.2 Information Security

.2.1 PHYSICAL SECURITY

.2.1.1 ADMINISTRATIVE SECURITY CONTROLS

Overview

This security is intended to reduce the risk of harm to users. Reduce and manage the enterprise's potential loss.

Purpose

The purpose of Administrative Security Controls is to ensure the legality of accessing confidential information and to classify if the person is trustworthy and loyal.

Policy

• All Safety Officers must demonstrate their credibility and ability to be trusted in their role. Especially for jobs where they are responsible for the security of information and confidential data.

• As part of the data collection process, information security should be discussed with the Safety Officer.

• Before accessing all information in the system, all safety officers should sign a Non-Disclosure Agreement.

• All safety officers should be aware of and reminded of the Non-Disclosure Agreement once they have completed their work, resigned, or been terminated.

• If anyone is caught being malicious and violating information security policies, the system will provide anonymous reporting of the violation.

Strategy

• All Safety Officers must validate their identity using the admin-provided account.

• To secure and protect both parties, all Safety Officers must sign a Non-Disclosure Agreement.

• All Safety Officers must be aware of the possible consequences of failing to maintain the confidentiality and integrity of data collected.

.2.1.1.1 ACCOUNT MANAGEMENT

Overview

A policy that sets the rules for various user accounts is known as account management. establishing a user's rights to use the given accounts and granting privileges to associated user accounts.

Purpose

The purpose of this policy is to establish a level of administrative control related to account management in School Management System: Safety and security . This policy sets the default policy for managing accounts.

Scope

This policy applies to all accounts directly managed by School Management System.

Policy

1.Access Control

• The Safety officer 3 account OIC has complete access to the entire safety and security system.

• Access to the safety and security system is restricted for Safety Officer 1 and 2 accounts.

• According to the Integration, different accounts are restricted from accessing other subsystems in order to protect confidential data within the Enterprise Integration system.

• If the Safety Officer is terminated or resigns, the associated accounts will be terminated as well.

2.Security Session

a. The user will automatically log out when he/she doesn’t do any activities on the system.

b. The system will provide a session time out to prevent intruders and unauthorized data.

3.Hash Function

• The system will have a cryptography hash function to secured the data in the system.

• The IT department will used an algorithm that will help implementing the security.

• Hash provides confidentiality to the system by transforming a data into fixed value or sized.

• It department will implement an encryption to ensures the security in transmitting data from one another.

• The IT department will used an encryption in the accounts of the users to secured their password and identity.

Strategy

• The Safety Officers have accounts that are restricted to their respective roles.

• If a user does not interact with the system for an extended period of time, the system will automatically log them out.

• If the account holder is terminated or leaves the department, the given accounts will be deleted.

• The password sets in the database should not easily determine it should have an security that will facilitate the account s of the users.

.2.1.2 IT AND SECURITY POLICY

Overview

This policy supports the maintenance and preservation of informational principles that establish a standard of security and protect School Management System from threats and unauthorized data.

Purpose

This policy is primarily concerned with protecting information from data leaks, destruction, and intruders, as well as ensuring the confidentiality, integrity, and availability of data, assets, and information in the system.

Scope

This policy is primarily concerned with protecting information from data leaks and destruction. It applies to all subsystems that integrate with the School Management System, as well as users, visitors, contractors, and any other parties who have access to the system.

Policy

• The School Management System, web application, and hardware are shred resources for authorized users to use fairly, legally, and exclusively within the school grounds.

• Access to the system will be restricted to authorized users and school-related operations.

• All information generated by school operations is kept solely at BESTLINK COLLEGE OF THE PHILIPPINES and is only accessible to authorized personnel.

• Data availability is determined by the level of access granted to users in order to avoid information disclosure.

1. Two-Factor Authentication

• The users need to verify their identity by inputting their password

• The users need to input a verification code which was sent to their registered email address.

• The users are required to input a strong password ,which has a combinations of characters ,letters and numbers.

• The password will have a combination of Letters, characters and numbers.

2. Data Privacy Act

• The users should know the RA.10173 also known as Data Privacy Act which protects the privacy of individuals whole ensuring free flow of information to promote innovation and growth.

• The users are informed about the law.

Strategy

• Users must validate their accounts by entering the proper password and code.

• Authorized personnel must be trustworthy and accountable.

• To avoid malicious activity, all devices that have been used will be monitored.

• Users are informed of their responsibilities as system account holders.

• The system will display a message box containing instructions for entering their password and username.

• The user should be aware of and knowledgeable about the law in order to protect their data and privacy.

• The aforementioned law will be posted in the system to remind them of their rights.

.2.1.3 TECHNICAL SECURITY CONTROLS

Overview

Controls the hardware and software devices t

Hat protect a system against cyberattacks.

Purpose

To ensure the safeguard of users and maintaining the security of the system.

Policy

• IT department will establish policy that maintain the system from cyberattacks

• IT personnel will conduct a Security method that will ensures the safeguard of the users .

• IT department will implement a authentication security to avoid intruders in the system.

• IT department will scheduled a vulnerability test I the system to help strengthen the security of the system.

• The devices are placed in a secured environment and only authorized personnel is allowed

• It personnel used a software licensed and supported .

.2.1.3.1 IT INFRASTRUCTURE SECURITY

Overview

The IT infrastructure security focuses on protecting the BESTLINK COLLEGE OF THE PHILIPPINES' hardware, software, and assets, as well as the devices, secure workplace, and system. It also includes backups and secure against physical and cyber threats.

Purpose

It secures the various hardware and software in Bestlink College of the Philippines. Devices, network systems, and cloud resources are frequently used. It safeguards against both physical and cyber-attacks.

Scope

In Bestlink College of the Philippines, infrastructure security is only applied to the School management system. The securities will be practiced and implemented to protect the Bestlink College of the Philippines' assets and users.

Policy

• Always lock and secure your workspace to prevent unauthorized access.

• Unauthorized personnel should be prohibited from entering workstations where information and data are processed and stored.

• The physical backup should have been stored in a safe or vault to prevent theft.

• Always monitor the system's user activity.

• Inspect the system and workstation for any suspicious attempts or actions.

• Personal, staff, security officers, administrators, and students' data should be stored in separate repositories and accessed only by authorized personnel.

• Students, personnel, and staff must provide any identification required to enter the school grounds.

• Visitors must provide their information in order to obtain a visitor pass

.2.1.3.2 SOFTWARE SECURITY MANAGEMENT

Overview

It is a protection applied in different software or application.

Purpose

It protects and secure al the data information, user and devices it self.

Policy

• IT department and authorized personnel will perform and maintain the patching of the system and software.

• The authorized personnel should educate and train all the user.

• IT department should check if the software security applied.

• IT department should monitor the activities of the users.

• IT department should have a documenting of the security and policies that will used by the users of School Management System.

• Licensed software are installed and followed.

• The System has a list if accounts that maintained and secured.

• The IT department will perform a Security measure that prevent the system, software and evidence from viruses a and malicious attack.

• The IT department has implemented a Security that filters spams and malicious activities in the system.

.2.1.3.3 CLOUD SECURITY

Overview

The Cloud Security Policy has the three core capabilities: confidentiality, integrity, and availability.

Purpose

The purpose of this policy is to maintain the security for cloud supported activities that protect School Management System . It’s protects the cloud-based information system ,networks, data, databases and other information assets of Bestlink College of the Philippines.

Scope

The scope of this cloud security is applicable only in School Management Systems in Bestlink College of the Philippines .including databases, network resources that implemented in cloud-based server.

Policy

• Cloudflare Inc, has been certified to a new international privacy standard for protecting and managing the processing of personal data — ISO/IEC 27701:2019. This standard is less than two years old, and adapts the existing Information Security Management System concept into the creation of a Privacy Information Management System (PIMS).

• Cloudflare Inc, will process the cloud security of School Management System: Safety and Security. It helps to utilize software and systems to reduce the threat of security breaches; regularly test the security parameters using forensic methods and document all the information regarding cloud procedures and controls.

• The team of Cloudflare Inc for School Management System will prepare and document information security plans and focus on cloud services that will facilitate the maintenance of the system.

• Cloudflare Inc, is responsible for complying the regulatory or contractual requirements that will notify their end-users and government authorities of any personal data breaches.

Strategy

• The Security team will conduct a risk assessment in internal and external threats and vulnerabilities of cloud servers.

• The Security team will establish policy for implementation of cloud services, creation ,storage and destruction.

• Cloudflare Inc, has a policy for accessing School Management Systems, network, applications and files that is implemented in cloud services. This policy also include authentication.

• Cloudflare Inc, ensures its clients that malwares is prevented through the use of antivirus software and other appropriate prevention and security detection .All third-party are approved by School Management System.

.2.1.3.4 CYBERSECURITY

Overview

Cybersecurity for IT infrastructure security is to protect computer systems and network from different attacks that the stakeholders of School Management System website may encounter. It protects the data and prevents any possible loss of information’s of school staff, students and school personnel.

Purpose

The purpose of this policy is to secured the School Management Systems in any different possible attacks and to avoid data loss that may affect to the website service, software and physical interaction.

Scope

The Cybersecurity policy only applied to the stakeholders of the School Management System in Bestlink College of the Philippines. Its has a policy or guidelines that covers all computing devices .

Policy

• The stakeholders should not copy or any data and information without authorization.

• The stakeholders should not visit unsafe websites to avoid possible cyberattacks.

• The stakeholders should not download or install different software using the school management system computing devices without authorization.

• Unauthorized personnel should not have a access in any information and data that is not need to their work description.

• Unknown personnel should not be in workplace where data is being processed. The networks must have Firewalls enabled.

• Unauthorized parties should not have a access in private IP address routing information.

Strategy

• All authorized personnel should have their own Identification exclusively for them.

• The system will have Restrictions in different account holders to protect data from system.

• The team will scheduled a maintenance and preservation of files and information in the system.

• All physical backup should be place in secured workplace that only authorized personnel has a access.

• Shared devices will automatically locked when left unattended or not supervised.

• The team will removed all users that is not or no longer affiliated in the system.

• The team will establish a policy that maintain the FAQ that set in the system.

• The team will disabled or deactivate the devices specially mobile if its stolen or loss.

.2.1.4 NETWORK SECURITY

Overview

The network is prone to cyber attackers, because of the network devices such as routers ,switches, firewalls and many more. This devices in not generally maintained at the same security level as the desktop and mobile devices.

Purpose

To protect and assure the users from accessing and using the website and mobile application.

.2.1.4.1 FIREWALL MANAGEMENT

Overview

Firewall Management Policy is a security that monitors and filters the inbound and outbound traffic according to School Management System policies.

Policy

• The cloudflare inc. has a built-in web firewall that protects the transmission and transaction of data online.

• The desktop used has a built-in firewall that protects devices from attacks.

• Firewalls must be updated and provide services such as permit and protocols.

• Accessing private IP address or rooting information are not be granted to unauthorized parties.

• All rule in firewall are well documented and approved by the authorized personnel .

• Any alert detected are required to investigate to assure the users ,devices and the system.

• Cloudflare uses a smart routing to identify the fastest routes in the internet.

• Cloudflare use a TLS that HTTPS website use to encrypt and authenticate communications.

• Cloudflare provide a Security that doesn’t allow the users from accessing the website while they’re using the public Wi-Fi.

.2.1.4.2 NETWORK DEVICES SECURITY

Overview

Refers to the Network Administrator use policies to configure, monitor and secure the network devices against unauthorized access.

Policy

• The system was Implemented with WAF (Web Application Firewall), that allows and blocks traffic and suspicious activity.

• The Firewalls are responsible in segregation of licensed devices and software to unsecured devices.

• Unsecured and unused services and devices should turned off.

• Setting passwords to devices is a must and held to higher standard than any other security.

.2.1.4.3 SOFTWARE PATCH MANAGEMENT

Overview

This policy is to create guidelines for the base configuration of School Management System server equipment that is operated. This policies will reduced if followed correctly.

Policy

• Licensed and Supported Software is used and followed by the IT personnel.

• Software updates a d Security patches is assess by the IT Personnel under the control and supervision of the owners and managers.

• The IT department will set up a patch testing environment that will test the functionality and to ensure it will not harm the system or web application.

.2.1.4.4 MALWARE PROTECTION

Overview

Malware is spread through links, email and file attachments. The malware was triggered when the user click links, open or download files and the malware will begin to spread malicious behavior in to the entire system and devices.

Policy

• Anti-malware should have been used or Implemented in the system .

• Malware protection should provide an audit logs.

• IT Security must have a precautionary measure to avoid or battle from malware attacks.

• Hostinger provide a automatic Malware scanner that will help to identify and remove malicious files and prevent the system from malware infections.

• Cloudflare Gateway helps to keep end users devices safe and secured by blocking attempts to download malware.

• Cloudflare automatically detects DDoS attacks .

• Cloudflare filters the spam attacks that protect website from DDoS attacks,SQL injection ,comment spam. This will ensure a safe environment to the website.