NeighborWorks America
Information Governance Policy

OUTLINE:

I. Purpose & Scope

The purpose of this policy is to establish uniform standards by which corporate records are stored, accessed, handled, transmitted, and destroyed at NeighborWorks America. This policy was drafted in accordance with applicable laws and industry best practices.

All Corporate records are subject to this policy regardless of their location, regardless of whether the record format is physical or electronic, and regardless of whether they are being managed by staff or third parties. This policy applies to Corporate records that are kept in individual offices, remote offices, mobile devices, and the Corporation's off-site storage facility. This policy applies to all NeighborWorks staff and third parties who handle Corporate records, including contractors, consultants, interns, temps, and auditors.

All original records must be maintained in established Corporate offices under the control of the Corporation. Corporate records may not be stored on personal computers at any time. Under no circumstance should any records be stored or maintained at home -- except for approved remote work locations, and in these instances, only duplicate records may be maintained at the remote work location.

II. Definitions

- Confidential Information - sensitive or private information that is subject to increased handling and protection requirements because disclosure outside of NeighborWorks America would be illegal, improper, or damaging. Examples include: sensitive internal communications, any material that includes non-public personally identifiable information, proprietary data such as NWO performance data, salary data, and staff performance evaluations.

- Corporate record – information owned, created, collected, stored or received by NeighborWorks America in the ordinary course of business. This includes emails, memoranda, grant agreements, compliance reviews, financial records, publications, and data compilations. Records are "physical records" when they are in paper format, and are "electronic records" or "digital records" when they are in a format enabled by information technology resources (including electronic media).
- Data Collection System – any of the technology-enabled systems or applications owned, controlled, or administered by NeighborWorks America that accept and store information.
- Division Document Manager – a position appointed by the Senior Vice President of each Division, who receives specific training and is responsible for organizing that Division's records management plan, liaising to access resources needed to implement that plan, and monitoring for compliance with this policy.
- Personally Identifiable Information ("PII") – information about a person (such as name, date of birth, account numbers) that can be used to identify that individual. NeighborWorks America uses the NIST definition of PII and requires that non-public PII be afforded special protections as it is handled, stored, and transmitted by NeighborWorks America. (See Section VI below.)
- Records Management – the activities that control the creation, distribution, access, destruction, and transmission of information.
- Retention Period – the defined amount of time a Corporate record is to be stored, after which it should be destroyed in a manner appropriate to its format and content. Retention periods for each type of document are stated in the Record Retention Schedule at Appendix A.

III. Roles and Responsibilities

a. Division Document Manager

Each Division will have an assigned Document Manager, who is responsible for working with the staff of that Division to design and implement a records management plan consistent with this policy, including: coordinating the retention and destruction of records, coordinating responses to litigation holds, ensuring the correct controls are in place for confidential and personally identifiable information, seeking guidance from OGC for records that don't fit within this policy, managing shared drive space of that Division, coordinating an annual file clean-up effort at the Division level, and acting as the single point of contact for off-site document storage.

b. Director of IT Operations

The Director of IT Operations is responsible for implementing data and document management policies and technical controls on digital records on NeighborWorks America's managed network. This business unit has administrative control of electronic documents and files that are on NeighborWorks' managed network.

c. IT&S Director of Security & Compliance

This position is responsible for advising on safeguards for handling, storing, destroying, and transmitting confidential records and personally identifiable information. This position is also available to examine the architecture of information systems for security, soundness, and risk.

d. Office of General Counsel ("OGC")

The Office of General Counsel is responsible for interpreting this policy and its application. OGC is available to assist Senior Vice Presidents and their designated Division Document Managers in applying this policy to the corporate records of their Division. OGC will provide special guidance for Divisions whose business needs are not met by this policy or whose Corporate records are not addressed by the Retention Schedule of this policy. OGC will also consider and grant requests for exceptions from this policy. At least once per year, each Division Document Managers will meet with the Office of General Counsel to review this policy and the Division-level plan for complying with it.

e. Senior Vice President.

The Senior Vice President is the owner of the Confidential Information created and handled by their Division, and as such is responsible for ensuring access controls are implemented, monitored, and maintained. And providing support to their appointed Document

f. Systems Administrator

Each data collection system will be assigned a System Administrator that is responsible for coordinating/providing access requests to the system and ensuring that the access to Confidential Information is restricted to those with proper authority.

IV. Records Management

a. Classification

Depending on its content, a record can be classified as public, internal use only, or confidential. The classification of a record determines how it should be stored, destroyed, reproduced, and transmitted.

- Public records – Corporate records that have been approved for release to the general public or could be released to a member of the public without causing harm. Examples include: web pages, annual reports, catalogs, funding announcements, press releases, policies, mass communications to Grantees.
- Internal use only records – Corporate records that are intended only for use only within NeighborWorks America, so that unauthorized disclosure outside of NeighborWorks America would be inappropriate or inconvenient. Examples include: sensitive communications, recommendation memos, NWO performance data, and program evaluation data.
- Confidential records – Corporate records are subject to increased handling and protection requirements because they contain sensitive or private information so that their disclosure outside of NeighborWorks America would be illegal, improper, or damaging. Examples of Confidential records include: sensitive internal communications, any material that includes non-public personally identifiable information, and proprietary data such as NWO performance data. The requirements for handling PII and private information are located at Section VI below.

b. Labeling Records

Some records should be labeled to ensure they are handled properly and protected from unintended disclosure.

Classification	Labeling Physical Records	Labeling Electronic Records
Public Records	No label required	No label required
Internal Use Only Records	No label required	No label required
Confidential Records	Label as "Confidential" at the bottom of each page, or on exterior of each file or box	Label as "Confidential" at the bottom of each page and in the file name.

c. Storing Records - Onsite

Materials that are obsolete, duplicative, extraneous, or drafts of an established final should be destroyed immediately. All other materials should be retained and destroyed according to the Records Retention Schedule at Appendix A to avoid the inference that material was destroyed in anticipation of a specific problem.

If the Classification is …	You should store the Physical Records by …	You should store the Electronic Records by …
Public Records	No special storage requirements.	No special storage requirements.
Internal Use Only Records	Store and control records properly.	Store and control properly; consult with ITS Director of Security & Compliance if you wish to implement storage methods such as encryption, password protection, or other methods.
Confidential Records	Ensure that confidential information is secure when not in use (ex: in a locked file drawer or locket closet)	Store securely; consult with ITS Director of Security & Compliance to determine appropriate storage methods – which may include encryption, password protected files, or other methods.

d. Storing Records - Off Site

Physical Corporate records that are no longer in active use can be sent to NeighborWorks' approved off-site storage facility. The storage and retrieval of boxes from the off-site storage facility is coordinated by Administrative Services Division. A box of Corporate records can only be sent to off-site storage if the box's transmittal form includes the name of the transmitting Division and contact, a description of the contents, and a destruction date consistent with the Records Retention Schedule at Appendix A. Administrative Services Division maintains an index of all boxes stored at the off-site storage facility and – together with OGC – will periodically review the index and recommend that abandoned boxes be destroyed or returned to the transmitting Division for inspection.

e. Destroying Records

As a general rule, Corporate records should be retained for as long as required by applicable law and as long as reasonably necessary to assure their availability when needed for a business purpose. Materials that are obsolete, duplicative, extraneous, or drafts of an established final should be destroyed immediately. All other materials should be retained and destroyed consistent with the Records Retention Schedule at Appendix A so as to avoid the inference that any material was destroyed in anticipation of a specific problem.

If the Classification is …	You should destroy the Physical Records by …	You should destroy the Electronic Records by …
Public Records	Trash bins	Delete*
Internal Use Only Records	*Recommended* disposal via secure bins.	Delete*
Confidential Records	*Required* disposal and shredding via secure bins. Records at off-site storage can be securely destroyed by that vendor.	Delete, empty recycling bin immediately*

* Consult IT&S when destroying or wiping electronic media devices such as USB drives, CDs, and external storage drives. Those devices must be sanitized or destroyed by authorized personnel.

f. Reproducing Records

The following controls are intended to help protect Corporate records from unintended disclosure, both internally and externally.

If the Classification is …	You should reproduce the Physical Records by …	You should reproduce the Electronic Records by …
Public Records	No limitations	No limitations
Internal Use Only Records	Copies made by authorized staff only	Copies made by authorized staff only
Confidential Records	Reproduction requires approval of the SVP of the Division that controls that data; copies made in a secure printing environment by authorized staff only; these records should never be left on printers, on desks, in unlocked drawers, or out in public areas	Copies made by authorized staff only; requires approval of the SVP of the Division that controls that data

g. Transmitting Records

Information is particularly vulnerable to disclosure when it is being transmitted. For that reason, the following requirements apply when transmitting Corporate records.

If the Classification is …	You should transmit the Physical Records by …	You should transmit the Electronic Records by …
Public Records	No restrictions	No restrictions
Internal Use Only Records	Sent by authorized staff only If sending internally, use an inter-office envelope If sending externally, use a sealed envelope	Sent by authorized staff only; send by NW email system (@nw.org)
Confidential Records	If sending internally, use a sealed envelope inside an inter-office envelope If external mail, use a sealed envelope and deliver by hand or send by certified mail or courier with signature required (such as Fed Ex). Transmission by authorized staff only; requires approval of the SVP of the Division that controls that data	Consult with ITS Director of Security & Compliance to determine appropriate transmission method – which may include encryption or use of a secure file transfer site. If sent by email, the following language must be included: "This email transmission contains information which may be Confidential. The information is intended to be for the sole use of the individual or entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution or other use of the contents of this transmission is strictly prohibited. If you have received this email in error, please notify the sender immediately."

h. Abandoned records

Due to factors such as staff turnover, program wind-down, and divisional restructuring, Corporate records sometimes are not managed according to the proper protocol. For example, digital records that have not been accessed in several years and physical records improperly sent to off-site storage might be considered abandoned. Where Corporate records are believed to be abandoned, they should be processed as follows: (1) identify the division from which the record (or file or box) originated; (2) ask the SVP of that division to approve the destruction of that record or assign responsibility for the management to current staff. If no division or employee can be identified as the originator of that record, then the management and destruction of that record will be decided by OGC on a case by case basis.

V. Litigation Holds

The Office of General Counsel is authorized to override this policy by issuing a "Litigation Hold." A litigation hold is an order not to destroy, tamper with, or dispose of Corporate records that pertain to the subject of a lawsuit, audit, FOIA request, or investigation (whether actual or potential). When OGC issues a litigation hold, it will provide details regarding scope, key words to guide the effort, and additional instructions about whether/how to segregate these materials. OGC will also follow-up to inform staff when a litigation hold is lifted.

VI. Special Requirements of Handling Personally Identifiable Information ("PII")

All Divisions that create, collect, handle, manage, or transmit non-public personally identifiable information have a heightened obligation to keep that information safe from unintended disclosure. Personally Identifiable Information ("PII") is information that can be used to trace a specific person's identity – whether alone or when linked with other data. NeighborWorks America uses the PII definition promoted by the National Institute of Standards & Technology ("NIST"). The NIST definition is the industry standard. It is available in full online[1] and excerpted here.

> PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace and individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Examples of PII include, but are not limited to:
>
> - Name, such as full name, maiden name, mother's maiden name, or alias
> - Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
> - Address information, such as street address or email address
> - Personal characteristics, including photographic image, especially of face or other identifying characteristic, fingerprints, handwriting, or other biometric data (eg, retina scan, voice signature, facial geometry)
> - Information about an individual that is linked or linkable to one of the above (eg, date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, financial information).
>
> -- *Guide to Protecting the Confidentiality of Personally Identifiable Information*.
> *NIST, Special Publication 800-122*
> *April 2010*

In practical application, an entire client-level record in NeighborWorks' possession should (as a unit) be deemed PII if it contains any of the following fields: first name, last name, street address, or any unique identifying numbers. Common examples of unique identifying numbers are: SSN, credit card numbers, account numbers, client ID numbers, and loan numbers.

a. Unintended Receipt of PII.

Where PII is inadvertently or improperly received by a NeighborWorks America staff person, he or she shall, where possible and as appropriate: (1) notify the sender that the PII was received, (2) inform sender of the proper method by which PII should be transmitted, (3) re-route the PII to the intended recipient; and/or (4) immediately destroy the subject PII in accordance with this policy.

b. Privacy Policy.

It is the policy of NeighborWorks America not to collect more PII than is necessary for the stated purpose, not to store PII for longer than necessary, and to limit access to (and distribution of-) PII on a "need to know basis" to staff who require that access to perform their required job tasks. The Senior Vice President of each Division is responsible for surveying the PII under their control, developing the protocol by which their staff are granted access to view or handle non-public PII (and by which that access is removed when the staff no longer needs it), and reviewing the managed access levels to

[1] http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf at Section 2-2

ensure they are current. OGC will provide a template on its Inside NW page to help SVPs in creating their Division-specific plans.

c. Access Controls.

When files or data systems that are owned or administered by NeighborWorks contain Confidential Information (including personally identifiable information), access controls must be implemented to deny unauthorized access. The SVP of the Division that owns the Confidential Information (or is in possession of Confidential Information) is responsible for ensuring that access controls are implemented, maintained, and monitored. Access controls will be maintained at the Division level, with support from Information Technology & Services Division.

Access to Confidential Information is granted in three steps at the Division level:

- STEP 1: Request made / business need documented. Staff member submits to the System Administrator a request for access to file/system that contains Confidential Information. The request must include description of the business need that justifies access and the date on which that need will expire.
- STEP 2: SVP approves access. System Administrator confirms (and documents) that the staff person has current clearance from HR to have access. SVP approves – in writing – the request for access to the system.
- STEP 3: Maintain access list. System Administrator maintains the request for access forms and confirms quarterly with SVP that the list of those staff with the expanded view is accurate and that those staff are still eligible to have access.

The NeighborWorks staff who are granted access to view or handle Confidential Information must meet two requirements (1) clearance by Human Resources Division to handle records according to established protocol, which includes a background check; and (2) satisfy requirements of IT&S Division, which might include annual training and annually signing an agreement to abide by NeighborWorks' security standards for handling Confidential Information.

d. Special Requirements for Storing Medical and Health Information.

Files that contain medical or health information about any current or former employee must be stored separate and apart from the individual's normal personnel file, in a locked storage area accessible only by approved personnel. Such records are confidential (as defined at Section IV above) and should be treated consistent with the records management practices in Section IV.

VII. Exceptions

Requests for exceptions from the Information Governance Policy must be submitted in writing to the Office of General Counsel, and should include: (1) description of the situation; (2) proposed alternative to what is required by the Information Governance Policy; and (3) explanation of how the basic objectives of the Information Governance Policy will be met. Standardizing records management protects NeighborWorks from the inference of improper destruction and protects confidential information from unintended disclosure. Therefore, exceptions shall not be routinely granted.

VIII. Enforcement

Violations of this policy – particularly those that involve unintentional disclosure of Confidential Information – should be reported to the Deputy General Counsel and SVP – Information Technology & Systems consistent with the Incident Response Plan and will be handled in accordance with the Incident Response Plan. Violations of this policy may result in disciplinary action.

Addendum Include within Technology Service Provider Agreements

Security of NeighborWorks America (NW) Data within Technology Service Provider Environment

1. **Security Measures.** "**Technology Service Provider"** agrees to implement data security measures that are consistent with industry best practices and standards so that it:
    a) Protects the privacy, confidentiality, integrity and availability of NW data;
    b) Protects against accidental, unauthorized, unauthenticated or unlawful access, copying, use, processing disclosure, alteration, transfer, loss or destruction of NW data;
    c) Complies with all applicable federal and state laws, rules, regulations, directives and decisions that are relevant to the handling, processing, and use of NW data in accordance with this Agreement.

2. **Risk Assessments.** "Technology Service Provider" shall perform comprehensive internal and external risk assessments (at least annually and/or after major changes) and provide results to NW.
    a) "Technology Service Provider" agrees to send us their completed ***Third Party – Information Gathering Questionnaire*** to NW for review prior to executing this agreement.
    b) "Technology Service Provider" agrees to provide NW with an information technology assessment and/or audit report as to provide an understanding of "Third Party" security controls and requirements in place currently. E.G. - System and Organization Controls (SOC) Type 2 Report
    c) Upon request by NW, "Technology Service Provider" agrees to provide NW with the results of their most recent vulnerability scans or penetration test conducted for review.
    d) Upon request by NW, "Technology Service Provider" agrees to allow NW or a mutually acceptable third party to conduct an information security control review as it pertains to the scope of service outlined within the agreement.

3. **Organizational Security Responsibility.** "Technology Service Provider" shall assign responsibility for information security management to a senior management officer or a designated data steward to maintain the security of NW data. "Technology Service Provider" will provide this point of contact information to NW. "Technology Service Provider" agrees to return NW data or provide NW with evidence of destruction of NW data upon end or termination of this agreement. This includes hard copy and all forms of electronic data including backups and archives. Upon request, "Technology Service Provider" will provide NW with their most current Privacy Policy.

4. **Third Party or Shared Hosting Service Provider.** If "Technology Service Provider" uses any third party or shared hosting service provider, the Technology Service Provider must require that the third party protects NW data to at least the same level as the service provider. NW requests to receive independent security assessment reports (e.g. – ISO 2700x Certification and Report, SSAE 16 SOC Reports, Shared Assessment Program – Agreed Upon Procedures Review, PCI DSS Report on Compliance, or IT Audit – External) from those parties and\or hosting service

providers. The third party must protect each entity's hosted environment and data. NW reserves the right to move NW data within its own data center at its discretion.

5. **Data Retention and e-Discovery**. Technology Service Provider s will provide means for NW to enforce its data retention policies on all data over which Technology Service Provider has custody or will enforce data retention policy on behalf of NW. This will require the Technology Service Provider to provide assurances that data including metadata and events when appropriate are retained for the duration of the retention period. It also requires the Technology Service Provider to provide assurances that all copies including backups and archives of expired data are thoroughly destroyed. NW program offices will coordinate with the Technology Service Provider to identify data which is in scope for retention and destruction. Technology Service Provider further agrees to comply with all reasonable e-Discovery requests.

6. **Classification of generated, collected and aggregated data.** When applicable, Technology Service Providers who generate, collect or aggregate data on behalf of NW shall coordinate with the program office to ensure that all new data or new data combinations which satisfy definition of Personally Identifiable Information (PII), as found in NeighborWorks America Award/Contract – Section H. Special Contract Requirements, are appropriately classified and protected. Generated data includes data which is produced by analysts or automatically by algorithms.

7. **Logging and event generation for applications.** Technology Service Provider and NW program office shall coordinate to identify security relevant data and activities in all applications. Technology Service Provider shall ensure that events are generated when sensitive data is accessed and security relevant activities take place. Technology Service Provider shall ensure that security events are logged, can be accessed by NW upon request, and that logs are retained as specified in Data Retention. Preferably through API (Application Program Interface) capabilities and/or syslog forwarding into NW's Security Incident & Event Monitoring (SIEM) solution.

8. **Business Continuity (BCP) & Disaster Recovery (DRP) Planning.** In the event the Technology Service Provider ceases to provide the service, the Technology Service Provider shall provide sufficient advanced warning to facilitate the exportation of data and work product to NW. NW may require regular exportation or archiving of data and work product to satisfy NW's BCP / DRP plans.

9. **Security Incident / event notification.** Technology Service Provider shall notify NW of any security incident or event which has material effect on NW data within 72 hours of discovery. Technology Service Provider shall have in place a defined and practiced IR plan and procedures. NW reserves the right to prosecute culpable parties at its discretion when NW data is impacted. Technology Service Provider agrees to assist with all reasonable requests from NW, NW's incident response contractors or law enforcement in all necessary investigations.

10. **Jurisdiction of data storage.** Technology Service Provider shall ensure that all data stored and processed on behalf of NW is kept within the Jurisdiction of the United States of America. Data shall not be transmitted outside this jurisdiction at any time without authorization and formal approval from NeighborWorks America.

11. **IDP (Identity Provider) and Single Sign On (SSO) Integration**. Technology Service provider shall ensure that identity authentication and access to application can be through Single Sign-on integration using the current standards (e.g. - Security Assertion Markup Language: SAML)for exchanging authentication and access authorization identities between security domains . Technology service provider should have the ability to integrate Single Sign-On access for NW employees - Workforce (WF) and customer identity access management (CIAM).