Policies, Standards and Procedures

Why Should a Non-Profit Develop Policies, Standards and Procedures?

Policies, standards, and procedures serve as the foundational guidelines for The Knowledge House's cybersecurity posture. They provide a well-defined roadmap to help the organization navigate the complex landscape of cybersecurity, ensuring that everyone understands their responsibilities and what is expected of them.

Why Should a Non-Profit Develop Policies, Standards and Procedures?

As an educational non-profit organization, The Knowledge House is subject to various regulations, including FERPA, COPPA, and PCI DSS. These regulations often require organizations to have specific policies and procedures in place to protect sensitive data. By maintaining up-to-date policies, standards, and procedures, The Knowledge House can demonstrate its compliance with these regulatory requirements.

Why Should a Non-Profit Develop Policies, Standards and Procedures?

As an educational non-profit organization, The Knowledge House is subject to various regulations, including FERPA, COPPA, and PCI DSS. These regulations often require organizations to have specific policies and procedures in place to protect sensitive data. By maintaining up-to-date policies, standards, and procedures, The Knowledge House can demonstrate its compliance with these regulatory requirements. The policies, standards and procedures developed for The Knowledge House include Access Management, Password Policies, Remote Work Policies, Incident Reporting, and Data Handling & Classification.

Understanding Access Management at The Knowledge House

Access Management is a critical component of our security infrastructure at The Knowledge House. It ensures that only authorized individuals can access specific systems, data, and applications based on their role. Our Access Management policy defines roles, user authentication procedures, data access controls, and account management.

Access Management at The Knowledge House: Your Role and Permissions

Each role within The Knowledge House has predefined access permissions, based on job responsibilities. It is crucial for employees to understand the scope of their roles and the permissions associated with them. Accessing systems or data beyond one's authorization is strictly prohibited and can have serious consequences.

User Authentication Procedures

User Authentication Procedures are essential for verifying the identity of users trying to access our systems. This involves the use of strong passwords, two-factor authentication, and ensuring that credentials are kept secure.

Managing Your User Account

Be vigilant with your account settings and permissions. Regularly review and update your account security settings. Report any suspicious activity related to your account immediately to the IT department.

Password Policies and Procedures

Strong, unique passwords are a cornerstone of security. Passwords must be complex and not easily guessable. Regularly changing passwords and employing two-factor authentication are highly recommended.

Remote Work Policies and Procedures

The Knowledge House supports remote work while ensuring that data and systems remain secure. Our Remote Work Policy encompasses secure access procedures, employee training, securing devices and home networks.

Remote Access Procedures

Remote access to The Knowledge House systems is secured through VPNs and requires multi-factor authentication. Employees must ensure that they are connecting through a secure network and that their devices are free of malware.

Incident Reporting Procedures

Employees are required to report any security incidents immediately. Our Incident Response Team will then take the necessary steps to contain and mitigate the impact of the incident.

Data Handling and Classification Policies and Procedures

Data Handling and Classification Policies guide how different types of data are to be handled within The Knowledge House. These policies categorize data based on sensitivity and specify the protocols for storing, sharing, and disposing of data.

Data Types and Handling Procedures

Data types include Personal Identifiable Information (PII), financial information, course materials, and more. Handling procedures encompass encryption, access controls, and proper disposal methods.

Compliance, Audit and Training

Regular audits are conducted to ensure compliance with our policies and external regulations. Training programs are in place for employees to stay updated on best practices and the importance of cybersecurity.

Policies, Standards and Procedures – Moving Forward

Policies, standards, and procedures are not static documents, but dynamic instructions that guide our daily operations. They establish The Knowledge House's commitment to incident and disaster preparedness, outlining the measures we take to mitigate potential threats and disruptions.

Presented by:
Mishelly Sandoval