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. This manual presents our commitment and strategic approach to managing access to these digital resources. The Technology Policies and Procedures detailed herein applies to every member of our organization, regardless of their role or function, as it is paramount that everyone understands and abides by the stipulated guidelines.

Access Management Policies & Procedures

The protection and security of our organization's data and resources are of paramount importance to fulfilling our mission. With our operations increasingly dependent on technology, safeguarding these digital assets is not only an operational necessity but a responsibility to our stakeholders, donors, and students. This Access Management Policy, therefore, outlines our commitment and approach to managing access to these digital resources.

Policy Statement

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 applies to all employees, from the CEO to the custodial staff, irrespective of their roles or functions within the organization. It is, therefore, crucial that everyone understands the implications and abides by this policy.

Definitions

In the context of this policy, "data" refers to any information that our organization processes, stores, or transmits, which may be in electronic or physical form. Data may include personal information, financial information, educational records, and any other type of information that the organization handles.

Access Management Procedures

1. *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. Never try to access systems or data that are beyond your scope of work or authorization.

2. *User Authentication*

Always follow the organization's user authentication procedures. Typically, this involves setting up strong, unique passwords for your accounts, changing them regularly, and utilizing multi-factor authentication when available. Do not share your credentials with anyone, even within the organization.

3. *Managing Your User Account*

Notify your IT department or manager immediately if you suspect your account has been compromised. If you are leaving the organization or changing roles, ensure that your old account permissions are updated or deactivated as appropriate.

4. *Respecting Data Access Controls*

Never attempt to bypass data access 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.

5. *Regular Access Reviews*

Cooperate with regular access reviews by 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.

6. *Training and Awareness*

Participate in all access management and cybersecurity training provided by the organization. Understand how to recognize phishing attempts, handle sensitive data appropriately, and report any suspicious activity.

7. *Monitoring and Logging*

Be aware that your activities may be monitored and logged for security purposes. This isn't intended to infringe on your privacy but to protect the organization's data and resources.

8. *Incident Response*

If you detect or suspect a security incident, such as unauthorized access or a breach, report it immediately according to the organization's incident response plan.

9. *Third-Party Access*

If your role involves dealing with external partners or vendors who require system access, make sure to follow the organization's guidelines. Ensure contracts include the required data protection measures and that third-parties comply with our access management policies.

10. *Compliance with Regulations*

Comply with all relevant data protection and privacy regulations. If your role involves handling personal or sensitive data, make sure you understand your responsibilities under these regulations.

Adherence to this policy is essential in preserving the integrity and security of our systems, data, and resources. We value your cooperation in maintaining this secure environment, ensuring our organization's resilience and ongoing success.

Passwords Policies & Procedures

The Knowledge House appreciates the vital role that cybersecurity plays in its successful operation. Passwords serve as our first line of defense in safeguarding our systems and data. It is crucial that each member of our team ensures the strength and confidentiality of their passwords. This policy aims to establish standards and guidelines for password creation, management, and usage, thereby enhancing our collective cybersecurity. We believe that adherence to this policy will facilitate our compliance with federal and state regulations and standards.

Policy Statement

TKH's password policy has been crafted to uphold the security and integrity of our data and digital resources. We expect all employees, irrespective of their roles, to create strong, unique passwords and use them responsibly. Our policy seeks to offer a comprehensive understanding of how to maintain password complexity, protection, and effective management. It also sets out procedures for password change, expiration, account lockouts, two-factor authentication, and consequences of policy violation. We also acknowledge the importance of regular training sessions to keep our employees aware and updated about password security best practices.

Procedures

1. *Password Complexity*: Each password should be at least 12 characters long, comprising a mix of uppercase and lowercase letters, numbers, and special characters. Common words, dictionary terms, or easily guessable information should be avoided. The use of sequential or repetitive characters is strictly prohibited.
2. *Password Protection*: Passwords should never be shared with anyone, including colleagues or IT staff. Each account should have a unique password, and writing down passwords is discouraged. If necessary, they should be stored securely, away from public view.
3. *Password Change and Expiration*: Passwords should be changed every 90 days at the least, and previous five passwords should not be reused. Passwords should be immediately changed if suspected to be compromised or if an employee exits the organization.
4. *Account Lockout and Failed Login Attempts*: An account lockout policy will be implemented if a certain number of unsuccessful login attempts are recorded.
5. *Password Management and Storage*: We encourage the use of secure password management tools for storing and generating strong passwords. Passwords should never be stored as plain text or in unencrypted files.
6. *Two-Factor Authentication (2FA)*: We advise activating 2FA for all accounts where possible. We also recommend using 2FA for personal email accounts and other external services.
7. *Employee Training and Awareness*: Regular training sessions will be organized to educate employees about the best practices of password security.
8. *Policy Enforcement and Consequences*: Violations of this policy can result in consequences, including temporary account suspension and other disciplinary actions.

By maintaining a strong password policy, we aim to bolster our cybersecurity strategy, protecting our systems and data integrity. Each member's active involvement in upholding the security of TKH's digital environment is vital for the successful implementation of this policy.

Remote Work Policies & Procedures

In response to the growing trend of remote work, The Knowledge House has established this Remote Work Policy to ensure the safe access and protection of our digital assets and infrastructure. This policy outlines the guidelines for accessing TKH's network remotely from any device, including mobile phones, tablets, and laptops. Our aim is to mitigate potential risks, such as unauthorized or unsafe usage of company resources, which could potentially lead to loss or exposure of sensitive data, harm to our reputation, internal systems, intellectual property, and financial liabilities.

Policy Statement

TKH employees, contractors, vendors, and agents with remote access permissions are obliged to ensure that their remote connection is as secure as their on-site connection. Unrestricted access to the internet for personal use through TKH's network is strictly limited. Those accessing our network from personal devices bear the responsibility to prevent unauthorized access to TKH resources or data. Any unauthorized usage or illicit activities conducted through TKH's network is strictly prohibited. TKH's networks should not be used to access the Internet for external business interests.

Procedures

1. *Connection Procedures*: Secure remote access should be established using TKH's Virtual Private Networks (VPNs) with encryption and strong pass-phrases. Users are expected to safeguard their login credentials, even from family members. TKH-owned devices used for remote connection should not be connected to any other network simultaneously, except personal networks under users' complete control. Usage of external resources for TKH business must be pre-approved by the relevant manager.
2. *Compliance*: TKH's IT team will periodically check compliance with this policy via various methods such as walk-throughs, video monitoring (if applicable), business tool reports, and internal and external audits. Policy violations may result in disciplinary action, including potential termination of employment.
3. *Employee Training and Awareness*: TKH will provide regular training sessions about this Remote Work Policy, educate employees about potential risks and threats associated with remote work, and encourage immediate reporting of any security concerns or incidents to the IT department.
4. *Locking Devices When Not in Use*: To prevent unauthorized access, users should always lock their devices when not in use and set devices to automatically lock after a certain period of inactivity.
5. *Secure Home Networks*: Given that home networks have become a part of our organization's security perimeter, we request employees to secure their Wi-Fi network with a strong, unique password, use the highest level of encryption available, regularly update and patch their router's firmware, and disconnect devices not in active use from their home network.
6. *Use of Virtual Private Networks (VPNs)*: To ensure a secure connection to TKH's resources, a VPN should be used when accessing TKH's network remotely. Only VPN solutions approved and provided by TKH should be used.

Compliance with this Remote Work Policy is essential for maintaining the security of TKH's data and systems. It is the collective responsibility of every employee, contractor, vendor, and agent of TKH to abide by these guidelines. This joint effort will contribute to TKH's continued success while creating a safe and secure digital environment.