SOLICITATION, OFFER AND AWARD

1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE OF PAGES
		1 | 20

2. CONTRACT NUMBER	3. SOLICITATION NUMBER	4. TYPE OF SOLICITATION	5. DATE ISSUED	6. REQUISITION/PURCHASE NUMBER
	RFP-24-0027	☐ SEALED BID (IFB) ☒ NEGOTIATED (RFP)	06/18/2024	

7. ISSUED BY	CODE	8. ADDRESS OFFER TO (If other than Item 7)
NEIGHBORWORKS AMERICA INFORMATION TECHNOLOGY SERVICES 1255 UNION ST NE SUITE 500 WASHINGTON DC 20002	ITS	

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder".

SOLICITATION

9. Sealed offers in original and _____ copies for furnishing the supplies or services in the Schedule will be received at the place specified in Item 8, or if hand carried, in the depository located in _____ until 1700 ET (Hour) local time 07/19/2024 (Date)

CAUTION: LATE Submissions, Modifications, and Withdrawals: See Section L, Provision No. 52.214-7 or 52.215-1. All offers are subject to all terms and conditions contained in this solicitation.

10. FOR INFORMATION CALL:	A. NAME	B. TELEPHONE (NO COLLECT CALLS)			C. E-MAIL ADDRESS
		AREA CODE	NUMBER	EXT.	
	Greg Smiling	202	683-6617		Gsmiling@nw.org

11. TABLE OF CONTENTS

(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES	
☒	A	SOLICITATION/CONTRACT FORM	3	☒	I	CONTRACT CLAUSES	17
☒	B	SUPPLIES OR SERVICES AND PRICES/COSTS	3			PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
☒	C	DESCRIPTION/SPECS./WORK STATEMENT	5	☒	J	LIST OF ATTACHMENTS	17
☒	D	PACKAGING AND MARKING	5			PART IV - REPRESENTATIONS AND INSTRUCTIONS	
☒	E	INSPECTION AND ACCEPTANCE	6	☒	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	19
☒	F	DELIVERIES OR PERFORMANCE	7				
☒	G	CONTRACT ADMINISTRATION DATA	7	☒	L	INSTRS., CONDS., AND NOTICES TO OFFERORS	20
☒	H	SPECIAL CONTRACT REQUIREMENTS	16	☐	M	EVALUATION FACTORS FOR AWARD	

OFFER *(Must be fully completed by offeror)*

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within _____0_____ calendar days (60 calendar days unless a different period is inserted by the offeror) from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the price set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT *(See Section I, Clause No. 52.232.8)*	10 CALENDAR DAYS (%)	20 CALENDAR DAYS (%)	30 CALENDAR DAYS (%)	CALENDAR DAYS (%)

14. ACKNOWLEDGEMENT OF AMENDMENTS *(The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related documents numbered and dated):*	AMENDMENT NO.	DATE	AMENDMENT NO.	DATE

15A. NAME AND ADDRESS OF OFFEROR	CODE	FACILITY	16. NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER *(Type or print)*

15B. TELEPHONE NUMBER			15C. CHECK IF REMITTANCE ADDRESS	17. SIGNATURE	18. OFFER DATE
AREA CODE	NUMBER	EXT.	☐ IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE.		

AWARD *(To be completed by government)*

19. ACCEPTED AS TO ITEMS NUMBERED	20. AMOUNT	21. ACCOUNTING AND APPROPRIATION

22. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:	23. SUBMIT INVOICES TO ADDRESS SHOWN IN *(4 copies unless otherwise specified)*	ITEM
☐ 10 U.S.C. 2304 (c) ( ) ☐ 41 U.S.C. 3304 (a) ( )		

24. ADMINISTERED BY *(If other than Item 7)*	CODE	25. PAYMENT WILL BE MADE BY	CODE

26. NAME OF CONTRACTING OFFICER *(Type or print)*	27. UNITED STATES OF AMERICA *(Signature of Contracting Officer)*	28. AWARD DATE

IMPORTANT - Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice.

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Delivery Location Code: WASHINGTON NEIGHBORWORKS AMERICA 1255 UNION ST NE SUITE 500 WASHINGTON DC 20002 USA Period of Performance: 10/01/2024 to 09/30/2029				

Section B - Supplies or Services/Prices

Contract Line Item	Description	Unit	# of Units	Unit Price	Extended Price
0001A	Base Year – Services as Specified in the RFP Period of Performance: 10/01/2024 – 09/30/2025	**Monthly**	12	$	$
0001B	Base Year – Implementation Period of Performance: 10/01/2024 – 02/01/2025	**One Time Fee**	1	$	$
0002	Option Period One - Services as Specified in the RFP Period of Performance: 10/01/2025 – 09/30/2026	**Monthly**	12	$	$
0003	Option Period Two - Services as Specified in the RFP Period of Performance: 10/01/2026 – 09/30/2027	**Monthly**	12	$	$
0004	Option Period Three - Services as Specified in the RFP Period of Performance: 10/01/2027 – 09/30/2028	**Monthly**	12	$	$
0005	Option Period Four - Services as Specified in the RFP Period of Performance: 10/01/2028 – 09/30/2029	**Monthly**	12	$	$
Total Contract Price					*$*

Section C - Description/Specifications (Scope)

NeighborWorks America seeks a vendor to provide the following services for the upkeep and maintenance of CounselorMax®:

To meet the need of NeighborWorks America, IT&S seeks a vendor who can provide ongoing, high-quality, high availability support, maintenance and software development services for

CounselorMax®. CounselorMax® is a housing counseling services client management system owned and operated by NeighborWorks®. CounselorMax® is used by over 700 housing counseling organizations across the country and throughout the NeighborWorks® Network. As such it's not just a network only service but an industry wide service that NeighborWorks® makes available to the community development/housing counseling industry. The CounselorMax® software application requires a software support and development vendor that can support the functioning and effectiveness of the application under the direction of NeighborWorks® internal staff. In addition, the vendor will provide the NeighborWorks Compass project with support developing the NeighborWorks Quarterly Production report compliance module, will assist with developing a tool for migration of data from CounselorMax to Compass, and will provide input on development of a bridge between Compass and NeighborWorks America's ORS system.

- Software Development Services: Ongoing software development services to NeighborWorks America to add/change features and functionality as needed and requested by NeighborWorks America staff to enhance and update the CounselorMax on-line software application. Typically, NeighborWorks America allots a set amount of dollars for CounselorMax development and maintenance to meet anticipated development, support and maintenance needs throughout the year.
- Software Support Services: Ongoing technical support services to NeighborWorks America staff to address support issues and bug fixes and to serve as a technical resource for system design, enhancement and implementation questions and solutions. We are seeking a partner that does more than passively respond to NeighborWorks America staff suggestions and takes a proactive approach to suggest improvements and enhancements that will make the application more efficient and effective at meeting its business and technical objectives. At NeighborWorks America staff request, provide "tier 3" support for software bug fixes and other software related support.
- Software Maintenance Services: Ongoing maintenance for CounselorMax functionality as required. Maintenance tasks include maintaining Web Services and other connectivity functionality, reviewing and analyzing logs and errors, technical documentation services and other related activities as requested by NeighborWorks America staff to maintain compliance with reporting and other requirements. The vendor shall acknowledge and provide an estimated resolution timeframe within 4 business hours of receipt of the problem.
- The vendor shall provide these services, as required between 7:00 AM and 10:00 PM (EST) Monday through Friday. There may be instances when support will be required on weekends or holidays. In addition, software releases or other updates may require work weekends or evenings/nights and the successful vendor should be willing and available to work during these instances.
- Migration/Implementation Services: to provide data migration tool building, data migration, and implementation services for converting legacy CounselorMax organizations to NeighborWorks Compass 2.0. The chosen vendor will develop custom data migration tools, ensure data integrity during extraction and transformation, and collaborate on seamless integration for NeighborWorks Compass 2.0.

Additional Requirements

- High-quality technological support from vendor.
- Support, Maintenance, and software development for the CounselorMax product.
- Support of the functioning and effectiveness of the application under the direction of NeighborWorks America internal staff.
- Support developing the NeighborWorks Quarterly Production report compliance module.
- Developing a tool for migration of data from CounselorMax to Compass.
- Will provide input on development of a bridge between Compass and NeighborWorks America's ORS system.
- Software development, support, and maintenance services.

- Technical documentation services and other related activities as requested by NeighborWorks America staff to maintain compliance with reporting and other requirements.
- Tier 3 support for the CounselorMax product, when needed, for software bug fixes and other software related support.
- Provide access to staff that can reliably assist NeighborWorks® support staff to troubleshoot issues on an as-needed basis when NeighborWorks® staff is unable to address the issues independently.
- Perform resolution of all Tier III support issues within 48 hours of acknowledgement of receipt or by mutually agreed upon timeframe if both parties agree that the specific incident requires more research, coding or resolution time.
- Perform all "Bug Fixes" as required in accordance with the accepted Service Level Agreement.
- Provide ongoing maintenance to the application as needed. Maintenance tasks include but are not limited to: a. Updating table values that change due to regulatory changes or other published updates (e.g., income tables, MSA tables, etc.) b. Reviewing error logs and proactively addressing issues in consultation with NeighborWorks® staff as needed. c. Other maintenance tasks as requested by NeighborWorks® staff.
- Improving or creating new features and functionality as requested by the business team to keep the CounselorMax application competitive in the marketplace.
- Perform development tasks required to keep CounselorMax compatible with the latest HUD HCS ARM ICD as published by HUD technical documentation.
- Provide development services to keep CounselorMax compliant with the NeighborWorks Quarterly Production report requirements and the Financial Capabilities reporting requirements.
- Assist with the conversion and onboarding of new clients, including data migration as needed.
- Provide other development and maintenance tasks that may be required during the contract period as requested by NeighborWorks® staff.
- Reporting statuses given during weekly meeting.
- Provide data migration tool building, data migration, and implementation services for converting legacy CounselorMax organizations to NeighborWorks Compass 2.0.
- Develop custom data migration tools, ensure data integrity during extraction and transformation, and collaborate on seamless integration for NeighborWorks Compass 2.0.
- Vendors must provide a minimum of 3 references of similar project experience.
- Proposals should be no longer than 10 Pages, excluding Cover Page.

Section D - Packaging and Marking (Deliverables)

Deliverable/Milestone	Delivery Method	Due Date
Kick Off Meeting	Virtual	Two weeks after Award Date
Monthly Reports	Email or Electronic Delivery	30th of every month
Bi-Weekly Meeting	Virtual	Every two weeks (Ongoing)
Ad Hoc Reports	Email	As Requested

Section E - Authority of NeighborWorks America Personnel

Point of Contact

The Point of Contact (POC) for this award is responsible for inspecting and approving invoices and – if required – accepting deliverables or services rendered. The POC does not have authority to take any action, either directly or indirectly, that would modify pricing, quantity, place of performance,

delivery schedule, or any other terms and conditions of this award, including taking effort which goes beyond the scope of this award. The POC for this award is: Jayme Hardy, jhardy@nw.org.

Contracting Officer

The Contracting Officer (CO) administering this award is the only person authorized to approve modifications in any requirements of this Contract. Notwithstanding any provisions contained elsewhere in this Contract, authority to amend this Contract on behalf of NeighborWorks America belongs solely to the CO. If Contractor effects any modifications at the direction of any person other than the CO, the modification will be considered to have been made without authority and no adjustment will be made to the Contract or contract price as a result thereof. The CO for administration of this Contract is: Jayme Hardy, jhardy@nw.org.

Section F - Performance Period & Options to Extend

Performance Period

This contract period of performance inclusive of options shall not exceed 10/1/2024 to 9/30/2029, unless otherwise terminated in accordance with the terms and condition of this Contract, as indicated below:

Base Year: 10/1/2024 to 9/30/2025

Option Year 1: 10/1/2025 to 9/30/2026

Option Year 2: 10/1/2026 to 9/30/2027

Option Year 3: 10/1/2027 to 9/30/2028

Option Year 4: 10/1/2028 to 9/30/2029

Authority to Exercise the Option to Extend the Performance Period

NeighborWorks America reserves to the right unilaterally to exercise the options outlined below without further competition.

Option to Extend

NeighborWorks America may exercise its option to extend the term of this Contract by providing written notice to the Contractor by one (1) day before the expiration of the contract period (inclusive of exercised option periods) provided that NeighborWorks America also gives the Contractor a preliminary written notice of its intent to extend 30 days prior to previous period of performance end date. Issuance of that preliminary written notice does not commit NeighborWorks America to an extension.

If NeighborWorks America exercises this option, the extended contract shall be considered to include this option clause.

The total duration of this Contract, including the exercise of any options under this clause, shall not exceed 5 years.

Standard Option to Extend for up to six (6) months

NeighborWorks America may require continued performance of any services within the limits and at the rates specified in the Contract. The total extension of performance under this option provision shall not exceed six (6) months. The Contracting Officer may exercise the option by providing written notice to the Contractor no later than 30 days prior to contract end.

Section G - Contract Administration

Contract Type

NeighborWorks America contemplates award of a(n) Firm-Fixed Price, Level of Effort.

Modifications to the Contract

The Contracting Officer (CO) administering this Contract is the only person authorized to approve modifications to any terms of this Contract. The Contractor shall not comply with any order or request altering the terms of this Contract unless it is issued in writing and signed by the CO, or is made pursuant to other specific authority described in this Contract. Modifications to the Contract will be deemed effected when countersigned by Contractor and returned to the CO administering this Contract. See also, Section E.II.

Submission of Invoices

Contractor is expected to submit a final invoice to the Corporation within 30 days after completion of all the Services (including Deliverables) set forth in the Contract/Task Order. The Corporation may deduct 30% of the fee if the final invoice is not received within six (6) months of the completion of all Services and reserves the right to void payment of any invoices that are not submitted within one year of the execution date of such Contract/Task Order. All invoices must contain the Contract Number, Task Order Number, and performance period and be submitted to CompassBilling@nw.org. As a 501(c)(3) registered nonprofit corporation, NeighborWorks America is exempt from Federal and State taxes. The tax-exempt form is available upon request.

Vendor Automated Clearing House (ACH) Payment Policy

NeighborWorks America pays its vendors via ACH Electronic Payment. Before a contract is executed, the Contractor is required to provide required payment information to NeighborWorks America using a form link emailed from NeighborWorks America (financecustomerservice@nw.org). The Contractor's legal name, tax ID number, current year W-9, and bank account information must all be confirmed as correct before a contract is finalized.

Section H - Special Contract Requirements

Key Personnel

Contractor shall assign key personnel to perform this Contract (Contractor Must Complete):

Name of Key Personnel	Role/Responsibility under this Contract
1.	
2.	

3.	
4.	
5.	

Key Personnel

A. Contractor shall assign key personnel to perform this Contract.

B. No substitution of key personnel shall occur except by the following process:

1. Timing. During the initial ninety (90) days of performance, Contractor shall make no substitutions of key personnel unless the substitution is necessitated by illness, death, or termination of employment. The Contractor shall notify the Contracting Officer within seven (7) calendar days after the occurrence of any of these events and provide Substitution Information below. After the initial ninety (90) day period, Contractor shall submit Substitution Information to the Contracting Officer at least fifteen (15) days prior to making any permanent substitutions.

2. Substitution Information. If Contractor proposes to substitute key personnel, it must provide a detailed explanation of the circumstances necessitating the proposed substitutions, complete resumes for the proposed substitutes, and any additional information requested by the Contracting Officer (collectively, "Substitution Information"). Proposed substitutions shall have comparable qualifications to those of the key personnel being replaced. The Contracting Officer will notify the Contractor within fifteen (15) calendar days after receipt of all required information of the decision on substitutions. The Contract will be modified to reflect any approved modifications of key personnel.

Compliance with Laws & Equal Employment Opportunity

Both NeighborWorks America and Contractor shall comply with all applicable federal laws, state laws, local laws and ordinances, regulations, and codes in performance of its obligations under this Contract. Contractor shall not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, disability, or national origin.

Confidentiality and Information Security

A. Confidentiality & Non-Disclosure. In performance of this Contract, NeighborWorks America and Contractor may be granted conditional access to confidential or proprietary information belonging to the other, including documents, methodologies, technical knowledge, and sensitive information the loss, misuse, or unauthorized disclosure of which could adversely affect the other party's interests (collectively, "Protected Information").

1. Both NeighborWorks America and Contractor shall take reasonable care to safeguard Protected Information from unauthorized use, modification, or disclosure. At a minimum, such reasonable care shall include:

a. Restricting use of Protected Information to performance of this Contract;

b. Limiting access to Protected Information to those employees and agents who have a need to know such information for performance of this Contract;

c. Not divulging Protected Information to any person without prior written consent of the other party; and

d. Not using Protected Information for any commercial or other purpose than required for performance of this Contract.

2. Protected Information is and shall remain the property of the disclosing party, except where it is "Work Product" as defined by this Contract. Upon expiration or termination of this Contract, or upon the request of the disclosing party, all copies of Protected Information of the disclosing party shall be destroyed or returned to the disclosing party, at the disclosing party's discretion.

3. Protected Information does not include information that has become part of the public domain through no violation of these Contract terms, was developed independently by the other party, or was provided lawfully and independently to the receiving party by a third party not obligated to confidentiality or otherwise prohibited from transmitting such information.

B. Data Security. In order to protect the resources and sensitive data of NeighborWorks America, Contractor shall adhere to certain administrative and technical controls in performance of this Contract. These controls include the following minimum security requirements:

1. Contractor shall satisfy all security requirements and specifications for hardware maintenance, software maintenance, and developer personnel stated in the Scope of Work.

2. In the event of an actual or potential risk to information resources, Contractor shall contact NeighborWorks America Information Technology & Security Management.

3. Where required for Contract performance, NeighborWorks America shall grant Contractor access to its network or information technology systems, as outlined in the Scope of Work. Such access shall be the most restrictive capabilities and privileges needed to perform the Contract. Access shall be limited to a specific timeframe, after which such access will be reviewed for termination. Contractor agrees to access only those applications, systems, and data authorized for performance of this Contract. Contractor agrees to notify NeighborWorks America when various access types are no longer required.

4. If Contract performance requires that Contractor access sensitive information technology resources or data of NeighborWorks America, Contractor shall – at its own expense – undergo a minimum background investigation performed either by one of an approved list of vendors or by a firm approved by NeighborWorks America. Where contract performance requires access to particularly sensitive systems or information, NeighborWorks America may require that Contractor undergo a more intensive background investigation.

5. Where appropriate, NeighborWorks America may also require that Contractor receive orientation on proper use of NeighborWorks America technology resources, install periodic security updates, and sign a written acknowledgement that it has read and understood NeighborWorks America's security requirements.

6. Contractor shall comply with all applicable state and federal laws regarding data security and use of technology resources.

C. Personally Identifiable Information. NeighborWorks America's Information Governance Policy applies to all third parties that have access to the information assets owned, created, collected, managed, stored, and disseminated by NeighborWorks America, including Personally Identifiable Information ("PII"). When handling PII, Contractor shall strictly comply with that policy's increased handling and protection requirements of confidential information.

1. PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. PII includes personal identification numbers like social security numbers, passport numbers, and driver's license numbers; tax forms; financial account or credit card numbers; mortgage information; loan numbers; full name, maiden name, mother's maiden name, or alias; address information, street address or email address (when linked with other personally identifiable information); personal characteristics, including photographic image; information identifying personally owned property, such as vehicle registration number, title number, or related information; information about an individual that is linked or linkable to one of the above (date of birth, place of birth, race, etc); employment, human resources, medical, and educational information.

2. NeighborWorks America mandates the following controls for PII in the following formats:

a. Physical Information - must be labeled "Confidential" at the bottom of each page, stored securely when not in use, and discarded via shredding and secure bins.

b. Electronic Information - must be labeled "Confidential" at the bottom of each page, accessed only with proper authorization from NeighborWorks America, and stored securely according to the requirements specified by NeighborWorks America.

c. Information Distribution - must be done using a sealed envelope inside an internal mail envelope when internal; done using a plain sealed envelope delivered by hand, by courier, or by registered mail when external; and done by a secure method authorized by NeighborWorks America when electronic.

d. Information Reproduction - must be done only with proper authorization from NeighborWorks America.

D. Scope and Enforcement.

1. The terms and conditions related to Information Security herein shall apply both during the Contract period and at all times thereafter.

2. Breach of the terms and conditions related to Information Security may cause the other party irreparable harm, so that the remedies available at law would not make the injured party whole. Accordingly, the injured party shall be entitled, without the requirement of posting a bond or other security, to equitable relief, including injunctive relief and specific performance. Such relief shall be in addition to, and not in lieu of, the other remedies available to injured party under this Contract or under law.

Conflicts of Interest

General

1. Duty to Disclose. Contractor agrees to make an immediate and full disclosure in writing to the CO at NeighborWorks America of facts surrounding any real or perceived conflicts of interest – including any changes to the facts that were previously disclosed by the Contractor prior to award of this

Contract. For example, such disclosure may be a description of action taken by Contractor to avoid or mitigate any resulting conflict of interest.

2. Waiver. Requests for waiver under this section shall be directed in writing to the CO and shall include a full description of the requested waiver and reasons in support thereof. If it is determined to be in the best interests of NeighborWorks America, the CO may grant such a waiver in writing.

3. Remedies. In the event of breach of any of the restrictions or misrepresentation of facts required to be disclosed concerning this Contract (including existence of an actual or potential conflict of interest at the time of award or after award), NeighborWorks America may terminate the Contract for default, disqualify Contractor from subsequent related contract work, and pursue other such remedies as may be permitted by law or this Contract.

4. Subcontracts. The financial, contractual, organizational and other interests of contractor personnel performing work under this Contract shall be deemed to be the interests of the Contractor for the purposes of determining the existence of a conflict of interest subject to this clause. Contractor shall include a clause, substantially similar to this section, including this paragraph, in all subcontracts and agreements related to performance of work under this Contract. Prior to award under this Contract of any subcontracts, Contractor shall determine whether interests disclosed by a subcontractor pose an actual or significant potential organizational conflict of interest. Where such a conflict of interest is identified, Contractor shall take actions to avoid, neutralize, or mitigate the organizational conflict to the satisfaction of the Contractor. If the conflict cannot be avoided or neutralized, the Contractor must obtain approval in writing from the Contracting Officer prior to entering into the subcontract.

Personal Conflicts of Interest.

1. Personal conflicts of interest exist where the financial interest, personal activity, or relationship of a Contractor or a NeighborWorks America employee could impair their ability to act impartially and in the best interest of NeighborWorks America when awarding or performing this Contract. (A de minimis interest is not within the scope of this policy.)

2. Contractor agrees to disclose to the CO in writing if it has a relationship with an employee, officer, Board member, or agent of NeighborWorks America that constitutes a personal conflict of interest. Such a conflict of interest would arise where the employee, officer, Board member, or agent is a member of his/her immediate family, is his/her partner, or an organization which employs or is about to employ any of the parties indicated herein, has a financial or other interest in or a tangible benefit from a firm considered for a contract.

3. Contractor shall avoid action which might result in or create the appearance of a NeighborWorks America employee, officer, Board member, or agent using NeighborWorks America's offices for private gain; giving preferential treatment to any organization or person; or losing independence or impartiality. Contractor agrees to notify CO in writing should an actual or apparent conflict of interest arise during the performance period of this contract.

Organizational Conflicts of Interest.

1. Organizational conflicts of interest exist where the Contractor's relationship with a parent company, affiliate, subsidiary, or successor makes it unable to be impartial – or to appear to be impartial – in performing work under Contract for NeighborWorks America.

2. In order to prevent situations where a Contractor may be biased because of its interests related to contract work performed for NeighborWorks America and to prevent any party from gaining unfair

competitive advantage over other parties by performing contract work, NeighborWorks America will impose the following restrictions on performance by the Contractor, its parent, affiliates, subsidiaries, and successors in interest:

a. To the extent Contractor prepares (in whole or in part) the specifications or Scope of Services to be used in a competitive acquisition, Contractor shall not be allowed also to participate in that Contract by providing those goods or services either as a prime contractor or subcontractor.

b. Contractor will not be awarded a contract to evaluate its own offer(s) for products or services or those of a competitor, without proper safeguards in place that ensure objectivity and protect the interests of NeighborWorks America. Contractor agrees to the terms and conditions set forth in the Scope of Services that are meant to ensure objectivity and protect the interests of NeighborWorks America.

c. Contractor will not be eligible to perform contracts (either as prime contractor or subcontractor) which stem directly from contracts where Contractor has provided advisory and assistance services, unless it is directed to do so in writing by the CO. Examples of advisory and assistance services are: providing outside perspectives on critical issues, advising on industry developments, providing expert opinion or special knowledge, developing alternative solutions to complex issues, improving organizational operations, and ensuring more efficient or effective operation of managerial or hardware systems.

3. Contractor shall be ineligible to participate in any capacity in NeighborWorks America contracts, subcontracts, or proposals (solicited and unsolicited) which stem directly from Contractor's performance of work under this Contract. This restriction shall apply to Awarded Vendor. This clause shall remain in effect for one (1) year after the completion of this Contract.

Contract Termination

Time is of the essence to this Contract. In certain circumstances, NeighborWorks America may terminate this Contract without being liable to the Contractor, except that NeighborWorks America shall pay the Contractor the reasonable value of satisfactory services or products delivered up to the date of termination.

A. NeighborWorks America may terminate the Contract in whole or in part, effective immediately, by written notice to Contractor if:

1. Contractor fails to begin or complete performance within the time period(s) specified in the Schedule;

2. Contractor breaches any term, condition, or provision of this Contract and fails to cure such breach within ten (10) days from the date it is notified by NeighborWorks America of the breach;

3. Contractor engages in fraud, willful misconduct, gross negligence, or misappropriation of funds or other property in the performance of its obligations under this Contract; or

4. Contractor becomes insolvent – including its making a general assignment for the benefit of creditors, having a receiver appointed, or being subject to any proceeding under bankruptcy or insolvency law whether domestic or foreign, voluntary or otherwise.

B. In addition to the foregoing, either party shall have the right to terminate the Contract without penalty by providing thirty (30) days written notice to the other party.

Impossibility

This clause is applicable to all NeighborWorks America supplies and services contracts. The performance of this Agreement by either party is subject to acts of God, war within the United States or war declared by the Congress or the President of the United States, [and] governmental authority (including any action or inaction by Congress that causes the federal government to shut down or that imperils Group's federal appropriation), disaster (including without limitation fire, flood, severe weather, earthquake, tornado and hurricane), pandemics and epidemics, strikes of third party, labor disputes or work stoppages in the city where the NeighborWorks Training Institutes and Community Leaderships Institutes are held (except that Contractor may not terminate this contract for strikes and other such situations involving Contractor employees), civil disorder within twenty (20)miles of Venue, acts of terrorism or threats of terrorism occurring within thirty (30) days of the dates of the Meeting, curtailment of transportation facilities (preventing at least 25% or more of Group's attendees from attending), or any other emergency of which make it illegal or impossible to provide the facilities or to hold either of the training events. The affected event may be terminated without a cancellation charge or any other liability to the other party of this Agreement for any of the above reasons as long as written notice from one party to the other is provided as soon as practical, but not less than five (5) days after an event listed in the immediately preceding sentence has occurred.

Indemnification

A. The Contractor will indemnify, defend, and hold harmless NeighborWorks America, its officers, directors, employees, successors, and permitted assigns from any losses, damages, claims, suits, judgments, liabilities and expenses (including attorneys' fees and court costs) incurred as a result of any act or omission by the Contractor, its employees, representatives, or contractors, which constitutes:

1. Failure to perform its obligations under this Contract;

2. Violation of a law, ordinance or regulation;

3. Negligence, willful misconduct, or otherwise tortious actions; or

4. Claim(s) brought by an employee or contractor of the Contractor against NeighborWorks America under a workers' compensation or similar employment law.

B. At the request of NeighborWorks America, the Contractor shall defend NeighborWorks America against any such claims, demands, judgments, and liabilities. The foregoing indemnification shall apply regardless of whether the Contractor or NeighborWorks America defends the claim. Should a death, injury, property damage, or loss be caused by the concurrent acts or omissions of both NeighborWorks America and Contractor, then indemnification shall be proportionate to Contractor's liability.

C. Intellectual Property. Contractor represents and warrants that its performance of this Contract does not infringe upon any United States patent, copyright or other intellectual property right of a third party. If a claim is made against NeighborWorks America asserting that Contractor's performance infringed on the intellectual property rights of a third party, Contractor shall, at its option: defend NeighborWorks America against such claim, acquire for NeighborWorks America the right to continue using the product in question without further infringement, or modify/replace the product with another product for which there exists no infringement claim.

1. Limitations. Contractor shall have no obligation to NeighborWorks America under this provision in situations where the infringement claim arises from Contractor's services or product being used in combination with software not licensed by Contractor, or Contractor's services or product being used in a manner inconsistent with this Contract.

2. Notice. If NeighborWorks America believes it is entitled to indemnification under this provision, it shall provide Contractor with written notice within fifteen (15) days of such discovery. Such notice shall state the nature of the claim with reasonable specificity.

Independent Contractor Status

This Contract is not intended to create an agency relationship, partnership, joint venture, or formal business organization of any kind. At all times the parties hereto shall remain independent contractors, each responsible for its own employees. Neither party shall have any express or implied authority to create any obligations on behalf of the other or to bind the other to any Contract, agreement, or undertaking with any third party. Services delivered under this Contract shall be performed by the Contractor as an independent contractor and not as an agent or employee of NeighborWorks America. All personnel furnished by the Contractor, including its contractors, shall be subject to the exclusive control and supervision of the Contractor and shall be considered solely the employees, agents, or contractors of the Contractor; and not employees, agents, or contractors of NeighborWorks America. The Contractor shall be responsible for compliance with all laws, rules, and regulations, including those related to employment of labor, hours of labor, state and municipal taxes chargeable or assessed with respect to its employees, including without limitation social security, unemployment, federal and state withholding and other taxes, and shall file in a timely manner all forms required in connection with such payments. Contractor agrees to defend, indemnify and hold harmless NeighborWorks America, its officers, directors, employees, representatives, successors, and permitted assigns from any loss, damage, penalty, fine or liability sustained because of the Contractor's non-compliance with this provision. Contractor further agrees to cooperate with NeighborWorks America in any investigation or proceeding by a regulatory or taxing agency challenging the Contractor's status as an independent contractor.

Insurance

A. Contractor shall be required to maintain insurance coverage that is customary and appropriate for the work being performed, so that coverage is in full force and effect through the term of the engagement. Upon request, Contractor shall – at its own expense – procure and maintain insurance policies in full force and effect throughout the term of the engagement.

1. Worker's compensation insurance coverage for employees, including any agents or subcontractors used, in coverages and amounts no less than that required by the state in which the Contractor has its headquarters.

2. Employer's liability insurance coverage (including state disability benefits coverage, where required) with a limit of at least $100,000 per occurrence.

3. The following are suggested minimum coverages for Comprehensive or Commercial General Liability Insurance:

a. For Contracts under $5,000: Comprehensive or commercial general liability insurance coverage is not required.

b. For Contracts between $5,000 and $100,000: Comprehensive or commercial general liability insurance coverage (including public liability) which insures the Insured Parties against any and all claims of personal injury and property damage occurring or arising in connection with performance of this Contract. The minimum limits of liability coverage under such policy shall be no less than $500,000 per occurrence of personal injury, bodily injury, or property damage, and at least $1,000,000 in the aggregate of such occurrences.

c. For Contracts over $100,000: Comprehensive or commercial general liability insurance coverage (including public liability) which insures the Insured Parties against any and all claims of personal injury and property damage occurring or arising in connection with performance of this Contract. The minimum limits of liability coverage under such policy shall be $1,000,000 per occurrence of personal injury, bodily injury, or property damage, and at least $2,000,000 in the aggregate of such occurrences.

4. Professional liability errors and omission insurance with limits of not less than $1,000,000 per occurrence, where Contractor is from a highly specialized profession (including law firms, architects, engineers, accountants, and insurance brokers).

5. Automobile liability insurance with a limit of not less than $1,000,000 combined and covering all owned, non-owned, and hired vehicles, where Contract performance involves Contractor's use of a motor vehicle.

B. Neither Contractor nor NeighborWorks America shall be deemed to be relieved of any responsibility by the fact that it carries insurance, nor shall the liability of either party be limited to the amount of insurance carried.

Ownership of Work Product

Contractor acknowledges that any and all products created and delivered to NeighborWorks America under this Contract are works for hire. All documents, reports, analyses, drawings, designs, blueprints, photographs, sketches, software and other materials (the "Work Product") prepared by or for the Contractor in the course of the Contractor's Services shall belong to NeighborWorks America, and Contractor grants to NeighborWorks America all right, title, and interest – including copyright and trademark – in the Work Product. Work Product does not include proprietary methodologies or materials created by the Contractor prior to this engagement.

Record Retention and Access

Contractor must adhere to the following requirements regarding record retention and access.

A. All records pertinent to performance of this Contract – including financial records and supporting documents – shall be retained for a period of three years from the date the final invoice is submitted. Copies of original records may be substituted for the original records.

B. If any litigation, claim, or audit is started before the expiration of the three year record retention period, records shall be retained until all litigation, claims, or audit findings involving the records have been resolved and final action taken.

C. NeighborWorks America shall request that Contractor transfer certain records to its custody when it determines those records possess long term retention value. When those records have been transferred or maintained by NeighborWorks America, Contractor is relieved of its obligation to further retain records.

D. Right to Audit. NeighborWorks America and its authorized representatives shall have the right to make site visits, to audit, to examine, and to make copies of or extracts from financial and related records (in whatever form they may be kept, whether written, electronic, or other) relating to or pertaining to performance of this Contract.

Subcontracting, Successors, and Assigns

Contractor shall not subcontract any portion of this Contract without prior written approval of NeighborWorks America. Contractor must maintain oversight to ensure that any such approved subcontractor(s) perform in accordance with the terms, conditions, and specifications of their Contract(s) and Task Order(s). This Contract and all provisions herein shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns. Nothing herein shall be construed to create any rights enforceable by any other person or third party. This Contract may not be assigned by any party without the prior written consent of the other party, which consent shall not be unreasonably withheld. Any assignment in violation of this provision shall be deemed null and void.

Warranty

The Contractor expressly warrants and represents to NeighborWorks America that it will conduct itself with the highest degree of integrity and honesty, that all goods provided or services performed will be done in a professional manner consistent with the highest industry standards, in conformance with the specifications contained in this Contract. Services that do not conform to any of these warranties will, at the discretion of NeighborWorks America, promptly be replaced or corrected by the Contractor at no cost to NeighborWorks America, until the Services are fully compliant with all warranties herein. This remedy shall be in addition to, and not in lieu of, any other remedies available to NeighborWorks America under this Contract.

Section I - Miscellaneous

Governing Law, Venue, Jurisdiction

This Contract shall be construed under and governed by the laws of the District of Columbia, without regard to conflict of laws provisions. Contractor hereby consents to jurisdiction of any state or federal court in the District of Columbia, waives personal service of process upon it, and consents that such service of process be made by registered mail and service so made shall be deemed to be completed upon actual receipt thereof. Both Contractor and NeighborWorks America hereby waive the right to trial by jury and consent to the granting of legal or equitable relief deemed appropriate by the court.

Disclosure Required by Law

All Contracts and related documents (including those created, held, or stored by the Contractor) are a matter of public record subject to disclosure in accordance with the requirements of the Freedom of Information Act and its analogues.

Entire Agreement

This Contract, including its exhibits and attachments, constitutes the complete understanding of the parties relating to this award. As such, this Contract supersedes all prior negotiations and discussions. Failure by either party to enforce a provision of this Contract shall not constitute a waiver of that provision or any other provision of this Contract. Furthermore, the invalidity or unenforceability of any provision of this Contract shall not affect the validity or enforceability of any other provision of

this Contract. Headings contained in this Contract are intended solely for convenience and shall not affect the rights of the parties to this Contract. This Contract may be executed in counterparts, all of which shall be considered one and the same Contract and each of which shall be deemed an original. If executed and transmitted by electronic copy, the scanned or facsimiled signature page shall be deemed an original signature page.

Contractor Organization Type:

[Contractor should identify company status below]

{ } Sole Proprietor

{ } C Corporation

{ } S Corporation

{ } Partnership

{ } Limited Liability Company

Section J - List of Attachments

Attachment Order	Title	Date
A	Information Governance Policy	05/13/2024
B	Third-Party Security Addendum and Questionnaire	05/13/2024

Section K - Contractor's Representations & Warranties Certification

1 RECITALS

WHEREAS Contractor has been awarded a Contract under RFP-24-0027 (“Contract”) with NeighborWorks America; and
WHEREAS Contractor is required to make certain representations and warranties regarding (i) its eligibility to perform the awarded work, and (ii) the obligations it must impose on any party it contracts with or engages to fulfill Contractor’s obligations under this Contract.

NOW, THEREFORE, the Contractor hereto certifies as follows:

1. All terms used herein shall have the same meaning as in the Contract. In the event of any conflict in meaning or use between terms as used in the Contract and this Certification, the Contract meaning shall control.

2. All sub-contractors or other entities engaged to perform the work of this Contract will be approved in writing by NeighborWorks America, will satisfy all of the requirements and certifications listed herein, and will sign a certification (to be retained by Contractor) documenting its compliance with these requirements. Contractor will maintain oversight to ensure that its sub-contractors perform in accordance with the terms, conditions, and specifications of their contracts or purchase orders.

3. Contractor represents and warrants the following:

A. That it understands the terms of this Contract can be modified only when such instructions are issued in a writing signed by the Contracting Officer.

B. That it will notify the Contracting Officer within five (5) business days if — at any point during the Contract performance period — it becomes the subject of a debarment or suspension action by a federal agency, or is otherwise deemed ineligible to perform work in federal procurement.

C. That it will notify the Contracting Officer within five (5) business days if it becomes aware of credible evidence of a Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations, or a violation of the civil False Claims Act.

D. That it will scan for personal and organizational conflicts of interest prior to executing this Contract, monitor for conflicts – real or perceived – that may emerge during the performance period, and make an immediate and full report to the Contracting Officer of any such conflicts.

E. That it will not discriminate against employees or applicants for employment on the basis of race, color, religion, sex, sexual orientation, gender identity, disability, or national origin.

F. That it will pay taxes on earnings under this Contract, as required by law, and will not become delinquent on tax debt owed the U.S. Internal Revenue Service.

G. That it will maintain insurance coverage no less than is customary and appropriate for the work and risk involved in this Contract.

H. That it will comply with all federal, state, and local laws in performance of its obligations under this Contract.

I. That it [Select is or is not] a former employee of NeighborWorks America.

J. That it will adhere to the NeighborWorks Contractor Code of Business Ethics and Conduct available on NW.org.

4. This Certification may be modified only by written instrument signed by both Contractor and NeighborWorks America. Failure by Contractor to enforce or adhere to a provision of this Certification shall not constitute a waiver of that or any other provision of this Certification. The invalidity or unenforceability of any provision of this Certification shall not affect the validity or enforceability of any other provision of this Certification.

CERTIFIED, as of the date stated below: [Contractor Must Complete and Sign Below]

_____

Contractor Name (type or print)

_____

Contractor Authorized Official:

_____

Contractor Authorized Official (signature)

_____

Date

Section L - Proposal Requirements

Proposal Requirements

The Contractor shall sign Page 1 of the RFP, complete the applicable fill-in sections (highlighted in yellow), and electronically submit the completed RFP with their technical and price proposals to: Jayme Hardy, jhardy@nw.org, Cc: ProcurementDept@nw.org, **no later than 5:00PM ET, 07/19/2024**. The subject line should read: Proposal for RFP-24-0027 - CounselorMax Developer RFP.

Question Submission

Questions must be submitted electronically to: Jayme Hardy, jhardy@nw.org, Cc: ProcurementDept@nw.org **no later than 5:00PM ET, 06/28/2024**. The subject line should read: Questions to RFP-24-0027 - CounselorMax Developer RFP. No further questions will be accepted after this date. Responses will be posted no later than 5:00PM ET, 07/08/2024.

Letter of Interest

All Vendors interested in submitting a proposal under this RFP may notify NeighborWorks at Jayme Hardy, jhardy@nw.org, Cc: ProcurementDept@nw.org **no later than 5:00PM ET, 06/28/2024**. The subject line should read: Intent to Propose RFP-24-0027 - CounselorMax Developer RFP. This is not required, but only suggested as a means of information to NeighborWorks about interest in this solicitation.

Technical Proposal Requirements

The technical proposal must include the following components outlined below:

A. Cover Letter that includes:
1. Official registered name (Corporate, D.B.A., Partnership, etc.), type of business entity, unique entity identifier from SAM.gov; primary and secondary NAICS numbers, address, main telephone number, toll-free numbers, and facsimile numbers, any if available.

2. Key contact name, title, address (if different from above address), direct telephone and fax numbers.

3. Person authorized to contractually bind the organization for any proposal against this RFP.

4. GSA Number if available.

5. Statement of capacity that addresses the firm's qualifications to meet the requirements of the RFP.

Price Proposal Requirements

The price proposal must be submitted in a separate file with pricing information as described in Section B. Cost of travel can be estimated in the proposal with final pricing determined at contract award.

Your price proposal should clearly indicate the total for each period of performance (for each year) and then a total contract value not-to-exceed amount.

Additional Requirements

Section M - Evaluation Criteria

Evaluation Criteria

1. Best Value. NeighborWorks America will make an award to the Contractor(s) whose proposal(s) represents the best value for NeighborWorks America, considering both cost and non-cost factors.

2. Establishment of a Competitive Range. NeighborWorks America may upon its discretion establish a competitive range of qualified proposals for award consideration. NeighborWorks America will not conduct discussions and/or negotiations with firms not in the competitive range and those firms will not be considered for award.

3. Evaluation of Options. Except when it is determined not to be in NeighborWorks America's best interests, NeighborWorks America will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate NeighborWorks America to exercise the option(s).

Additional Criteria

Evaluation Criteria	**Percentage**
Company Overview	20%
Implementation	20%
Customer Service & Technical Support	30%
Price	10%
Contracting Components	10%
Customer References	10%
Total Evaluation Criteria	**100%**

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).

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).