Secure Programs: Development of Policies, Procedures, and Standards

What is Access Management?

Access Management is a critical part of our security infrastructure, designed to identify, control, and manage access to our systems, data, and applications.

This policy is a blueprint for our approach to Access Management, which involves defined roles and permissions, user authentication procedures, account management, data access controls, and more.

Password Policies and Procedures

Welcome to Password Policies and Procedures

The Knowledge House recognizes the vital role that password security plays in safeguarding our systems and data. This policy establishes standards and guidelines for password creation, management, and usage. By adhering to this policy, we can enhance our collective cybersecurity and facilitate our compliance with federal and state regulations and standards.

Protecting Your Passwords

Passwords should never be shared with anyone, including colleagues or IT staff. Each account should have a unique password. If you need to write down passwords, store them securely, away from public view. Never store passwords as plain text or in unencrypted files.

Password Management and Two-Factor Authentication

We encourage the use of secure password management tools for storing and generating strong passwords. We also advise activating two-factor authentication (2FA) for all accounts where possible. 2FA adds an extra layer of security and significantly reduces the risk of account compromise.

Remote Work Policies and Procedures

Welcome to the Remote Work Policy and Procedures

The Knowledge House recognizes the growing trend of remote work and its benefits. This Remote Work Policy aims to ensure that our digital assets and infrastructure are accessed safely and protected. The purpose of this policy is to mitigate potential risks such as unauthorized or unsafe usage of company resources, and to prevent potential loss or exposure of sensitive data.

Remote Work Policy Statement

All employees, contractors, vendors, and agents with remote access permissions must ensure that their remote connection is as secure as their on-site connection. The Knowledge House's networks should not be used to access the Internet for external business interests.

Remote Access Procedures

Remote access must be established using our Virtual Private Networks (VPNs), with encryption and strong pass-phrases. TKH-owned devices used for remote connection should not be connected to any other network simultaneously. The use of external resources for TKH business must be pre-approved by the relevant manager.

Securing Home Devices and Home Networks

To prevent unauthorized access, devices should always be locked when not in use. We also ask employees to secure their home Wi-Fi networks, disconnect devices not in use, and use a VPN when accessing TKH's network remotely.

Incident Reporting and Response Policies and Procedures

Welcome to Incident Reporting and Response Policies and Procedures

At The Knowledge House, we recognize the significant risks that cybersecurity incidents pose to our operations, reputation, and data. This policy provides clear steps for reporting and responding to potential cybersecurity incidents.

Incident Report Policy Statement

Our goal is to create an environment well-equipped to handle cybersecurity incidents by adopting a proactive approach, including a responsive team, a well-defined response process, and frequent practice drills to ensure readiness.

Incident Reporting Procedures

Any unusual or suspicious activities on devices or within the organization's network should be reported immediately. Reports should contain as much detail as possible, and employees should cooperate fully with the IRT.

Incident Reporting Procedures

Any unusual or suspicious activities on devices or within the organization's network should be reported immediately. Reports should contain as much detail as possible, and employees should cooperate fully with the IRT.

Data Handling and Classification Policies and Procedures

Welcome to Data Handling and Classification Policies and Procedures

At The Knowledge House, we handle a large amount of sensitive data. Our Data Handling and Classification Policy is designed to provide clear guidelines for handling, storing, and transmitting different types of data.

Data Types

Our data is divided into four categories: Public, Internal, Confidential, and Sensitive. Each category requires a different level of security and has specific guidelines for handling, storing, and transmission.

Data Handling Procedures

All data types, from Public to Sensitive, have specific handling procedures. These procedures dictate how the data should be used, stored, shared, and transmitted. Non-compliance with these procedures may result in disciplinary action.

Building a Stronger Cybersecurity Culture at TKH Together

All employees are expected to adhere to the guidelines presented in the policy. Regular training sessions will be provided to increase cybersecurity awareness. Open and prompt communication is crucial, especially in reporting potential cybersecurity incidents.

Remember, cybersecurity is not solely the IT department's responsibility; it's everyone's.