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.

Incident Reporting and Response

At The Knowledge House, we understand the significant risks that cybersecurity incidents pose to our operations, reputation, and the data of our stakeholders and employees. This policy is designed to provide explicit steps for reporting and responding to a potential cybersecurity incident. This policy will define what constitutes a data and cybersecurity incident and lay out the responsibilities and procedures that all TKH employees must abide by to prevent, identify, report, and respond to these incidents.

Policy Statement

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

Definitions

1. Cybersecurity Incident: An event that could negatively impact the confidentiality, integrity, or availability of TKH's systems, networks, applications, or data. This includes, but is not limited to, data breaches, unauthorized access or disclosure of data, malware infections, and denial of service attacks.
2. Incident Response Team (IRT): A group consisting of staff, advisors, and service providers that coordinates incident responses. The IRT includes individuals with specific roles and responsibilities.
3. Incident Response Manager (IRM): A member of the IRT responsible for organizing and coordinating the response during an incident.

Procedures

1. *Identification*: The first step is for employees to identify any unusual or suspicious activities on their devices or within the organization's network. This could include but is not limited to, unexpected system behavior, unusual network traffic, unauthorized account activity, or unexpected data modifications. Employees should be familiar with the normal operations of their systems to detect abnormal situations.
2. *Immediate Reporting*: As soon as an incident is identified, it should be reported immediately. Employees should be aware of the reporting procedure in the organization, which typically involves notifying their immediate supervisor or the IT department. The report should contain as much detail as possible, including what was observed, when it was noticed, and any other relevant information.
3. *Preserve Evidence*: If possible, employees should take steps to preserve any evidence related to the incident. This could involve taking a screenshot of the unusual activity, noting down any error messages, or retaining logs if available. This can be of significant help to the Incident Response Team (IRT) in their investigation and mitigation process.
4. *Avoid Independent Actions*: Employees should not attempt to investigate or mitigate the incident on their own unless they are part of the IRT. Untrained personnel may unintentionally disrupt or destroy crucial evidence or exacerbate the situation.

5. *Cooperation with the IRT*: Once the incident is reported, employees should fully cooperate with the IRT. This may involve providing further information about the incident, participating in interviews, or handing over affected devices for examination.
6. *Post-Incident Follow-Up*: After the incident has been handled, employees may be required to participate in post-incident activities. This can involve reviewing and understanding any changes to policies or procedures, implementing new security measures, or participating in training and awareness sessions.

The cybersecurity of TKH is everyone's responsibility. By adhering to this policy, all members contribute to the safety and security of our data, infrastructure, and reputation. By regularly monitoring systems, promptly reporting potential security incidents, and participating in remediation and recovery efforts when necessary, we can collectively safeguard TKH against cyber threats. Your commitment to this policy ensures that TKH can continue to fulfill its mission without unnecessary disruption.

Data Handling and Classification Policies & Procedures

As a nonprofit organization committed to providing tuition and debt-free technology courses to low-income students, we handle a vast amount of sensitive data. This ranges from donor information, student personal details, to online payment information. Ensuring the trust of our students, donors, and partners is paramount to us. We understand the need to protect this data meticulously. The Data Classification and Handling Policy serves as our guiding framework to ensure this protection. It sets clear guidelines for handling, storing, and transmitting different types of data. But remember, this policy is not solely about security - it's also about demonstrating respect for individuals' privacy and compliance with applicable laws and regulations.

Definitions

1. Public Data: Information that can be freely shared, within and outside the organization, without any encryption. Examples include our course descriptions, public event details, and research publications.
2. Internal Data: Information that should be shared only on a need-to-know basis, even within the organization. It requires basic security measures like password protection for storage and should ideally be sent via secure, authenticated channels. Examples include administrative details, internal communications, and operational schedules.
3. Confidential Data: Data that can only be accessed by authorized individuals and is shared strictly on a need-to-know basis. It requires strong security measures, such as encryption for storage and transmission through secure, authenticated, and encrypted channels. Examples include personal details of students and donors, and proprietary research data.
4. Sensitive Data: Information that should only be accessed by specifically authorized personnel and is never shared unless required by law enforcement. This type of data must be stored in encrypted form and transmitted only over secure, authenticated, and encrypted channels. Examples include credit card numbers, bank details, and Social Security Numbers of students and donors.

Data Handling and Classification Procedures

1. *Public Data*: Public data should be used to inform the public about our programs, events, and research findings. It can be freely shared with any interested party without restrictions, as long as the data's integrity and accuracy are maintained. Before public data is shared or published, it should be reviewed for accuracy and relevance by the appropriate personnel or department. It can be distributed through various channels such as the organization's website, social media platforms, press releases, and public reports. All data should be reviewed and updated regularly to ensure it remains current and relevant.
2. *Internal Data*: Internal data should only be used for organization-related activities and decision-making processes. It should be shared only with authorized employees who need the data to fulfill their job responsibilities. Each employee should have access only to the internal data that they need for their role. Use of personal storage devices or non-secure cloud storage for storing internal data should be prohibited. Any suspected or actual breach involving internal data should be promptly reported to the organization's designated security officer or team.
3. *Confidential Data*: Confidential data must be protected with strong security measures. It should be stored only in secure systems with stringent access controls and should be encrypted during transmission. Employees are expected to protect confidential data at all times, including outside of working hours and off-premises.
4. *Personal Data*: Personal data should be handled in compliance with the relevant privacy laws and regulations such as the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), and others applicable in our operating areas. Any sharing of this information should be done in accordance with the law, ensuring the explicit consent of the individual concerned.
5. *Sensitive Data*: Sensitive data should be stored only in systems with the highest level of security measures, including end-to-end encryption. Transmission of sensitive data should also be encrypted and use secure, authenticated channels. A secure disposal or deletion process should be followed once this data is no longer needed. If an employee suspects a security breach involving sensitive data, they should immediately report it to the security team. Our organization will then follow the procedures outlined in the Data Breach Response Plan, which includes notifying the affected individuals and taking corrective actions to prevent such incidents in the future.
6. *Compliance, Audit, and Training*: All employees are expected to comply with this policy. Regular audits will be conducted to ensure compliance and identify areas of potential improvement. We will provide training to all employees on data handling procedures and best practices. This training will also cover the legal obligations related to data privacy and protection, helping our employees understand the importance of these practices and their role in maintaining the organization's credibility and reputation.
7. *Policy Violation and Disciplinary Action*: Violation of this policy may result in disciplinary action, including termination of employment. Any unlawful action can also result in legal action against the individual. If an employee discovers a possible violation, they should

report it to their supervisor or the security team immediately. All reports will be treated confidentially, and the reporter will be protected from retaliation.

We share the responsibility of understanding and adhering to this policy, irrespective of our roles within the organization. In our commitment to helping you understand these guidelines, we will provide training and support as needed. By adhering to this policy, we uphold our commitment to our students, donors, and the wider community, fostering a secure and trustworthy environment for all.

Thank you for taking the time to familiarize yourself with this Technology Policies and Procedures manual. Adherence to the policies outlined are essential for maintaining the integrity and security of our systems, data, and resources. Your cooperation in this endeavor plays a crucial role in fostering a secure environment, thus contributing to the resilience and ongoing success of our organization. Remember, the protection of our digital assets is a shared responsibility, and your commitment to following these policies and procedures is highly valued. Let's work together in ensuring the security of our digital environment and the fulfillment of our mission.

References

Federal Trade Commission. (2020). Tips for using public Wi-Fi networks. FTC Consumer Information. https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks

Federal Trade Commission. (2023). Protecting Personal Information: A Guide for Business. Retrieved June 4, 2023, from https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

KeePass. (2022). KeePass password safe. KeePass. https://keepass.info/

LastPass. (2021). LastPass remote work resource center. LastPass. https://www.lastpass.com/resources/remote-work-resource-center

LastPass. (2023). How to create a secure password. Retrieved June 4, 2023, from https://www.lastpass.com/password-generator

Microsoft. (2022). Protect your organization with security policies. Microsoft 365 Security. https://docs.microsoft.com/en-us/microsoft-365/security/mtp/security-policies?view=o365-worldwide

National Cybersecurity Centre. (2023). Password guidance: Simplifying your approach. Retrieved June 4, 2023, from https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

National Institute of Standards and Technology. (2012). Guide to test, training, and exercise programs for IT plans and capabilities. NIST Special Publication 800-84. https://csrc.nist.gov/publications/detail/sp/800-84/final

National Institute of Standards and Technology. (2013). Computer Security Incident Handling Guide. NIST Special Publication 800-61. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

National Institute of Standards and Technology. (2013). Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53). Gaithersburg, MD: NIST.

National Institute of Standards and Technology. (2017). Digital Identity Guidelines: Passwords and Authentication (NIST Special Publication 800-63B). https://doi.org/10.6028/NIST.SP.800-63b

National Institute of Standards and Technology. (2020). Guide to enterprise telework, remote access, and bring your own device (BYOD) security (Special Publication 800-46 Rev. 2). https://doi.org/10.6028/NIST.SP.800-46r2

New York State. (2019). Stop Hacks and Improve Electronic Data Security Act (SHIELD Act). Albany, NY: New York State Legislature.

New York State Department of State. (n.d.). Cyber security tips for small businesses. https://dos.ny.gov/cyber-security-tips-small-businesses

New York State Department of State, Division of Consumer Protection. (2023). Cybersecurity Information and Resources. Retrieved June 4, 2023, from https://www.dos.ny.gov/consumerprotection/cybersecurity/

SANS Institute. (2014). SANS Security Policy Resource. Retrieved from https://www.sans.org/security-resources/policies

SANS Institute. (2020). The importance of security awareness training. SANS Institute InfoSec Reading Room.

https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-38378
SANS Institute. (2021). Handling an Incident.
https://www.sans.org/security-resources/idfaq/incident.php
SANS Institute. (2021). Incident Response: Step-by-Step Guide.
https://www.sans.org/blog/incident-response-a-step-by-step-guide/
Sherwood, J. (2013). Information assurance handbook: Effective computer security and risk management strategies. McGraw Hill Professional.
Tipton, H. F., & Krause, M. (2007). Information Security Management Handbook. Auerbach Publications.
Viega, J., & Messier, M. (2002). Secure Programming Cookbook for C and C++. O'Reilly Media.
Winkler, I. S. (2011). Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies. Syngress.

Secure Program Capstone 2023
Author: Jane Pierre and Elizabeth Bond
Contributors: Mishelly Sandoval, Lucas Higgs, Shamar Brown, Tianna Green, Frederick Asante, Jonathan Henao and Aaron Kaah