms of attack can affect individuals and large organizations (CISA, n.d.). Developing a system-specific protection plans for intellectual property is important when data classification is implemented, strong encryption method is utilized for data at rest and in transit and strict access controls at put in place to ensure that sensitive information is accessible for authorized personnel only.

To protect Taaj Scholar Academy from unauthorized users, the following security models to information Security Management must be applied. Role-Based Access Control (RBAC) must be implemented, multi-factor authentication must be enforced for accessing critical systems and data and audits and reviews must be conducted regularly.

Management of Access Control Mechanisms that should be applied to ensure information is protected against unauthorized users includes access policies, continuous monitoring and real-time alert and training for staff.

When it comes to the roles in the planning and managing of the security plan by examining C-level functions that impact cybersecurity, the following personnel play is major role

Board of Directors: Strategic directions and ensure alignment with organizational goal are provided and approvals of any sort is overseen to support the budget

Senior Management: Resources are allocated to ensure the integration of security practices into overall management. Their role plays a major impact in cybersecurity initiatives and communicating their importance across the organization (NIST, 2011).

Chief Information Security Officer (CISO): Oversee their organization's information security strategy, ensuring all systems and networks remain secure and compliant with industry regulations. They lead the development and implementation of the cybersecurity strategy (SANS n.d.).

IT Management (CIO, IT Director, etc.): IT resources are managed while they oversee the technical implementation of security measures. In addition, the security infrastructure supports the overall cybersecurity strategy and remains up to date.

Functional Area Management: Security practices are implemented within their respective areas and ensure compliance. Organizations assess and protect public data about themselves that could, if properly analyzed and grouped with other data by a clever adversary, reveal a bigger picture that ought to stay hidden (ISACA, 2021).

Information Security Personnel: Execute day-to-day security tasks and respond to incidents. Impact: Monitor, detect, and address security issues in real-time, and contribute to continuous improvement

End Users: In simple terms, security policies and practices must be established and followed**.** They must act as the first line of defense against security breaches and sensitive information should be kept safe.

References

CISA, (n.d.). https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

ISACA (2021) Operational Security: A Business Imperative. Retrieved from https://www.isaca.org/resources/news-and-trends/industry-news/2021/operational-security-a-business-imperative

NIST, (n.d.). https://csrc.nist.gov/CSRC/media/Projects/cybersecurity-framework/documents/Framework_Quick%20Start_Guide.pdf

NIST, (2011) Managing Information Security Risk. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

SANS, (n.d). https://www.sans.org/cyber-security-certifications/ciso-certification/