Northern Kentucky Area Development District

Information Security Policy

Use and Protection of NKADD Technology and Data

Contents

1. Purpose 7
2. Scope 8
3. Definitions 10
4. Governance & Responsibilities 13
4.1 Board of Directors 13
4.2 Executive Director 13
4.3 IT Director 13
4.4 Senior Staff and Department Leadership 14
4.5 Employees and Authorized Users 14
4.6 Third-Party Vendors and Contractors 15
5. Acceptable Use Policy 16
5.1 General Use 16
5.2 Ownership and Monitoring 16
5.3 Appropriate Use 16
5.4 Prohibited Activities 16
5.5 Email and Communication Systems 17
5.6 Internet and Cloud Usage 17
5.7 Social Media 18
5.8 Mobile Devices and Remote Use 18
5.9 Personally Owned Devices (BYOD) 18
5.10 Enforcement 19
6. Access Control 20
6.1 User Accounts 20
6.2 Account Provisioning and Deprovisioning 20
6.3 Authentication Requirements 20
Password Requirements 20
Modern Authentication Methods 21
Credential Management 21

6.4 Multi-Factor Authentication (MFA) 21
6.5 Account Security and Monitoring 21
6.6 Access Reviews 22
6.7 Remote Access 22
7. Data Protection 24
7.1 Data Classification 24
7.2 Data Handling 24
7.3 Data Storage and Cloud Services 25
7.4 Data Transmission 25
7.5 Data Retention and Disposal 25
7.6 Portable Media and Devices 26
7.7 Personally Owned Devices (BYOD) 26
7.8 Data Backup and Recovery 26
8. Endpoint & Network Security 28
8.1 Endpoint Security 28
8.2 Patch Management 28
8.3 Device Security 28
8.4 Network Security 29
8.5 Remote Access Security 29
8.6 Software and Application Control 29
9. Remote Access & Telework 30
9.1 General Requirements 30
9.2 Secure Access Methods 30
9.3 Device Security for Remote Work 30
9.4 Network and Environment Security 31
9.5 Data Protection During Remote Work 31
9.6 Remote Work Equipment and Peripherals 31
9.7 Session Management 31
10. Encryption 33

10.1 General Requirements 33
10.2 Data in Transit 33
10.3 Data at Rest 33
10.4 Email and File Sharing 33
10.5 Encryption Management 34
11. Electronic Signatures 35
11.1 Approved Use 35
11.2 Email and Document Use 35
11.3 Integrity and Control 35
11.4 Legal and Compliance Considerations 36
12. Logging, Monitoring & Auditing 37
12.1 Logging Requirements 37
12.2 Monitoring Activities 37
12.3 Microsoft 365 and Cloud Monitoring 37
12.4 Log Retention 37
12.5 Auditing 38
12.6 Incident Support 38
13. Security Incident Response 39
13.1 Definition of an Incident 39
13.2 Reporting Requirements 39
13.3 Incident Response Activities 39
13.4 Communication and Escalation 40
13.5 Evidence Preservation 40
13.6 Coordination with the Incident Response Plan 40
13.7 Post-Incident Review 40
13.8 Cyber Insurance Coordination 40
14. Breach Notification 41
14.1 Definition of a Data Breach 42
14.2 Notification Requirements 42

14.3 Internal Reporting and Escalation 42
14.4 Investigation and Response 43
14.5 Documentation 43
15. Security Awareness & Training 44
15.1 General Requirements 44
15.2 Training Program 44
15.3 Phishing Simulations 44
15.4 Remedial Training 45
15.5 New User Training 45
15.6 Program Oversight 45
16. Vendor & Third-Party Security 46
16.1 Vendor Access and Responsibilities 46
16.2 Data Protection Requirements 46
16.3 Contracts and Agreements 46
16.4 Vendor Risk Management 46
16.5 Incident and Breach Reporting 47
16.6 Termination of Access 47
17. Policy Enforcement 48
17.1 Enforcement Authority 48
17.2 Violations 48
17.3 Disciplinary Actions 48
17.4 Legal and Regulatory Consequences 49
18. Review & Maintenance 50
18.1 Policy Review 50
18.2 Policy Updates 50
18.3 Responsibility for Maintenance 50
18.4 Continuous Improvement 50
Approval and Governance 52
Monitoring and Administration 52

Review 52
Approval 52
Approval Record 52
Document Version Control 53
Revision History 53
Supersession 53

1. Purpose

The purpose of this Information Security Policy is to establish the requirements to protect NKADD information systems, technology resources, and data from unauthorized access, disclosure, modification, disruption, or destruction.

Information security supports NKADD's mission by enabling the secure and reliable delivery of services to local governments, partner organizations, and the communities NKADD serves.

This policy defines the minimum security requirements that employees, contractors, vendors, and other authorized users must follow when accessing or using NKADD technology resources, including networks, systems, devices, cloud services, applications, and data.

These requirements are intended to:

- Protect sensitive and confidential information, including Personally Identifiable Information (PII), Protected Health Information (PHI), financial information, and other critical data
- Reduce cybersecurity and operational risk
- Support the continuity and availability of business operations
- Ensure compliance with applicable laws, regulations, contracts, and grant requirements
- Promote a culture of shared responsibility for information security

NKADD reserves the right to monitor, log, and review the use of its technology resources at any time to ensure compliance with this policy, protect organizational assets, and support operational, security, legal, and regulatory requirements.

2. Scope

This policy applies to all Northern Kentucky Area Development District (NKADD) employees, contractors, consultants, temporary staff, volunteers, and any other individuals who are granted access to NKADD systems, technology resources, or data.

It applies to all information systems, applications, technology resources, and information assets owned or used by NKADD, including but not limited to:

- Desktop and laptop computers
- Mobile devices and tablets
- Servers and network infrastructure
- Applications, software platforms, email systems, and communication services
- Internet access and cloud-based services, including NKADD-approved platforms such as Microsoft 365 and other approved cloud or vendor-managed systems
- Removable media and portable storage devices
- Data stored, transmitted, processed, or archived in any format

This policy applies to all methods of access, including:

- On-site access within NKADD facilities
- Remote access from off-site locations
- Access through approved cloud platforms, mobile devices, or third-party systems

This policy also applies to NKADD data or information resources that are accessed, stored, processed, or transmitted on systems not directly owned by NKADD, including vendor-managed systems such as financial, accounting, human resources, or program-specific platforms, as well as approved personal devices.

Where NKADD data is shared with or managed by third parties, contractors, vendors, or partner organizations, those entities must maintain security practices consistent with applicable contractual, legal, and organizational requirements.

Where NKADD data or systems are subject to additional or more restrictive requirements under applicable grant agreements, contracts, program regulations, or state or federal law (including, but not limited to, HIPAA-covered program data), the more restrictive requirement applies in the event of a conflict with this policy.

This policy applies regardless of the technology platform or method used to process, store, or transmit NKADD information.

Where this policy and the NKADD Administrative Regulations address the same matter, both shall be followed, as provided in Section 18 of the Administrative Regulations.

Where this policy and the NKADD Personnel Policies address the same matter, both shall be followed, as provided in Chapter 1, Section 11 of the Personnel Policies.

3. Definitions

For the purposes of this policy, the following terms are defined as follows:

Access

The ability to view, use, modify, transmit, or otherwise interact with NKADD systems, applications, networks, or data.

Authorized User

Any employee, contractor, or individual who has been granted access to NKADD systems or data for approved business purposes.

Cloud Service

A technology service delivered over the internet, including software, storage, platforms, or infrastructure provided by third-party vendors.

Confidential Data

The highest tier of NKADD's data classification system (see Section 7.1), encompassing information such as personally identifiable information (PII), protected health information (PHI), financial data, and personnel records that requires the greatest level of protection from unauthorized access or disclosure.

Data Breach

The unauthorized acquisition, access, disclosure, alteration, loss, destruction, or use of sensitive, confidential, or regulated information.

Data Classification

The categorization of NKADD data as Public, Internal, or Confidential based on its level of sensitivity, as described in Section 7.1, used to determine appropriate handling, access, and protection requirements.

Electronic Signature

A digital representation of a signer's intent to approve or authenticate an electronic document or communication, applied using a secure signing method that provides identity verification and an auditable record of the signing event. A typed name, scanned image, or other unverified visual representation of a signature does not meet this definition and may be used only as approved under Section 11.1.

Endpoint

Any device that connects to NKADD systems or networks, including desktops, laptops, mobile devices, tablets, printers, and other network-connected equipment.

Information Security Incident (Incident)
Any event or activity that may compromise the confidentiality, integrity, or availability of NKADD systems or data. This includes malware infections, unauthorized access, data breaches, or suspicious system activity.

Least Privilege
A security principle requiring that users are granted only the minimum level of access necessary to perform their job functions.

Multi-Factor Authentication (MFA)
A security process that requires users to verify their identity using two or more authentication factors, such as a password and a mobile device verification.

NKADD Systems
All technology resources owned, managed, or approved by NKADD, including hardware, software, networks, cloud platforms, and vendor-managed systems.

Personally Identifiable Information (PII)
Information that can be used to identify or distinguish an individual, such as name, Social Security number, address, date of birth, or other identifying data.

Personally Owned Device (BYOD)
A smartphone, tablet, laptop, or other computing device owned by an employee or authorized user, rather than by NKADD, that is used to access NKADD systems, accounts, or data.

Protected Health Information (PHI)
Health-related information protected under applicable laws and regulations, including information that identifies an individual and relates to their health status, treatment, or payment for healthcare services.

Remote Access
Access to NKADD systems or data from outside NKADD facilities, using approved methods such as secure remote access tools or cloud-based platforms.

Removable / Portable Media
USB drives, external hard drives, SD cards, or other portable storage devices capable of storing or transferring data outside of NKADD's core systems.

Sensitive Information
Information that requires protection from unauthorized access, modification, disclosure, or destruction due to legal, regulatory, contractual, operational, or reputational considerations.

This term is used broadly throughout this policy to describe information warranting protective measures and includes, but is not limited to, Confidential Data as defined above.

Technology Resources

Hardware, software, networks, cloud services, applications, communication systems, and other technology assets used to conduct NKADD business.

User Account

A unique identifier assigned to an individual, service, or application that provides authorized access to NKADD systems or resources.

Vendor

Any third-party organization, contractor, service provider, consultant, or business partner that provides services to or processes information on behalf of NKADD.

4. Governance & Responsibilities

Information security at NKADD is a shared responsibility involving leadership, IT, and all users of NKADD systems. This section defines the roles and responsibilities needed to protect NKADD systems and data.

4.1 Board of Directors

The NKADD Board of Directors provides oversight of the organization and its information security program. This includes:

- Approving major policies, including the Information Security Policy
- Providing governance and accountability for organizational activities
- Supporting leadership in ensuring adequate resources for security and compliance

4.2 Executive Director

The Executive Director is responsible for the oversight of NKADD's information security program and serves as the primary point of accountability for information security operations. This includes:

- Enforcing information security policies and organizational standards
- Supporting the IT Director and ensuring adequate resources, authority, and organizational priority are given to implementing security controls
- Ensuring that information security aligns with organizational operations and priorities
- Communicating significant risks or incidents to the Board of Directors

4.3 IT Director

The IT Director (Director of IT and Facilities) is responsible for the implementation, operation, and oversight of NKADD's information security program.

The IT Director serves as the organization's primary authority on information security controls, standards, and practices and works in coordination with Senior Staff to ensure the consistent implementation of information security requirements across all departments. This includes:

- Maintaining and enforcing this policy
- Approving documented exceptions to this policy, consulting with the Executive Director on exceptions involving significant risk, sensitive data, or compliance implications
- Implementing technical safeguards and security controls
- Monitoring systems for security threats and activity
- Managing user access and system configurations
- Leading incident response and recovery efforts

- Providing security guidance and training
- Assessing and communicating information security risks to organizational leadership
- Establishing and enforcing security standards, controls, and technical requirements across NKADD systems and environments
- Providing direction and guidance to departments to ensure consistent implementation of security requirements

In the IT Director's absence, the IT Support Specialist shall assume interim responsibility for urgent security matters, including initiating immediate containment actions (such as isolating an affected device from the network). The IT Support Specialist shall promptly notify the Executive Director of the situation and shall coordinate with the Executive Director on any decision involving significant risk, legal exposure, or external notification. Policy exceptions during this period must be approved jointly by the IT Support Specialist and the Executive Director.

4.4 Senior Staff and Department Leadership

Senior Staff consists of the Executive Director, IT Director, Director of Finance and Administration, and Associate Directors. (The IT Director's specific information security duties are detailed in Section 4.3; this section reflects their broader role as part of organizational leadership.) These individuals are responsible for leading their respective areas and ensuring that information security requirements are implemented and followed within their areas and, as applicable, across the organization. This includes:

- Ensuring that staff follow information security policies and practices within their departments
- Approving and requesting appropriate system access based on job responsibilities
- Ensuring IT is notified of role changes, transfers, or employee departures in a timely manner
- Supporting and reinforcing security awareness and training efforts
- Ensuring that data within their areas is handled appropriately and protected according to policy requirements

The Director of Finance and Administration oversees Human Resources, which is typically responsible for coordinating human resources aspects of policy enforcement, including disciplinary actions referenced in Section 17.3.

4.5 Employees and Authorized Users

All users are responsible for protecting NKADD systems and data in their daily work. This includes:

- Following all policies and security requirements

- Using technology resources for approved business purposes
- Protecting login credentials and not sharing accounts
- Reporting suspicious activity or incidents immediately
- Handling sensitive data responsibly

4.6 Third-Party Vendors and Contractors

Vendors and contractors who access NKADD systems or data must follow appropriate security practices (see Section 16 for detailed requirements). This includes:

- Following NKADD security requirements and contract terms
- Protecting NKADD data from unauthorized access or disclosure
- Reporting any suspected security incidents involving NKADD data
- Maintaining security practices appropriate to the services provided and consistent with contractual, legal, and regulatory requirements

5. Acceptable Use Policy

NKADD technology resources are provided to support the organization's mission and daily operations. All users are expected to use these resources responsibly, securely, and in a manner that supports official NKADD business.

5.1 General Use

NKADD systems, networks, and devices are intended primarily for business use. Limited personal use is permitted if it:

- Is infrequent and brief
- Does not interfere with job responsibilities
- Does not create additional cost or risk for NKADD
- Does not violate any policies or laws

5.2 Ownership and Monitoring

All NKADD technology resources, including systems, devices, networks, and data, are the property of NKADD.

Users should have no expectation of privacy when using NKADD systems. NKADD reserves the right to monitor, access, and review system activity, communications, and stored data as needed to maintain security, ensure compliance, and support operations.

See Section 12 for additional detail on logging and monitoring practices.

5.3 Appropriate Use

Users must:

- Use NKADD systems for authorized business purposes
- Protect their login credentials and not share accounts
- Follow all applicable policies, procedures, and security requirements
- Exercise good judgment when accessing internet and communication resources

5.4 Prohibited Activities

The following activities are prohibited unless explicitly authorized:

- Engaging in illegal activities or activities that violate NKADD policies
- Attempting to bypass or disable security controls
- Accessing, downloading, or distributing inappropriate, offensive, or harmful content
- Installing or using unauthorized software or applications

- Using NKADD resources for personal business or commercial gain
- Sending unsolicited or excessive messages (e.g., spam, chain emails)
- Misrepresenting identity or using another user's account without authorization
- Purchasing, downloading, installing, or subscribing to software, applications, or technology services without appropriate authorization
- Soliciting support for political campaigns, candidates, or religious causes using NKADD resources
- Advocating for or against political candidates, parties, or ballot measures, or endorsing religious positions, in any official NKADD capacity or using NKADD resources
- Downloading, copying, or distributing copyrighted material (such as software, music, movies, or publications) without proper licensing or authorization
- Using a hand-held mobile device to make calls, send texts or emails, or access navigation while operating a motor vehicle on NKADD business, except through hands-free or voice-activated methods
- Recording the statements or actions of other NKADD employees by audio, video, or other electronic means without their prior knowledge or consent, except as specifically authorized by the Executive Director

5.5 Email and Communication Systems

NKADD email and communication systems are intended for official business use. Users must:

- Use professional and appropriate language
- Avoid sending or forwarding unnecessary or non-business-related messages
- Exercise caution regarding phishing attempts, fraudulent communications, suspicious links, attachments, or requests for sensitive information
- Verify any request to change payment instructions, vendor banking information, or direct deposit details by calling the requester at a phone number already on file (not a number provided in the request) or confirming in person, before any change is made
- Not use NKADD email accounts to register for personal services unrelated to business
- Understand that emails, messages, and records created or stored using NKADD systems may be subject to public records laws and legal disclosure requirements
- Report suspected phishing emails using NKADD-approved reporting tools (such as the KnowBe4 Phishing Alert Button)

5.6 Internet and Cloud Usage

Users must use internet and cloud services responsibly:

- Access to websites must support business purposes
- Users must not use unauthorized cloud storage or file-sharing services

- Only NKADD-approved platforms (such as Microsoft 365) may be used for storing or sharing organizational data

Confidential Data or Sensitive Information (as defined in Section 3) must not be entered into any public or unapproved AI or generative AI platform. If NKADD adopts an approved AI tool, its use will be governed by IT guidance and this policy. Use of AI tools must never expose NKADD data or violate the data protection requirements of this policy.

5.7 Social Media

Employees who use social media, whether personally or on behalf of NKADD, must do so in a manner that protects NKADD's data, reputation, and legal obligations.

- NKADD time and equipment must not be used for personal social media activity except for incidental, infrequent use consistent with Section 5.1
- Employees must not disclose confidential or sensitive NKADD information via social media, including HIPAA-protected information or other client information protected by law
- Employees must not post photographs or personal information about coworkers, clients, or program participants without their express consent
- Employees authorized to post on behalf of NKADD must follow guidance established by the Executive Director or designee
- Employees identifying themselves as NKADD staff when discussing NKADD-related matters on personal social media should note that views expressed are their own and not NKADD's
- This section addresses social media use as it relates to information security and data protection; conduct-related social media expectations are addressed in Chapter 8, Section 7 of the NKADD Personnel Policies

5.8 Mobile Devices and Remote Use

When using laptops, mobile devices, or remote access:

- Devices must be secured when unattended
- Users must avoid using public or unsecured networks without protection
- Sensitive information must not be exposed in public or shared environments

See Section 9 for additional remote access and telework requirements.

5.9 Personally Owned Devices (BYOD)

Employees may use personally owned devices to access NKADD email, Teams, and other NKADD

systems through NKADD-approved apps, as described in Section 7.7. Any other use of a personal device to access NKADD systems or data must be approved by the IT Director.

NKADD is not responsible for the maintenance or support of personal devices. Approved devices must meet minimum security requirements established by IT.

5.10 Enforcement

Use of NKADD technology resources is a privilege. Violations of this policy may result in:

- Loss of access to systems or data
- Disciplinary action, up to and including termination
- Legal action where applicable

NKADD reserves the right to suspend or restrict access at any time to protect its systems or data.

See Section 17 for additional details on policy enforcement.

6. Access Control

Access to NKADD systems and data must be controlled so that only authorized individuals have access to the information and resources necessary to perform their job duties. NKADD follows a "least privilege" approach, meaning users are granted only the access they need to carry out their responsibilities.

Failure to follow access control requirements may result in restricted access or disciplinary action.

6.1 User Accounts

Each user must be assigned a unique user account.

- Shared, generic, or service accounts are not permitted unless required for business operations and explicitly approved by the IT Director
- Users are responsible for all activity performed using their account
- User access must be approved by the appropriate supervisor or department leadership

6.2 Account Provisioning and Deprovisioning

User access must be managed consistently throughout the employee lifecycle.

- Access must be requested and approved before being granted
- Access must be adjusted promptly when an employee changes roles
- Access must be removed at the end of the last day of employment or contract, or immediately for an involuntary separation (see Personnel Policies, Chapter 12, Section 9)
- Supervisors or Human Resources are responsible for notifying IT of any changes in employment status

6.3 Authentication Requirements

Authentication methods are a critical component of system security and must be managed appropriately. NKADD supports the use of modern authentication methods, including passwords, PINs, and biometric authentication (such as facial recognition), where supported.

Password Requirements

- Passwords must meet the minimum length and complexity requirements enforced by NKADD systems, which will be at least 8 characters for accounts protected by multi-factor authentication
- Passwords must not be shared or stored insecurely
- Default or temporary passwords must be changed upon first use

Modern Authentication Methods

- When available, users should use NKADD-approved modern authentication methods, such as Windows Hello for Business (PIN or biometric authentication)
- Authentication methods must be configured and managed in accordance with NKADD security requirements
- Authentication credentials, security tokens, PINs, biometric registrations, and other authentication factors must not be shared with others
- Users must not attempt to bypass or disable approved authentication controls

Credential Management

- Users must not store passwords in an insecure manner, such as in plain text files, spreadsheets, sticky notes, or unencrypted documents
- If NKADD adopts an approved password or credential management tool, its use will be required for storing and managing authentication credentials
- Users are responsible for protecting all authentication methods associated with their account

6.4 Multi-Factor Authentication (MFA)

Multi-factor authentication is required for NKADD-managed systems that present elevated risk or provide access to sensitive data, including Microsoft 365, administrative systems, and remote access environments.

MFA must be used for:

- Remote access to NKADD systems
- Email and cloud-based services administered by NKADD, including Microsoft 365
- Administrative, privileged, and other high-risk accounts as determined by IT
- Third-party or vendor-managed platforms or services registered with an NKADD email address or account, where MFA is offered (the user is responsible for turning it on)

Where a choice of MFA method is available, an authenticator app or hardware security key is preferred over SMS text message codes. SMS-based MFA may be used where no stronger option is supported by a given system.

For third-party or vendor-managed systems that are not administered by NKADD, MFA and other authentication controls are expected to be implemented in accordance with the vendor's security practices and applicable contractual requirements.

6.5 Account Security and Monitoring

User accounts must be actively managed and monitored to prevent unauthorized access.

- Accounts may be locked after repeated failed login attempts
- Inactive accounts may be disabled after a defined period of inactivity
- IT is responsible for monitoring access and investigating suspicious activity
- Users must immediately report suspected account compromise, unauthorized access, or credential exposure to IT
- Administrative or privileged accounts must only be used for administrative tasks and not for routine day-to-day activities where feasible
- Third-party, vendor, contractor, and service-provider accounts must be reviewed periodically and disabled promptly when access is no longer required

6.6 Access Reviews

Access to NKADD systems and data must be reviewed periodically to ensure it remains appropriate and aligned with job responsibilities.

Access reviews are conducted at the system, application, and tenant level, with a focus on user roles, group memberships, and administrative privileges.

- User access should be reviewed at least annually
- Access must be reviewed when employees change roles or responsibilities
- Administrative, privileged, and high-risk access must be reviewed more frequently as determined by IT
- Access that is no longer required must be removed promptly

Granular permissions at the individual file, folder, or document level are managed by departments and users in accordance with data handling requirements and are not subject to centralized periodic review unless identified as high risk.

Systems or data identified as high risk may require more detailed or targeted access reviews.

6.7 Remote Access

Remote access to NKADD systems must be restricted to authorized users and controlled in accordance with access management requirements.

- Access to NKADD-approved cloud platforms, such as Microsoft 365, is available remotely to authorized users through approved secure methods. Any other form of remote access to NKADD systems, such as remote desktop or VPN access to internal systems, must be approved by the IT Director before it is granted
- Access must use NKADD-approved secure methods and be limited to authorized users with a defined business need
- Access permissions must be reviewed and adjusted when no longer required

See Section 9 for additional remote access and telework requirements.

7. Data Protection

NKADD is responsible for protecting the confidentiality, integrity, and availability of the data it creates, stores, and processes. All users must handle information in a manner that prevents unauthorized access, disclosure, alteration, or loss.

7.1 Data Classification

NKADD data must be handled according to its level of sensitivity. Data is generally categorized as:

- Public – Information intended for public release
- Internal – Information intended for internal NKADD use only
- Confidential – Sensitive information requiring protection, including personally identifiable information (PII), protected health information (PHI), financial data, and personnel records

NKADD's status as a public agency subject to the Kentucky Open Records Act (KRS 61.870–61.884) does not mean all NKADD data is public. The Act exempts certain categories of records — including information that would constitute an unwarranted invasion of personal privacy (KRS 61.878) — from mandatory disclosure. This classification framework governs the day-to-day handling and protection of NKADD information; it is separate from, and does not replace, the legal determination of what must be disclosed or may be withheld in response to a specific open records request, which is made by the official custodian of records under the Administrative Regulations, in consultation with legal counsel as needed, at the time of the request.

When the appropriate classification of a piece of information is unclear, users should treat it as Confidential until its classification can be confirmed with a supervisor or the IT Director.

Protected Health Information (PHI) is handled by NKADD in connection with certain programs and services. In addition to being classified as Confidential under this policy, PHI is subject to additional requirements under the Health Insurance Portability and Accountability Act (HIPAA), including limitations on access and disclosure, and specific breach notification obligations (see Section 14). Departments handling PHI must follow any additional program-specific requirements established by IT, the Executive Director, or applicable funding agreements. Workplace procedures for protecting PHI are in Appendix E of the Personnel Policies.

Users must apply appropriate care when handling data based on its classification.

7.2 Data Handling

Users are responsible for protecting NKADD data in their daily work.

- Access to sensitive data must be limited to authorized users with a business need

- Sensitive data must not be shared with unauthorized individuals
- Users must take reasonable steps to prevent accidental disclosure of information
- Unauthorized access to data ("browsing") is prohibited
- Confidential information in paper form must be protected from unauthorized access and secured when not in use
- Suspected loss, exposure, or unauthorized disclosure of sensitive information must be reported immediately to IT

7.3 Data Storage and Cloud Services

NKADD data must be stored only in approved systems.

- Only NKADD-approved platforms, such as Microsoft 365 and other authorized cloud or vendor systems, may be used for storing or processing organizational data
- Storage of NKADD data on personal accounts, personal cloud storage services, or unapproved systems is prohibited
- Data stored in cloud or vendor-managed systems must be protected through appropriate contractual, administrative, and technical safeguards suited to the services provided

7.4 Data Transmission

Sensitive data must be protected when transmitted.

- Sensitive data must be shared using secure, NKADD-approved, encrypted methods. See Section 10 for encryption requirements
- Users must verify recipients before sending sensitive information

7.5 Data Retention and Disposal

NKADD data must be retained in accordance with established records retention schedules and applicable legal, regulatory, and operational requirements.

- Data must be retained in accordance with the Local Government General Records Retention Schedule and the Area Development District (ADD) General Records Retention Schedule
- When no longer needed, data must be securely deleted or destroyed
- Physical records must be disposed of using approved methods (e.g., shredding)
- Electronic data must be removed in a manner that prevents recovery
- NKADD-owned computers, phones, removable media, and other equipment that may store NKADD data must be given to IT for data removal before disposal, transfer, or return to a lessor (see Administrative Regulations, Section 4)

7.6 Portable Media and Devices

The use of removable or portable storage must be controlled.

- Sensitive data must not be stored on portable media unless necessary
- Portable media containing NKADD data must be protected from loss or theft
- Use of external storage devices may be restricted and may require approval from the IT Director

Portable media containing sensitive information must be encrypted whenever supported and practical. See Section 10 for encryption requirements.

7.7 Personally Owned Devices (BYOD)

Use of personally owned devices to access NKADD systems or data must comply with NKADD security requirements as established by the IT Director.

- Access to NKADD data from personal devices must be approved or otherwise authorized in accordance with IT-defined standards and practices
- Personal devices must meet minimum security requirements, including updated software, device locking, and other controls established by IT
- NKADD data must not be permanently stored on personal devices unless specifically approved

Any personally owned device that stores NKADD information or documents locally may be subject to access, review, or other legal requirements, including public records requests.

7.8 Data Backup and Recovery

NKADD's data primarily resides within its Microsoft 365 environment, which is protected through built-in retention and version history, supplemented by a third-party backup service (Druva) that provides independent backup of the NKADD M365 tenant. This provides an additional recovery layer beyond native Microsoft 365 retention in the event of accidental deletion, corruption, or a ransomware incident.

- Backup coverage and retention settings must be reviewed periodically by IT to confirm they remain adequate for NKADD's needs
- Backup restoration must be periodically tested to confirm data can be recovered when needed
- Hosted, vendor-managed systems (e.g., AccuFund and other SaaS platforms) are backed up by their respective vendors as part of NKADD's service agreements; NKADD does not separately back up data that resides solely within those platforms

8. Endpoint & Network Security

NKADD systems and networks must be protected from unauthorized access, malware, and other cybersecurity threats. Security controls must be in place to safeguard all devices and network resources used to store, process, or transmit NKADD data.

8.1 Endpoint Security

All devices connected to NKADD systems or networks must meet minimum security requirements.

- All endpoints must use approved endpoint protection software (such as antivirus or endpoint detection and response tools)
- Devices must have current security updates and patches installed
- Devices must be configured and maintained according to IT standards
- Users must not disable or bypass security controls on any device
- Mobile devices used to access NKADD systems or data must comply with applicable security requirements established by IT
- Users must immediately report suspected malware infections, security warnings, or unusual device behavior to IT

See Section 5.9 and Section 7.7 for additional requirements specific to personally owned devices (BYOD).

8.2 Patch Management

Keeping systems up to date is a critical part of maintaining security.

- Operating systems and applications must be updated regularly
- Critical security updates should be applied as soon as practical
- Systems that cannot be updated must be evaluated and approved by IT
- Systems that are no longer supported by the manufacturer must not be used unless approved compensating controls have been implemented

8.3 Device Security

Devices must be physically and logically secured to prevent unauthorized access.

- Devices must be locked when unattended
- Screen locks and automatic timeouts must be enabled
- Sensitive information should not be visible or accessible to unauthorized individuals
- NKADD maintains an inventory of devices and technology assets connected to organizational systems

- Lost or stolen devices must be reported immediately

8.4 Network Security

NKADD networks must be monitored and protected to prevent unauthorized access.

- Firewalls must be used to protect internal systems
- Network access must be limited to authorized users and devices
- Wireless networks used for NKADD business must be secured using approved authentication and encryption methods
- Network activity may be monitored to detect and respond to threats
- Users must not connect unauthorized devices to NKADD systems or networks without IT approval

8.5 Remote Access Security

Remote access to NKADD systems must be protected using appropriate technical security controls to prevent unauthorized access and ensure the integrity of systems and data.

- Remote access activity may be monitored to detect and respond to unauthorized or suspicious activity

See Section 6 for remote access approval, authentication, and review requirements, and Section 9 for telework-specific security requirements.

8.6 Software and Application Control

Software installed on NKADD systems must be managed to reduce risk.

- Only approved software may be installed on NKADD devices
- Software must be properly licensed and maintained
- IT is responsible for evaluating and approving software before use

9. Remote Access & Telework

Remote access and telework are important to NKADD operations but introduce additional security risks. Remote work arrangements are governed by NKADD's Personnel Policies (Chapter 4, Section 4 – Working Remotely). This section defines the information security requirements that apply when working remotely.

9.1 General Requirements

Remote access to NKADD systems must follow all applicable policies and security requirements.

- Remote access is permitted for authorized users in accordance with NKADD's Personnel Policies and business needs
- Access must comply with NKADD security requirements, including approved methods and authentication controls
- The IT Director reserves the right to restrict, suspend, or revoke remote access at any time to protect NKADD systems and data
- Users must follow all security practices outlined in this policy when working remotely

9.2 Secure Access Methods

All remote access must use secure, NKADD-approved technologies.

- Access to NKADD systems must occur through approved platforms such as Microsoft 365 or other authorized cloud-based services
- Multi-factor authentication (MFA) is required for remote access
- Users must not attempt to bypass or disable security controls when accessing systems remotely

9.3 Device Security for Remote Work

Devices used for remote access must meet NKADD security standards.

- NKADD-issued devices should be used for remote access whenever possible
- Personally owned devices must comply with NKADD BYOD and security requirements
- Devices must have current updates, endpoint protection, and security controls enabled
- Devices must be secured when not in use
- Lost, stolen, damaged, or compromised devices used for remote work must be reported immediately to IT

See Section 5.9, Section 7.7, and Section 8.1 for additional BYOD and endpoint security requirements.

9.4 Network and Environment Security

Users are responsible for maintaining a secure remote environment.

- Remote work should be conducted over secure and trusted networks
- Public or unsecured Wi-Fi must not be used to access NKADD systems unless connecting through an NKADD-approved secure method (such as a properly authenticated, MFA-protected connection to NKADD-approved cloud platforms). If in doubt, use a personal hotspot or wait until a trusted network is available
- Sensitive information must not be viewed, discussed, or exposed in public or unsecured environments

9.5 Data Protection During Remote Work

NKADD data must be protected at all times, including during remote access.

- Data must only be accessed and stored in approved systems
- Users must not download or store sensitive data locally unless necessary and approved
- Printed materials containing sensitive data must be secured when not in use and disposed of in accordance with Section 7.5 (e.g., shredding)

9.6 Remote Work Equipment and Peripherals

Remote work equipment and peripherals must be used in accordance with NKADD policies and IT requirements.

- NKADD-issued devices remain the primary computing equipment for remote work
- NKADD may provide limited equipment, such as one external monitor and necessary cabling, for approved remote work arrangements
- Additional personal devices and peripherals may be used but are not provided, managed, or supported by NKADD
- NKADD-issued equipment must be used for business purposes only and must be returned upon request or at the end of employment
- Users are responsible for maintaining the physical security of equipment in remote environments

9.7 Session Management

Remote sessions must be properly managed to reduce risk.

- Users must log out or disconnect from systems when work is complete
- Idle sessions must not be left unattended
- Devices must be locked when unattended

10. Encryption

Encryption is used to protect NKADD data from unauthorized access, both while it is stored and while it is being transmitted. Appropriate encryption controls must be used to safeguard sensitive information.

10.1 General Requirements

Encryption must be used to protect sensitive NKADD data when supported by approved systems and technical capabilities.

- Sensitive data must be protected against unauthorized access
- Encryption must be used in accordance with NKADD standards and technical capabilities
- Users must not attempt to disable or bypass encryption controls

10.2 Data in Transit

Sensitive data must be protected when transmitted across networks.

- Data containing sensitive information must be transmitted using secure, encrypted methods
- NKADD-approved systems such as Microsoft 365 must be used for sharing sensitive data
- Users must verify recipients before transmitting sensitive information

10.3 Data at Rest

Sensitive data stored on devices or systems must be protected.

- NKADD-issued laptops, mobile devices, and other supported devices that store sensitive information must utilize encryption
- Portable storage devices containing sensitive information must utilize encryption whenever supported and practical
- Access to stored data must be restricted to authorized users
- Sensitive data must not be stored in unapproved locations or systems
- Cloud and vendor-managed systems storing sensitive NKADD data must provide encryption capabilities appropriate to the services provided

10.4 Email and File Sharing

This section provides additional requirements specific to email and file sharing; see Section 10.2 for general requirements on transmitting sensitive data.

- Users must use NKADD-approved tools and services when sharing files or documents containing sensitive data

- Confidential Data (as defined in Section 3), particularly PHI and financial account information, must be sent using additional safeguards, such as encryption, secure file sharing, or password-protected documents

10.5 Encryption Management

Encryption technologies must be managed appropriately.

- Encryption methods and tools must be approved by IT
- Encryption keys, certificates, and related security credentials must be protected from unauthorized access and managed according to NKADD standards
- IT is responsible for evaluating and maintaining encryption standards

11. Electronic Signatures

Electronic signatures may be used to verify the authenticity and integrity of electronic communications and documents. When used appropriately, electronic signatures help ensure that information has not been altered and that it originates from a trusted source.

11.1 Approved Use

Electronic signatures must be applied using NKADD-approved tools and must provide a verifiable record of the signer's identity and the integrity of the signed document.

Electronic signatures that consist solely of typed names, images, or handwritten representations without supporting authentication, audit trail, or verification controls do not meet NKADD requirements for official or sensitive documents unless specifically approved by the IT Director.

- Only approved applications and platforms may be used for applying electronic signatures
- NKADD-approved electronic signature tools (such as Adobe Acrobat Pro) must be used for official documents and agreements
- Users must not use unapproved or unauthorized tools to sign official NKADD documents
- Electronic signatures must only be applied by authorized individuals

11.2 Email and Document Use

Electronic signatures may be used for email and document verification where appropriate.

- Users may apply electronic signatures to email communications when identity verification is necessary
- Electronic signatures should be used on official or sensitive documents where authenticity is important
- Signed documents must be retained in accordance with NKADD records retention requirements

11.3 Integrity and Control

Electronic signatures must be protected and used responsibly.

- Users must not share credentials or tools used to create electronic signatures
- Signed documents must not be altered after signing
- Any suspected misuse, compromise, loss, or unauthorized use of electronic signature credentials or tools must be reported immediately to IT
- Users must take reasonable steps to verify the identity of signers when processing official documents or agreements

11.4 Legal and Compliance Considerations

Electronic signatures must comply with applicable legal and regulatory requirements.

- Electronic signatures used for official purposes must be legally valid and recognized
- NKADD-approved electronic signature tools must be used for formal agreements or contracts
- Users must follow established processes for documents requiring formal approval or execution
- Use of an electronic signature does not grant authority to approve, execute, or enter into agreements on behalf of NKADD

For grant agreements, contracts, or documents submitted to auditors or funding agencies, users should confirm the receiving party accepts electronic signatures before relying on one.

Electronic or facsimile signatures on checks are additionally governed by NKADD Administrative Regulations, Section 2 (Disbursements).

12. Logging, Monitoring & Auditing

NKADD uses logging and monitoring controls to identify, respond to, and prevent unauthorized access to systems and data. These activities help ensure the security, integrity, and availability of NKADD technology resources.

12.1 Logging Requirements

NKADD systems must maintain appropriate logging to support security and operational needs.

- Systems must log key events such as user logins, access to systems, and administrative actions
- Logs must be stored in a secure and controlled manner
- Access to logs must be limited to authorized personnel
- Systems must maintain accurate date and time settings to support reliable logging and event correlation
- At minimum, logs should capture the user or account involved, the date and time of the event, and the type of action taken

12.2 Monitoring Activities

System activity must be monitored to detect security threats or policy violations.

- IT is responsible for monitoring systems and reviewing security-related events
- Monitoring may include user activity, system access, and network behavior
- Suspicious or unusual activity must be investigated promptly

12.3 Microsoft 365 and Cloud Monitoring

NKADD relies on Microsoft 365 and other cloud platforms to provide logging and monitoring capabilities.

- Logging features within Microsoft 365 (such as audit logs and security alerts) must be enabled and used
- Security alerts and notifications must be reviewed by IT
- Cloud-based systems must be monitored in accordance with NKADD security requirements
- Where available, logging and monitoring capabilities provided by third-party or vendor-managed systems must be enabled and reviewed

12.4 Log Retention

Logs must be retained for an appropriate period to support investigations and compliance.

- Logs must be retained for at least the period provided by the applicable system (for Microsoft 365, the retention included with NKADD's licensing), or longer where required by legal, contractual, or operational needs
- Logs must be protected from unauthorized modification, deletion, or access
- Archived logs must remain accessible for review if needed

12.5 Auditing

Periodic reviews must be conducted to ensure compliance with this policy.

- IT is responsible for conducting audits of system access, user activity, and security controls to verify compliance with NKADD policies and security requirements
- Departments may be asked to participate in reviews of data access and usage
- Identified issues must be addressed in a timely manner

12.6 Incident Support

Logging and monitoring must support incident response activities.

- Logs must be used to investigate suspected security incidents
- Relevant logs and system data must be preserved during an investigation
- Findings from monitoring and auditing activities must be used to improve security controls

13. Security Incident Response

NKADD must respond promptly and effectively to security incidents in order to minimize impact and restore normal operations. All users share responsibility for identifying and promptly reporting potential incidents.

13.1 Definition of an Incident

A security incident is any event that may compromise the confidentiality, integrity, or availability of NKADD systems or data.

- Incidents may include unauthorized access, malware infections, ransomware, data breaches, phishing attempts, loss or theft of devices, or system disruptions
- Suspicious activity or unusual system behavior may also be considered an incident

13.2 Reporting Requirements

All users must report suspected security incidents immediately.

- Incidents must be reported to the IT Director or designated IT staff without delay
- Reports should include relevant details such as the nature of the issue, time of occurrence, and affected systems
- Users must not attempt to investigate or remediate incidents on their own unless directed by IT
- Lost or stolen devices that access, store, or process NKADD data must be reported to IT immediately. The employee must also file a police report as soon as practical, with a copy provided to the employee's supervisor and IT. When the applicable contract requires it, IT will forward the report to the funding cabinet. Whether to notify KALF is decided under Section 13.8.

13.3 Incident Response Activities

NKADD will respond to incidents in a structured and timely manner.

- IT is responsible for assessing, containing, and investigating incidents
- Appropriate steps will be taken to limit impact and prevent further damage
- Systems and data will be restored as quickly as possible following an incident
- External support, including vendors or legal counsel, may be engaged as needed, subject to the insurance coordination requirements in Section 13.8
- Incidents may be categorized based on severity, scope, or impact to support appropriate response and escalation

13.4 Communication and Escalation

Incidents must be communicated to appropriate leadership based on severity.

- Significant incidents must be escalated to the Executive Director by the IT Director
- The Executive Director will determine if escalation to the Board of Directors is necessary
- External communications must be coordinated through authorized personnel
- Where required, NKADD will coordinate legal, regulatory, contractual, and breach notification activities through authorized personnel

See Section 4.3 for escalation and coordination requirements when the IT Director is unavailable.

13.5 Evidence Preservation

Information related to incidents must be preserved to support investigation and response.

- Logs, backup data, system data, and affected devices must be retained and protected
- Users must not alter or delete information that may be relevant to an incident
- IT is responsible for maintaining the integrity of evidence

13.6 Coordination with the Incident Response Plan

NKADD will maintain an Incident Response Plan (IRP) that provides detailed procedures for handling security incidents.

- The IRP will define specific roles, workflows, and response actions
- Once the IRP is adopted, incident response activities must follow it
- Until the IRP is adopted, the IT Director directs incident response under this Section 13

13.7 Post-Incident Review

NKADD will review incidents to improve security and prevent recurrence.

- Significant incidents must be documented and evaluated following resolution
- Lessons learned must be incorporated into policies, procedures, or controls
- Identified gaps must be addressed in a timely manner

13.8 Cyber Insurance Coordination

NKADD's cyber liability coverage is provided through the Kentucky Association of Counties All Lines Fund (KALF). Coverage depends on timely notice, preservation of evidence, and obtaining consent before incurring response costs, so the following requirements apply.

Notice to KALF is a condition of coverage rather than a legal obligation. The IT Director, in consultation with the Executive Director, will determine whether to notify KALF. Notice should be provided as soon as practicable when an incident:

- Is expected to result in costs NKADD may seek to recover, such as forensic investigation, legal counsel, data restoration, notification of affected individuals, or business interruption
- Involves actual or reasonably suspected unauthorized access to personal information, or may require notification under KRS 61.931–61.934 or HIPAA
- Could reasonably be expected to lead to a claim, lawsuit, or regulatory inquiry against NKADD
- Involves a ransom or extortion demand

When in doubt, NKADD should notify KALF. Notice preserves coverage and does not commit NKADD to filing a claim. Routine incident handling, such as blocked phishing attempts or alerts resolved without compromise, does not require notice.

- When NKADD decides to notify KALF, the IT Director, in coordination with the Executive Director, must provide written notice as soon as practicable. The notice period begins when NKADD leadership becomes aware of the incident, not when the investigation is complete
- IT may take immediate steps to contain an active threat. Beyond initial containment, NKADD must not engage outside forensic, legal, data recovery, notification, credit monitoring, or public relations services for an incident reported to KALF without prior written consent from KALF or its insurer
- Logs, backup data, and affected systems related to an incident reported to KALF must be retained and made available to KALF or its insurer on request
- NKADD must not pay, or agree to pay, any ransom or extortion demand without authorization from the Executive Director, Board approval where required by the Administrative Regulations, and prior written consent from KALF or its insurer
- NKADD must not admit liability, offer settlements, or take on financial obligations to third parties related to an incident reported to KALF without consent from KALF or its insurer
- Coverage details, contact information, and notice procedures will be maintained in the Incident Response Plan. Until it is adopted, the IT Director maintains this information

14. Breach Notification

NKADD is committed to complying with all applicable laws and regulations regarding the protection of sensitive information. In the event of a data breach, NKADD will take appropriate steps to investigate, contain, and notify affected parties as required.

14.1 Definition of a Data Breach

A data breach is an incident in which sensitive, protected, or confidential information may have been accessed, disclosed, or acquired without authorization.

- Data breaches may involve personally identifiable information (PII), protected health information (PHI), financial data, or other confidential records
- A suspected or potential exposure of sensitive data may also be treated as a breach until evaluated
- Not all security incidents constitute a data breach; breach determinations will be made based on investigation and applicable legal requirements

Breaches involving PHI may trigger additional notification requirements and timelines under HIPAA, separate from and in addition to the notification requirements described in this section (see Section 14.2).

14.2 Notification Requirements

NKADD will provide notification of data breaches in accordance with applicable laws, including Kentucky Revised Statutes (KRS) 61.931–61.934.

- Affected individuals will be notified when required by law
- Where KRS 61.931–61.934 applies, NKADD must notify the Commissioner of the Kentucky State Police, the Auditor of Public Accounts, and the Attorney General within 72 hours of determining or being notified of a breach of personal information, followed by the additional notices and deadlines in KRS 61.933
- Notification will be made without unreasonable delay, consistent with legal and investigative requirements
- Notifications may include information about the nature of the breach and recommended actions for affected individuals
- Notification requirements arising from contractual, regulatory, grant, or partner obligations must also be considered where applicable
- NKADD may notify regulators, law enforcement, insurers, partner organizations, or other entities when required by law, contract, or operational necessity
- Notice to KALF is governed by Section 13.8

14.3 Internal Reporting and Escalation

All suspected data breaches must be reported immediately.

- Users must report potential breaches to the IT Director or designated IT staff
- IT, in coordination with leadership and legal counsel when appropriate, is responsible for assessing whether a breach has occurred and whether notification obligations exist

- Confirmed breaches must be reported to the Executive Director
- The Executive Director will determine if escalation to the Board of Directors is required

14.4 Investigation and Response

NKADD will investigate all suspected breaches in a timely manner.

- IT will work to identify the scope and impact of the breach
- Appropriate steps will be taken to contain and remediate the issue
- External support, including legal counsel or vendors, may be engaged as needed, subject to the insurance coordination requirements in Section 13.8

14.5 Documentation

All breaches must be properly documented.

- Details of the incident, investigative findings, response actions, notification decisions, and outcomes must be recorded
- Documentation must be maintained in accordance with NKADD policies and requirements
- Lessons learned should be used to improve security practices and controls

15. Security Awareness & Training

NKADD requires all users to participate in ongoing security awareness training to help protect systems and data from threats such as phishing, malware, and unauthorized access. Security awareness is a shared responsibility, and all users must remain informed about current risks and best practices.

15.1 General Requirements

All users must complete security awareness training as a condition of access to NKADD systems.

- Security awareness training is required for all employees and other users with NKADD accounts, as determined by IT
- Training must be completed in accordance with NKADD requirements and schedules
- Users are responsible for understanding and applying security practices in their daily work

15.2 Training Program

NKADD utilizes a structured security awareness program to provide ongoing education.

- NKADD uses KnowBe4 security awareness training modules to educate users on current security threats and best practices
- Training modules are assigned monthly
- Users must complete all assigned training within the required timeframe
- Training topics may include phishing, social engineering, payment and invoice fraud, password security, data protection, ransomware, remote work security, and other emerging threats

15.3 Phishing Simulations

Simulated phishing exercises are used to test and improve user awareness.

- NKADD conducts simulated phishing campaigns on a regular basis
- Users must report suspicious emails, messages, websites, or other suspected security threats
- The KnowBe4 Phishing Alert Button (PAB) must be used when reporting suspected phishing emails
- Use of the PAB helps IT track and respond to potential threats and measure user awareness
- Results of phishing simulations may be used to identify training needs and improve security awareness

15.4 Remedial Training

Additional training is required for users who do not successfully identify simulated threats.

- Users who fail a simulated phishing test are required to complete additional security awareness training
- Remedial training must be completed within the timeframe specified by IT
- Repeat failures may result in additional training, supervisory review, or other corrective actions as determined by NKADD

15.5 New User Training

New users must complete security training prior to or shortly after receiving system access.

- All new employees and other new users with NKADD accounts, as determined by IT, must complete an initial security awareness training module
- Initial training must be completed within 3 business days of receiving system access
- Access to systems may be limited until required training is completed
- Additional role-based security training may be required for users with elevated privileges or access to sensitive information, including HIPAA-specific training for users who handle PHI in the course of their work

15.6 Program Oversight

The security awareness program must be maintained and monitored.

- IT is responsible for administering the training program and tracking completion
- Training content will be updated periodically to reflect emerging threats
- Training and participation records must be maintained for compliance and audit purposes

16. Vendor & Third-Party Security

NKADD works with third-party vendors and service providers that may have access to systems, services, or data. These relationships must be managed to ensure that NKADD information remains secure and that risks are appropriately controlled.

16.1 Vendor Access and Responsibilities

Vendors and third parties must meet NKADD security expectations when accessing systems or data.

- Vendors must only be granted the access necessary to perform their services
- Vendor access must be approved by the IT Director or appropriate authority
- Vendors must follow NKADD security requirements and applicable policies
- Vendor access must be periodically reviewed and may be monitored by NKADD

16.2 Data Protection Requirements

Vendors must protect NKADD data in accordance with applicable standards.

- Vendors must implement reasonable safeguards to protect NKADD data from unauthorized access or disclosure
- NKADD data must only be used for authorized business purposes
- Vendors must not share NKADD data with unauthorized parties
- Data must be stored and processed in approved systems or environments
- Vendors remain responsible for ensuring that subcontractors or downstream service providers handling NKADD data maintain appropriate security protections
- NKADD retains ownership of its data regardless of where the data is stored or processed

16.3 Contracts and Agreements

Vendor relationships must include appropriate security and data protection terms.

- Contracts or agreements must define security expectations and responsibilities
- Agreements must include provisions for protecting confidential or sensitive data
- Where applicable, agreements must include breach notification requirements and timelines
- Vendors must comply with applicable legal and regulatory requirements
- Where KRS 61.932 applies, agreements must specify how the costs of breach investigation and notification are apportioned

16.4 Vendor Risk Management

NKADD must manage and evaluate risks associated with third-party vendors.

- Vendors must be evaluated prior to engagement based on the sensitivity of the data or services involved
- Higher-risk vendors may require additional review or documentation
- Vendor access and risk may be reviewed periodically
- Vendors that store, process, or transmit sensitive NKADD data may be required to provide security documentation, audit reports, certifications, or other evidence of security controls

16.5 Incident and Breach Reporting

Vendors must report security incidents involving NKADD data.

- Vendors must notify NKADD without unreasonable delay, and no later than 72 hours, following discovery of an actual or suspected security incident involving NKADD data
- Notifications must include relevant details to support investigation and response
- NKADD will coordinate response activities in accordance with Sections 13 and 14 of this policy

16.6 Termination of Access

Vendor access must be removed when no longer required.

- Vendor access must be revoked upon completion of services or contract termination
- NKADD data must be returned or securely destroyed in accordance with contract requirements
- Vendors must confirm the secure handling or disposal of NKADD data when requested

17. Policy Enforcement

Compliance with this Information Security Policy is required for all NKADD employees, contractors, and authorized users. Failure to follow the requirements outlined in this policy may result in disciplinary action, up to and including termination of employment or contract, and may also include legal consequences where applicable.

17.1 Enforcement Authority

NKADD reserves the right to enforce this policy to protect its systems, data, and operations.

- NKADD may monitor systems, accounts, and user activity to ensure compliance with this policy
- NKADD may restrict, suspend, or revoke access to systems or data at any time when necessary to maintain security
- Enforcement actions will be taken in accordance with NKADD policies and procedures
- Users who report suspected security concerns or incidents in good faith will not be subject to retaliation for making such reports
- Exceptions to this policy may only be granted through documented approval as described in Section 4.3

17.2 Violations

Violations of this policy may include, but are not limited to:

- Unauthorized access to systems or data
- Failure to follow security requirements or procedures
- Misuse of NKADD technology resources
- Failure to report security incidents or suspicious activity
- Unauthorized disclosure of sensitive or confidential information
- Failure to cooperate with authorized security investigations or audits
- Failure to complete required security awareness training within the timeframe specified in Section 15

17.3 Disciplinary Actions

Violations of this policy may result in disciplinary action.

- Disciplinary actions may include verbal or written warnings, suspension, termination of employment or contract, or other corrective measures as appropriate. For employees, disciplinary action follows Chapter 11 of the NKADD Personnel Policies.
- Restricting or revoking access to protect NKADD systems or data (see Section 17.1) is a security measure and is not, by itself, disciplinary action

- The severity of the action will depend on the nature and impact of the violation
- Disciplinary actions will be coordinated with NKADD management and Human Resources, as appropriate

See Section 4.4 regarding the role of Human Resources in coordinating disciplinary matters.

17.4 Legal and Regulatory Consequences

Certain violations may result in legal or regulatory action.

- Violations involving illegal activity must be referred to law enforcement
- Violations involving sensitive data may result in reporting obligations under applicable laws
- NKADD may pursue legal remedies where necessary to protect its systems and data

See Section 14 for breach notification requirements when a violation involves a suspected data breach.

18. Review & Maintenance

This Information Security Policy must be reviewed and updated regularly to ensure it remains effective, accurate, and aligned with NKADD's operational and regulatory requirements.

18.1 Policy Review

The policy must be reviewed on a regular basis.

- This policy will be reviewed at least every two years, or more frequently as needed
- Reviews may be conducted in response to significant changes in technology, operations, or regulatory requirements
- Updates must be approved in accordance with NKADD governance processes

18.2 Policy Updates

The policy must be updated as necessary to reflect changes and improvements.

- Revisions must be documented and version-controlled
- Significant changes must be communicated to users
- Updated policies should be made available to all employees and authorized users
- Policy review and approval activities must be documented and retained in accordance with NKADD recordkeeping requirements
- Updates that resolve a previously identified pending item (e.g., naming a newly adopted tool or confirming a compliance status) are considered administrative rather than substantive, unless they materially change a requirement of this policy

18.3 Responsibility for Maintenance

Responsibility for maintaining this policy must be clearly defined.

- The IT Director is responsible for coordinating policy reviews and updates
- The Executive Director provides oversight of policy reviews and updates
- The Board of Directors approves this policy and any substantive revisions to it, in accordance with the Approval and Governance section of this document. Minor administrative updates — such as updating a named tool, contact, or role once previously identified as pending — may be made by the IT Director without requiring full Board re-approval, but must be documented in the Revision History.

18.4 Continuous Improvement

NKADD is committed to improving its information security practices over time.

- Findings from audits, incidents, and risk assessments must be used to improve the policy

- Feedback from users and departments may be considered during updates
- Changes in technology and emerging threats should be evaluated and addressed
- Changes in applicable laws, regulations, contractual obligations, and industry best practices should be considered during policy reviews

Approval and Governance

This policy is maintained, reviewed, and approved in accordance with NKADD governance requirements.

Monitoring and Administration

- The IT Director and IT staff are responsible for the ongoing monitoring and administration of this policy
- The IT Director oversees policy implementation and ensures compliance with established controls

Review

- This policy is reviewed by the IT Director and Executive Director, with input from IT staff and other stakeholders, as appropriate
- Reviews are conducted in accordance with the policy review cycle or as needed based on operational or regulatory changes

Approval

- This policy and any substantive revisions are formally approved by the NKADD Board of Directors (see Section 18.3 for the process governing minor administrative updates).

Approval Record

Approved by: Robb W Adams
Robb W Adams (Nov 3, 2026 10:44:52 EST)
Title: Chair

Approved by: J.Ryan Morris
J.Ryan Morris (Oct 22, 2026 16:00:31 EDT)
Title: First Vice Chair

Board Approval Date / Resolution Reference: 10/22/2026
Effective Date: 10/22/2026

Document Version Control

This section tracks the drafting and revision history of this policy, including updates made both before and after formal Board approval. Maintaining a revision history ensures transparency, accountability, and proper governance of policy updates over time.

All updates to this document must be reviewed and approved in accordance with NKADD policy governance requirements.

Revision History

Version	Date	Author	Description
1.0	6/5/2026	IT Director	Initial Policy Draft
1.1	6/15/2026	IT Support Specialist	Internal Revisions
1.2	8/28/2026	IT Director	Internal IT revisions
1.3	9/4/2026	ED / IT Director Review	ED review revisions; Chapter 13 provisions carried forward
1.4	9/23/2026	IT Director	Senior Staff and HR review revisions
1.5	10/13/2026	IT Director	KALF insurance alignment; Administrative Regulations and Personnel Policies alignment; final revisions for Board approval

Supersession

This policy supersedes any previous Information Security Policy, Internet Use Policy, Chapter 13: Technology of the Personnel Policies Manual, or related information security guidance previously adopted by NKADD.

Appendix E (Workplace Privacy Procedures for Protected Health Information) of the NKADD Personnel Policies is not superseded by this policy.