KINDCODY Information Security Policy

KINDCODY

APRIL 2021

Contents

Preface

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential KINDCODY information and must be distributed to all KINDCODY employees. All KINDCODY staff must read Part 1 of this document and sign the form confirming they have read and understand this policy fully.

Any individuals (including external contractors) involved in information technology support must read Parts 1 & 2 of this policy and sign the form confirming they have read and understand this policy fully.

2. Policy review and update

This document will be reviewed and updated by KINDCODY management on an annual basis or when relevant to include newly developed security standards or regulations into the policy.

All changes must be agreed with the KINDCODY ICF Finance and General-Purpose Committee and then disseminated to all employees, interns and contractors.

Part I: Staff information security policies

1. Information Security Policy

KINDCODY handles sensitive information daily. Sensitive information must have adequate safeguards in place to protect them, to protect privacy, to ensure compliance with the law, regulations and to guard the future of the charity.

KINDCODY commits to respecting the privacy of all its donors, recipients, staff and outside parties - to this end, management is committed to maintaining a secure environment in which to process information.

Employees handling sensitive information should:

- Ensure KINDCODY information is handled in a manner that fits with its sensitivity.
- Limit personal use of KINDCODY information and telecommunication systems and ensure it doesn't interfere with your job performance.
- Understand that KINDCODY reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose.
- Not use e-mail, internet and other KINDCODY resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal.
- Not disclose personnel information unless authorised.
- Protect sensitive information.
- Keep passwords and accounts secure.
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.
- Not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval.
- Always leave desks clear of sensitive documents and lock computer screens when unattended.

- Report information security incidents without delay to the individual responsible for incident response locally.

We each have a responsibility for ensuring that KINDCODY's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

2. Roles and Responsibilities

Information Security Officer (or equivalent) is responsible for overseeing all aspects of information security, including but not limited to:

- Creating and distributing security policies and procedures.
- Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel.
- Creating and distributing security incident response and escalation procedures that include maintaining a formal security awareness program for all employees that provide multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings).

The Information Technology Support provider (or equivalent) shall maintain daily administrative and technical operational security procedures that are effective (for example, user account maintenance procedures, and log review procedures):

- Monitor and analyse security alerts and information and distribute to appropriate personnel.
- Administer user accounts and manage authentication.
- Monitor and control all access to data.
- Maintain a list of service providers.
- Ensure there is a process for engaging service providers including proper due diligence prior to engagement.
- Maintain a program to verify service providers' -KINDCODY Information Security Policy compliant status, with supporting documentation.

The Chief of Staff (or equivalent) is responsible for tracking employee participation in the security awareness program, including:

- Facilitating participation upon hire and at least annually.

- Ensuring that employees acknowledge in writing at least annually that they have read and understand KINDCODY's information security policy.

The Treasurer (or equivalent) will ensure that for service providers with whom information is shared:

- Written contracts require adherence to the KINDCODY Information Security Policy by the service provider.
- Written contracts include acknowledgement or responsibility for the security of data by the service provider.

3. Security Awareness and Procedures

The policies in this document must be incorporated into KINDCODY working practices and disseminated to maintain a high level of security awareness. The protection of sensitive information demands regular training of all employees and contractors. The Information Security Officer will:

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day KINDCODY practice.
- Distribute this security policy document to all KINDCODY employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- Ensure all employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with KINDCODY.
- Ensure KINDCODY security policies are reviewed annually and updated as needed.

4. Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to KINDCODY's established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and KINDCODY from illegal or damaging actions by individuals, either knowingly or unknowingly.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorised access to confidential data.
- Employees should ensure that technologies should be used and setup in acceptable network locations.
- Keep passwords secure and do not share accounts unless requested to do so.
- Authorised users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All Point of Sales and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from an KINDCODY email address to external websites should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of KINDCODY, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

KINDCODY will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

5. Safeguarding Passwords

All users, including staff, contractors, interns and donors with access to KINDCODY systems, are responsible for ensuring that passwords are not shared and that passwords are not written down

The responsibility for selecting a password that is hard to guess generally falls to users. A strong password must:

- Be (never shorter than 8 characters).
- Include mixed-case letters.
- Include digits and punctuation marks.
- Not be based on any personal information.

Any exceptions must be agreed with the Chief of Staff and documented.

6. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee or intern will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment may not be used as excuses for non-compliance.

7. Protect Stored Data

All sensitive information stored and handled by KINDCODY and its employees must be securely always protected against unauthorised use, loss or damage:

- Any sensitive information that is no longer required by KINDCODY for business reasons must be discarded in a secure and irrecoverable manner.
- The integrity of storage media should be validated on a regular basis.
- Storage media must not be used past its expected lifespan.
- Off-site backups of KINDCODY information must be taken daily. Tests of backup media must be carried out on a regular basis.
- In the event of a loss of the KINDCODY server, recovery procedures must be able to reinstate data from a backup onto a new server within 72 hours.

KINDCODY personnel must not store:

- The PIN or CVV/CVC (the 3- or 4-digit number on the signature panel on the reverse of KINDCODY payment cards) on any media.

8. Information Classification

Data and media containing sensitive information must always be labelled "Confidential":

- Sensitive data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to KINDCODY or third parties if disclosed or modified or lost.

Data and media containing non- sensitive information may be labelled:

- "Internal Use" data might include information that the data owner feels should be protected to prevent unauthorised disclosure.
- "Public" data is information that may be freely disseminated.

Documents prepared for external consumption must contain KINDCODY's full name, address, registration number and a copyright statement that protects KINDCODY's intellectual property.

9. Access to sensitive information

All access to sensitive information must be controlled and authorised:

- Any job function that requires access to sensitive information should be clearly defined.
- Access rights to privileged user ID's should be restricted to least privileges necessary to perform job responsibilities.
- Privileges should be assigned to individuals based on job classification and function.
- Access to sensitive information, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need – to be determined by KINDCODY management.

10. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive information.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should take all necessary steps to prevent unauthorised access to confidential data.
- Employees should ensure that technologies should be used and setup in acceptable network locations.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive information. (A "visitor" is defined as a donor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day).
- Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, USB drives, back-up media, computer hard drive, etc.
- Media containing sensitive information must be handled and distributed in a secure manner by trusted individuals.
- Sensitive documents must be stored securely when not in use.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on KINDCODY sites. A "visitor" is defined as a donor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Strict control is maintained over the storage and accessibility of media.
- All computers on which sensitive information is stored must have a password protected screensaver enabled to prevent unauthorised use.

11. Protect Data in Transit

All sensitive information in transit must be protected securely if it is to be transported physically or electronically:

- If there is a business justification to send sensitive information via email or via the internet or any other modes then it should be done after authorization and password protected or encrypted as appropriate.
- The transportation of media containing sensitive information to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

12. Wireless Use Policy

- KINDCODY staff may use mobile devices (mobile phones, iPads, etc) to access the KINDCODY network providing that the use of KINDCODY's systems and network complies with this information Security Policy.
- The unauthorised installation or use of any wireless device or wireless network intended to be used to connect to any of the KINDCODY networks or environments is prohibited.

13. Remote Access policy

It is the responsibility of KINDCODY employees, contractors, vendors and agents with remote access privileges to KINDCODY's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to KINDCODY.

14. Archival of Stored Data

Since 2009, all final copies of KINDCODY electronic records have been stored on the KINDCODY server. This server is used for both active and archived electronic records. Paper-based records are archived externally:

- All final copies of electronic documents prepared in relation to KINDCODY's activities will be stored on KINDCODY servers. Duplicate copies of such documents held on workstations should be deleted.
- Email servers for individuals that leave KINDCODY will be retained. Access to these archives will be provided on the basis on need and subject to authorisation from the KINDCODY management team.
- Hard copies of signed contracts and other legal documents will be retained.
- Other paper records will be kept for as long as is required by statute or regulation.
- Soft copies of important documents must be made and stored on the KINDCODY server in an appropriate location.
- Paper records to be archived are to be stored off-site in a secure location.

15. Disposal of Stored Data

The disposal of stored data must be subject to appropriate levels of security to prevent the disclosure of sensitive information to third parties:

- All data must be securely disposed of when no longer required by KINDCODY, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of data must be manually destroyed as when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non- electronic data has been appropriately disposed of in a timely manner.
- All hardcopy materials containing sensitive information that are no longer needed by KINDCODY must be crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- All data on electronic media that is no longer required by KINDCODY must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military-grade secure deletion processes or the physical destruction of the media.
- If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.

- All information awaiting destruction must be held in lockable storage containers clearly marked "To Be Destroyed". Access to these containers must be restricted.

Part 2 – IT support information security policies

16. Password Standards

A password, sometimes called a passcode, is a memorized secret used to confirm the identity of a user. Passwords provide a means for controlling access to KINDCODY's information systems to authorised persons only.

The easier a password is for the owner to remember generally means it will be easier for an attacker to guess. However, passwords that are difficult to remember may also reduce the security of a system because (a) users might need to write down or electronically store the password, (b) users will need frequent password resets and (c) users are more likely to re-use the same password across different accounts.

Information systems support personnel responsible for configuring KINDCODY systems, are must take steps as outlined below, that allow users to select and secure their passwords:

- A system configuration standard must be developed along industry acceptable hardening standards (SANS, NIST, ISO)
- System configurations should be updated as new issues are identified.
- System configurations must include common security parameter settings.
- The systems configuration standard should be applied to any news systems configured.
- All vendor default accounts and passwords for the systems must be changed at the time of provisioning the system/device into KINDCODY network and all unnecessary services and user/system accounts must be disabled.
- All unnecessary default accounts must be removed or disabled before installing a system on the network.
- Security parameter settings must be set appropriately on system components.
- All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.) must be removed.
- All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system.

- Any insecure protocols, daemons, services in use must be documented and justified.
- All user must use a password to access KINDCODY network or any other electronic resources.
- All user ID's for terminated users must be deactivated or removed immediately.
- The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account.
- All system and user level passwords must be changed on at least a quarterly basis.
- A minimum password history of four must be implemented.
- A unique password must be setup for new users and the users prompted to change the password on first login.
- Group, shared or generic user account or password or other authentication methods must not be used to administer any system components.
- System services and parameters will be configured to prevent the use of insecure technologies like File Transfer Protocol (FTP) and other remote login tools.
- Administrator access to web-based management interfaces is encrypted using strong cryptography.
- If an operating system without security features is used (such as DOS, Windows or MacOS), then an intruder only needs temporary physical access to the console to insert a keyboard monitor program. If the workstation is not physically secured, then an intruder can reboot even a secure operating system, restart the workstation from his own media, and insert the offending program.
- To protect against network analysis attacks, both workstation and server should be cryptographically secured. Examples of strong protocols are the encrypted Netware login and Kerberos.

17. Anti-virus policy

All machines must be configured to run the latest anti-virus software as approved by KINDCODY. The preferred application to use is the Managed Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically daily. The antivirus should have periodic scanning enabled for all the

systems.

- The antivirus software in use should be capable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits).
- All removable media (for example: USB drives) should be scanned for viruses before being used.
- All the logs generated from the antivirus solutions must be retained as per legal/regulatory/contractual requirements.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans.
- Users must not be able to modify and any settings or alter the antivirus software.
- E-mail with attachments coming from suspicious or unknown sources should not be opened.
- All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail that they suspect may contain virus.

18. Network security

KINDCODY's telecommunications network provides access to network services outside of KINDCODY (e.g. the internet) and within KINDCODY (e.g. within and between KINDCODY offices). Information transmitted or received by KINDCODY across these networks must be subject to appropriate levels of security:

- Firewalls must be implemented at each internet connection and any "Demilitarized Zone" (DMZ) and the internal KINDCODY network.
- A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every six months.
- A firewall and router configuration document must be maintained that includes a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the card holder data environment.
- All inbound network traffic must be blocked by default, unless explicitly allowed and the restrictions must be documented.

- All outbound traffic must be authorized by management (i.e. what are the red listed category of sites that cannot be visited by the employees) and the restrictions must be documented
- KINDCODY will have firewalls between any wireless networks and the data environment.
- KINDCODY will quarantine wireless users into a DMZ, where they will be authenticated and fire walled as if they were coming in from the Internet.
- Disclosure of private IP addresses to external entities must be authorised.
- A topology of the firewall environment must be documented and must be updated in accordance to the changes in the network.
- The firewall rules will be reviewed on a six months basis to ensure validity and the firewall must have clean up rule at the bottom of the rule base.
- KINDCODY must quarantine wireless users into a DMZ, where they were authenticated any fire walled as if they were coming in from the Internet.
- No direct connections from Internet to KINDCODY data environment will be permitted. All traffic must traverse through a firewall.

19. Patch Management Policy

All laptops, desktops, workstations, servers, software, system components etc. owned by KINDCODY must have up-to-date system security patches installed to protect the asset from known vulnerabilities:

- The IT support team must ensure that wherever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors.
- Security patches must be installed within one month of release from the respective vendor and must follow the process in accordance with change control process.
- Any exceptions to this process must be documented.

20. Remote Access Set up

Secure remote access must be strictly controlled. Control will be enforced by two-factor authentication via one-time password authentication or public/private keys with strong pass- phrases:

- Donor accounts with access to KINDCODY network will only be enabled during the time period. the access is required and will be disabled or removed once access is no longer required.
- Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity.
- All hosts that are connected to KINDCODY internal networks via remote access technologies will be monitored on a regular basis.
- All remote access accounts used by donors or 3rd parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification.

21. Vulnerability Management Policy

- All the vulnerabilities to be assigned a risk ranking such as High, Medium and Low based on industry best practices.
- KINDCODY will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- Quarterly internal vulnerability scans must be performed by KINDCODY by internal staff or a 3rd party vendor and the scan process must include that rescans will be done until passing results are obtained, or all High vulnerabilities are resolved.
- Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor. Scans conducted after network changes may be performed by KINDCODY's internal staff. The scan process should include re-scans until passing results are obtained.

22. Configuration standards:

All network device configurations must adhere to KINDCODY required standards before being placed on the network as specified in the KINDCODY configuration guide. Using this guide, a boilerplate configuration has been created that will be applied to all network devices before being placed on the network:

- Before being deployed into production, a system must be certified to meet the applicable configuration standard.
- Updates to network device operating system and/or configuration settings that fall under the KINDCODY standards as defined by the Information security Office. Updates must be applied within the time frame identified by the Information security Office.
- Administrators of network devices that do not adhere to KINDCODY standards (as identified via a previous exception) must document and follow a review process of announced vendor updates to operating system and/or configuration settings. This process must include a review schedule, risk analysis method and update method.
- All network device configurations must be checked annually against the configuration boilerplate to ensure the configuration continues to meet required standards. Where possible, network configuration management software will be used to automate the process of confirming adherence to the boilerplate configuration.
- For other devices an audit will be performed quarterly to compare the boilerplate configuration to the configuration currently in place.
- All discrepancies will be evaluated and remediated by Network Administration.

23. Change control Process

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, released in a controlled manner and that the status of each proposed change is monitored:

- The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical KINDCODY information resources (such as hardware, software, system documentation and

operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.

- All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented. A documented audit trail, containing relevant information shall always be maintained. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.
- A risk assessment shall be performed for all changes and dependant on the outcome, an impact assessment should be performed. The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.
- All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.
- Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.
- Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.
- All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user; the impact assessment was performed and proposed changes were tested.
- All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.
- Implementation will only be undertaken after appropriate testing and approval by stakeholders.
- All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.

- Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert to what they were prior to implementation of changes.
- Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.
- Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.
- All changes will be monitored once they have been rolled-out to the production environment.
- Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

24. Audit and Log review

- This procedure covers all logs generated for systems within the data environment, based on the flow of data over KINDCODY network, including the following components:

    - Operating System Logs (Event Logs and SU logs).
    - Database Audit Logs.
    - Firewalls & Network Switch Logs.
    - IDS Logs.
    - Antivirus Logs.
    - CCTV Video recordings.
    - File integrity monitoring system logs.

- Audit Logs must be maintained for a minimum of 3 months online (available for immediate analysis) and 12 months offline.

- Review of logs is to be carried out by means of KINDCODY's network monitoring system (KINDCODY to define hostname), which is controlled from KINDCODY console (KINDCODY to define hostname). The console is installed on the server (KINDCODY to define hostname / IP address), located within KINDCODY data centre environment.
- The following personnel are the only people permitted to access log files (KINDCODY to define which individuals have a job-related need to view audit trails and access log files).
- The network monitoring system software (KINDCODY to define) is configured to alert the KINDCODY Information Security Officer to any conditions deemed to be potentially suspicious, for further investigation. Alerts are configured to:
    - A dashboard browser-based interface monitored by the KINDCODY Information Security Officer.
    - Email / SMS alerts to KINDCODY mailbox with a summary of the incident. KINDCODY Information Security Officer also receives details of email alerts for informational purposes.
- The following Operating System Events are configured for logging, and are monitored by the console (KINDCODY to define hostname):
    - Any additions, modifications or deletions of user accounts.
    - Any failed or unauthorised attempt at user logon.
    - Any modification to system files.
    - Any access to the server, or application running on the server, including files that hold data.
- Actions taken by any individual with root or administrative privileges.
- Any user access to audit trails.
- Any creation / deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system).

The following Database System Events are configured for logging, and monitoring (KINDCODY to define software and hostname):

- Any failed user access attempts to log in to the SQL database.
- Any login that has been added or removed as a database user to a database.
- Any login that has been added or removed from a role.
- Any database role that has been added or removed from a database.
- Any password that has been changed for an application role.
- Any database that has been created, altered, or dropped.
- Any database object, such as a schema, that has been connected to.
- Actions taken by any individual with DBA privileges.

The following Firewall Events are configured for logging, and are monitored by the network monitoring system (KINDCODY to define software and hostname):

- Access Control List (ACL) violations.
- Invalid user authentication attempts.
- Log-on and actions taken by any individual using privileged accounts.
- Configuration changes made to the firewall (e.g. policies disabled, added, deleted, or modified).

The following Switch Events are to be configured for logging and monitored by the network monitoring system (KINDCODY to define software and hostname):

- Invalid user authentication attempts.
- Logon and actions taken by any individual using privileged accounts.
- Configuration changes made to the switch (e.g. configuration disabled, added, deleted, or modified).

The following Intrusion Detection Events are to be configured for logging, and are monitored by the network monitoring system (KINDCODY to define software and hostname):

- Any vulnerability listed in the Common Vulnerability Entry (CVE) database.
- Any generic attack(s) not listed in CVE.
- Any known denial of service attack(s).
- Any traffic patterns that indicated pre-attack reconnaissance occurred.
- Any attempts to exploit security-related configuration errors.
- Any authentication failure(s) that might indicate an attack.
- Any traffic to or from a back-door program.
- Any traffic typical of known stealth attacks.

The following File Integrity Events are to be configured for logging and monitored by (KINDCODY to define software and hostname):

- Any modification to system files.
- Actions taken by any individual with administrative privileges.
- Any user access to audit trails.
- Any creation / deletion of system-level objects installed by Windows. (Almost all system- level objects run with administrator privileges, and some can be abused to gain administrator access to a system).

For any suspicious event confirmed, the following must be recorded and KINDCODY Information Security Officer informed by email:

- User Identification.
- Event Type.
- Date & Time.
- Success or Failure indication.
- Event Origination (e.g. IP address).
- Reference to the data, system component or resource affected.

25. Incident Response Plan

'Security incident' means any incident (accidental, intentional or deliberate) relating to KINDCODY's communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee. Their intention might be to steal information or money, or just to damage KINDCODY.

The incident response plan must be tested once annually. Copies of this incident response plan are to be made available to all relevant staff members, who must take steps to ensure that they understand it and what is expected of them.

Employees of KINDCODY will be expected to report to the Information Security Officer any security related issues. KINDCODY security incident response plan is as follows:

- Each employee must report an incident to the Information Security Officer (preferably) or to another member of the Response Team.
- That member of the team receiving the report will advise the Response Team of the incident.
- The Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of data and in mitigating the risks associated with the incident.
- The Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties as necessary.
- The Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.
- If an unauthorised wireless access point or devices is identified or detected as part of the quarterly test this is should be immediately escalated to the Information Security officer or someone with similar privileges who has the authority to stop, cease, shut down, and remove the offending device immediately.
- Anyone who reasonably believes there may have been an account breach, or a breach of information or of systems related to the environment in general, must inform the KINDCODY Incident Response Team. After being notified of a

compromise, the Response Team, along with other designated staff, will implement the Incident Response Plan to assist and augment KINDCODY's response.

KINDCODY Security Incident Response Team: (Update as applicable)

- Chief of Staff.
- Treasurer.
- IT advisor.
- Legal Counsel (if needed).

Incident Response Notification:

- Director of KINDCODY Communications.
- Escalation – Trustees.

26. User Access Management

Access Controls are used to manage access to KINDCODY information and systems:

- Access to KINDCODY information systems is controlled through a formal user registration process beginning with a formal notification from the Chief of Staff.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorised by HR/line management.
- The job function of the user decides the level of access the employee has to data.
- A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

    - Name of person making request.
    - Job title of the newcomer(s) and start date.

- Services required (default services are: MS Outlook, MS Office and Internet access).

- Each user will be given a copy of their new user form to provide a written statement of their access rights signed by an IT representative after their induction procedure. The user must sign the form to indicate that they understand the conditions of access.
- Access to all KINDCODY systems is provided by the Information Security Officer and can only be started after proper procedures are completed.
- As soon as an individual leaves KINDCODY employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process the Chief of Staff will inform the Information Security Officer of all leavers and their date of leaving.

27. Access Control Policy

Access Control systems are in place to protect the interests of all users of KINDCODY information systems by providing a safe, secure and readily accessible environment in which to work:

- KINDCODY will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorisation provided jointly by the system owner and IT Services. The Chief of Staff shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of sensitive information even if technical security mechanisms fail or are absent.

- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
- Users are obligated to report instances of non-compliance to the KINDCODY Information Security Officer.
- Access to KINDCODY information resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any KINDCODY information resources and services will be provided without prior authentication and authorisation of a user's KINDCODY Windows Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Minimum password length, complexity and expiration times will be often be controlled using user account management set up parameters.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by KINDCODY policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights.

28. Wireless Set Up Policy

If the need arises to use wireless technology, it should be approved by KINDCODY and the following wireless standards must be adhered to:

- Default passwords, passphrases, encryption keys/security related vendor defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves KINDCODY.
- The firmware on the wireless devices must be updated accordingly as per vendors release schedule.
- The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
- Any other security related wireless vendor defaults should be changed if applicable.
- Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission of data.
- A quarterly test should be run to discover any unauthorised wireless access points connected to the KINDCODY network.
- Usage of appropriate testing using tools like net stumbler, kismet, etc. must be performed on a quarterly basis to ensure that any devices that support wireless communication remain disabled or decommissioned.
- If any violation of the Wireless Policy is discovered as a result of the normal audit processes, the Information Security Officer has the authorisation to stop, cease, shut down, and remove the offending device immediately.
- An Inventory of authorised access points along with a business justification must be maintained. (Update Appendix B).

Part 3 – Authority

1. Entry into Force

This policy has been reviewed and approved by the KINDCODY Finance and General-Purpose Committee and is effective immediately.

This policy is to be subject to an annual review and update.

Policy approved by:

KINDCODY DIRECTORS

Represented by the Chief Operating Officer, Chris Frost

August 2019

Appendix A – Agreement to Comply with Information Security Policies

_____

Employee Name (printed)

_____

Department

I agree to take all reasonable precautions to assure that KINDCODY internal information, or information that has been entrusted to KINDCODY by third parties such as donors, will not be disclosed to unauthorised persons. At the end of my employment or contract with KINDCODY, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Chief of Staff or the Treasurer who are the designated information owners.

I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the KINDCODY security policy that are relevant to me (Part 1: Staff Information Security Policies). I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the designated Information Security Officer.

_____

Employee Signature

Appendix B - Inventory management

An inventory of all IT equipment and devices must be maintained. The inventory should contain the following information:

Asset/Device Name	Asset number	Description	Owner/Approved User	Location