# Secure Programs: Development of Policies, Procedures, and Standards

# Welcome to The Knowledge House Technology Policies and Procedures

Welcome to our Technology Policies and Procedures manual. In our digitally connected world, the security and protection of our organization's data and resources are vital to successfully fulfilling our mission. With our operations heavily reliant on technology, the safeguarding of these digital assets becomes not just an operational necessity, but also a core responsibility to our stakeholders, donors, and students.

# Who does this apply to?

This manual applies to every member of our organization, regardless of their role or function. Everyone from the CEO down to the intern staff is included, as it is paramount that everyone understands and abides by the stipulated guidelines.

# Understanding Your Role and Permissions

# 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.

# Understanding Your Role and Permissions

Every role in the organization has predefined access permissions based on job responsibilities. As an employee, you must understand what your role entails and what permissions you have. It is essential never to try to access systems or data that are beyond your scope of work or authorization.

# User Authentication Procedures

Always follow the organization's user authentication procedures. This involves setting up strong, unique passwords for your accounts, changing them regularly, and utilizing multi-factor authentication when available. Under no circumstances should you share your credentials with anyone, even within the organization.

# Managing Your User Account

If you suspect your account has been compromised, notify your IT department or manager immediately. When leaving the organization or changing roles, ensure that your old account permissions are updated or deactivated as appropriate, to prevent any potential misuse.

# Respecting Data Access Controls

Access controls are in place to protect sensitive data and systems. Do not attempt to bypass these controls. If you believe you require access to certain data that you currently do not have access to, request the access through proper channels, explaining your requirements clearly.

# Regular Access Reviews

Regular access reviews ensure that employees have the appropriate access rights for their current role. These reviews involve confirming your current role and access permissions. If you no longer require certain permissions, notify your manager or IT department so they can be removed.

# Training and Awareness

Participate in all access management and cybersecurity training provided by the organization. This training will help you recognize phishing attempts, handle sensitive data appropriately, and report any suspicious activity.

# Monitoring and Logging

As part of our cybersecurity measures, your activities may be monitored and logged. This isn't intended to infringe on your privacy but to protect the organization's data and resources. Understanding and accepting this policy is crucial for maintaining a secure digital environment.

# Third-Party Access

If your role involves dealing with external partners or vendors who require system access, ensure that you follow the organization's guidelines. Contracts should include the required data protection measures, and third-parties must comply with our access management policies.

# Compliance with Regulations

As a New York-based organization, we are subject to various federal and state data protection and privacy regulations. If your role involves handling personal or sensitive data, ensure you understand your responsibilities under these regulations. Non-compliance can lead to severe consequences for both the individual and the organization.

# 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.

# Creating Strong, Unique Passwords

Each password should be at least 12 characters long and contain a mix of uppercase and lowercase letters, numbers, and special characters. Avoid using common words, dictionary terms, or easily guessable information such as birthdays or names. The use of sequential or repetitive characters is strictly prohibited.

# 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.

# Changing and Expiring Passwords

Change your passwords every 90 days at the least, and never reuse any of your previous five passwords. If you suspect that your password has been compromised, change it immediately. When an employee leaves the organization, their passwords should be changed or accounts deactivated.

# Account Lockouts and Failed Login Attempts

An account lockout policy will be implemented if a certain number of unsuccessful login attempts are recorded. This policy is designed to prevent unauthorized access attempts and protect your account.

# 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.

# Employee Training and Awareness

We will provide regular training sessions to educate employees about this Remote Work Policy, potential risks and threats associated with remote work, and encourage immediate reporting of any security concerns or incidents to the IT department.

# 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.

# Compliance, Audit and Training

All employees are expected to comply with this policy. Regular audits will be conducted, and training will be provided to all employees on data handling procedures and best practices. Violation of this policy may result in disciplinary action, including termination of employment.

# 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.