SMALL PURCHASE REQUEST FORM

PART 1 – REQUESTOR AND SCOPE OF SERVICES INFORMATION

PROJECT TITLE	SP ITS 80540_SymPro Investment Management (Software)
REQUESTING DEPARTMENT / DIVISION	Procurement & Contracts / Information Technology
REQUEST ISSUED	3/28/2025
QUOTE DUE DATE AND TIME	4/11/2025 at 1:00 PM CT
PERFORMANCE PERIOD Initial and Option Periods (if applicable)	5 Year Base Term
PROJECTED CONTRACT START DATE	5/1/2025
CONTACT PERSON NAME/EMAIL	Frederica Juste – FJuste@thecha.org

PART 2 – SCOPE OF WORK

The Chicago Housing Authority (CHA) Treasury Department is procuring SymPro Investment Management Software to support the management of its $500 million investment portfolio. This software will replace manual processes and legacy systems by automating investment tracking, compliance reporting, and financial integrations.

SymPro implementation services, data migration, training, and support shall be provided with this software.

Specification/ Service Description	*Estimated Qty	Bidder's Unit Price *Per Item	Item Total (Inclusive of Discounted Rates)
Investment Management System Annual Subscription – Includes: ▪ Access for 3 Users & Unlimited Technical Support ▪ Annual Maintenance, Hosting, ▪ Software Upgrades/Enhancements ▪ General Ledger Interface & Creation/Export of Journal Entries to GL (Lawson) ▪ Market Pricing – Once per month for up to 300 portfolios) ▪ Export of Purchases to Any Selected Financial Institute	5		
Additional Users (as needed)	3		
Consulting, Migration/Conversion of Data, Implementation, & Training (Base Year 1)	1		
Rewrite General Ledger Interface	1		
Invoice Payments will be issued based on annual amounts and services rendered		**5 YEAR BASE CONTRACT TOTAL**	

*(See Exhibit I. **CHA** Information Security Policy & Exhibit II. **CHA** Investment & Cash mgmt. policy)*

**CHA reserves the right to increase or delete any scheduled items, and/or increase or reduce the quantity of any scheduled item as deemed necessary, to waive informalities and technicalities, and to make other changes and modifications consistent with CHA's policies, and the laws and regulations governing HUD programs.*

1. **Software Functionality**
   - **Investment Portfolio Management:**
     - Tracking and management of uncapped active portfolios with real-time updates.
     - Support for Treasury bonds, corporate bonds, money market accounts, and other securities.
       - In accordance with generally accepted accounting principles with an average of 150 – 300 active securities, the CHA is required monthly to price all securities throughout the portfolio at market value utilizing a standard pricing service - currently IDC (International Data Corporation).
     - Investment compliance monitoring based on CHA's investment policies.
   - **Accounting & Compliance Reporting:**
     - Automated journal entries for investment transactions, directly interfacing with CHA's general ledger system & ERP Systems (Currently Lawson & changing in FY26 to Yardi).
     - Built-in compliance with GASB 31, 40, and 72 reporting standards.
     - Customizable audit and performance reports with over 50 pre-built templates (excel & pdf formats)
   - **Risk Management & Forecasting:**
     - Scenario modeling, stress testing, and performance benchmarking.
     - Liquidity forecasting tools to manage cash flow and investment maturities.
   - **System Integration:**
     - Automated transaction imports from current custodians (BMO Harris, Bank of New York).
     - General ledger integration to sync investment activities with financial statements.

2. **Implementation & Project Management Services**
   - **Project Governance & Planning:**
     - Develop and maintain a detailed project plan, including milestones, deliverables, dependencies, and resource allocations.
     - An assigned main point of contact & dedicated Project Manager to oversee implementation, coordinate with CHA stakeholders.
     - Provide regular status reports outlining progress, risks, and mitigation strategies.
     - Conduct weekly meetings with CHA Treasury team.
   - **Data Migration Plan & Execution:**
     - Develop a data migration plan outlining steps for securely extracting, transforming, validating, and migrating data from EVARE to SymPro with an expected completion of migration of September 2025
     - Perform data mapping and validation to ensure accuracy and completeness of active historical data.
     - Conduct data reconciliation and testing, including sample audits to confirm the accuracy of imported records.
     - Provide a rollback and contingency plan in case of migration issues.
   - **System Configuration & User Acceptance Testing (UAT):**
     - Collaborate with CHA to define current & any future system configurations, user roles, and access permissions before deployment.
     - Support CHA in developing test cases for user acceptance testing (UAT).
     - Conduct joint UAT sessions and address identified defects or gaps before going live.

- **Go-Live Readiness & Deployment:**
  - Provide a go-live checklist ensuring all necessary configurations, integrations, and training completion.
  - Offer on-site or remote support during go-live to assist with troubleshooting and system stabilization.
  - Develop a post implementation support plan outlining continued assistance and system optimization.

3. **Knowledge Transfer & System Administration Access**
   - The vendor shall provide a comprehensive knowledge transfer to CHA's Treasury management team with training of necessary skills to manage and support the system post-implementation.
   - The vendor shall provide system administration access to CHA's Treasury team allowing them to manage user permissions, configurations, and integrations.
4. **User Training & Documentation**
   - Training sessions for up to 5 Treasury, Finance, and Accounting users, including hands-on sessions for daily operations.
   - Administrator training on system setup, user management, and reporting.

All Quote Responses Must Be Typed & Signed by an Authorized Representative from the Respondent's company.

PART 3 – VENDOR INFORMATION

_____

(INDICATE **CORPORATE NAME ATTACHED TO FEDERAL TAX ID NUMBER**) has thoroughly read all pages of ITS SP 80540_SymPro Investment Management (Software) *and all associated addenda* (if applicable) and can provide the services as described at the offer submitted on this Quote Form.

CONTACT INFORMATION FOR CORPORATE OFFICIAL AUTHORIZED TO BIND RESPONDENT

DATE	
CORPORATE AUTHORIZED REPRESENTATIVE	
CORPORATE OFFICIAL E-MAIL ADDRESS	
COMPANY PHONE NUMBER	
COMPANY ADDRESS	
CORPORATE AUTHORIZED REPRESENTATIVE SIGNATURE	

The successful Respondent(s) will be required to submit mandatory CHA forms and affidavits within seven days of notice of award found at https://www.thecha.org/contracting-opportunities/forms-and-documents.

The mandatory forms will be forwarded to the successful Respondents prior to contract award. Forms should be completed, signed, and notarized where required or marked "not applicable" where appropriate. The mandatory forms are:

- Diversity Inclusion Utilization Plan**
- Compliance Certification Form
- Contractors Affidavit
- Economic Disclosure Statement Form
- HUD-50071 - Certification of Payments to Influence Federal Transactions
- HUD 5369-A Representations, Certifications and Other Statements of Bidders
- Required Insurance Certificate (see below **Insurance Requirements**)

Failure by the Respondent to provide such information within the allotted time will render the Respondent ineligible for award.

CHA may reject any or all quotes. Action to reject all quotes shall be taken only for unreasonably high prices, error in the solicitation, cessation of need, unavailability of funds, failure to secure adequate competition, or any other reason deemed appropriate by CHA.

Insurance Requirements

Prior to the commencement of this Agreement, Vendor/Consultant shall procure and maintain at all times during the term of this Agreement insurance against claims for security breaches, system failures, injuries to persons, damages to software, or damages to property (including computer equipment) which may arise from or in connection with the performance of the work hereunder by the Vendor, its agents, representatives, or employees. The Vendor shall procure and maintain for the duration of the contract insurance claims arising out of their services and including, but not limited to loss, damage, theft or other misuse of data, infringement of intellectual property, invasion of privacy and breach of data. The insurance carriers used must be authorized to conduct business in the State of Illinois and shall have an A.M. Best rating of not less than A: VII.

Minimum Coverage and Limit Requirements – Information Technology Agreements

1. **Commercial General Liability**: General Liability Insurance on an occurrence basis with limits not less than $1,000,000 per occurrence with an aggregate of not less than $2,000,000 covering bodily injury and property damage. This coverage shall also include, but not be limited to, contractual liability, products and completed operations, personal and advertising injury.

2. **Auto Liability**: Required when any vehicles (owned, hired and/or non-owned) are used in connection with the Services to be performed, coverage limits of not less than $1,000,000 each accident combined single limit for Bodily Injury and Property Damage.

3. **Workers' Compensation and Employer's Liability:** Coverage must be in accordance with the laws of the State of Illinois and include a waiver of subrogation in favor of Chicago Housing Authority.
    - Coverage A – Statutory Limits
    - Coverage B - Employers Liability - $500,000 bodily injury or disease each accident; each employee

4. **Technology Errors & Omissions (including Cyber Liability)** required when Vendor/Consultant provides technology services or technology products under this Agreement, insurance appropriate to the professional services being performed shall provide coverage for the acts, errors, or omissions of Vendor/Consultant with a limit of not less than $1,000,000 per occurrence or claim and $2,000,000 in aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Vendor in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs, regulatory fines and penalties as well as credit monitoring expenses.

Related Insurance Requirements

The Certificate of Insurance evidencing the minimum coverages required herein shall be in force on the Effective Date of the Contract and continuously throughout the duration. The required documentation must be received prior to the commencement of work under this Agreement. It is understood and agreed to by the parties hereto that Chicago Housing Authority and others listed below shall be included as Additional Insureds on Vendor's liability policies, with the exception of Professional Liability and Employer's Liability and such insurance is primary to and will not seek contribution from any insurance, deductibles, self-insured retentions and/or self-insured programs available to Chicago Housing Authority.

Certificate Holder: Chicago Housing Authority
60 E Van Buren
Chicago, IL 60605

Additional Insureds: Collectively referred to as the "Additional Insureds" shall include Chicago Housing Authority, Chicago Housing Administration, LLC; and/or other Partnership, Limited Liability Company as established by CHA; its respective commissioners, board members, officers, directors, agents, property management firms, agents, employees, invitees and visitors.

Primary Coverage: For any claims related to this Agreement, the Vendor's insurance coverage shall be the primary policy. The Vendor expressly understands and agrees that any insurance or self-insurance programs maintained by the CHA shall apply in excess of and shall not contribute with insurance provided by the Vendor.

Prior to the issuing of the Notice to Proceed by the CHA, the Vendor shall submit a Certificate of Insurance via PINS Advantage Certificate Tracking System, evidencing compliance with the insurance requirements set forth above. You will receive an email with instructions for the submission of your insurance. Copies of the endorsement(s) adding the CHA to the Vendor's policy as an additional insured are required upon request. Updated Certificates of Insurance are required for policies which renew during the term of this Agreement or extensions thereof. Under no circumstances shall the Vendor allow any required coverage to lapse, cancel or non-renew throughout the duration of the Agreement or extensions thereof.

At the CHA's option, non-compliance will result in (1) all payments due the Vendor being withheld until the Vendor has complied with the Agreement; or (2) the Vendor will be assessed Five Hundred Dollars ($500.00) for every day of non-compliance; or (3) the Vendor will be immediately removed from the premises and the Agreement will be terminated for default. The receipt of any certificates does not constitute agreement by the CHA that the insurance requirements in the Agreement have been fully met or that the insurance policies indicated on the certificate comply with all Agreement requirements. The insurance policies shall provide for thirty (30) days prior written notice to be given to the CHA in the event coverage is substantially changed, canceled or non-renewed.

The Authority in no way warrants that the minimum limits contained herein are sufficient to protect the Authority from liabilities that might arise out of the performance of the work under this Agreement by the Vendor or its Subcontractors. Vendor shall assess its own risks and, if it deems appropriate and/or prudent, maintain higher limits and/or broader coverages. The Vendor is not relieved of any liability or other obligations assumed or pursuant to the contract by reason of its failure to obtain or maintain sufficient insurance.

The Vendor shall require all subcontractors to carry the insurance required and adhere to the same requirements and conditions as outlined above.

The Vendor expressly understands and agrees that any insurance or self-insurance programs maintained by the CHA shall apply in excess of and will not contribute with insurance provided by the Vendor and/or any of its subcontractors.

PART 4 – ADMINISTRATIVE TERMS AND CONDITIONS

- ### Required CHA Vendor Registration

  In order to do business with CHA, Respondent must be a registered vendor prior to submitting a response. IfRespondent has already registered with CHA, the Respondent's (Vendor) profile must be up to date.

  Respondent is responsible for contacting their local authorities to ensure that Respondent has complied with all laws and is authorized and/or licensed to do business in the Territory. All applicable fees associated therewith are the responsibility of Respondent now or hereafter in effect during the contract. Respondent and its employees, agents and subcontractors shall also comply with all Federal, State and local laws regarding business permits and licenses that may be required to carry out the services performed under the contract.

- ### Acceptance Period

  All Respondents submitting a quote must agree to honor the terms and conditions contained herein for a period of one hundred twenty (120) days.

- ### Quote Signature

  The person signing the Quote Form must be a person authorized to bind the Respondent contractually. Unsigned offers will be rejected. Unsigned offers cannot be signed after the quote has been received.

- ### Ownership of Documents

  All work products generated, prepared, assembled and provided to CHA pursuant to this RFQ become the property of CHA upon receipt. Work products include but are not limited to reports, memoranda, data, survey responses, presentations, and other materials of any nature, or information related to any of the foregoing, which are or were generated in connection with the scope of services described in the contract. Respondents shall not copyright, or cause to be copyrighted, any portion of any document submitted to CHA as a result ofthis RFQ.

- ### Contractor Status

  The Contractor shall be an independent Contractor and will not be an employee of CHA.

- ### Funding Limitations

  This procurement may be funded, in whole or in part, by grant funds provided by the U.S. Department of Housing and Urban Development ("HUD"). CHA will not be bound to any contract if funding has been disallowed by HUD.

- ## Taxes

  CHA is exempt from sales tax. The Contractor agrees to pay all taxes incurred in the performance of an awarded contract. Freight, handling costs, and taxes shall not be charged to the CHA.

- ## Advertising

  Respondent agrees not to use the fact of or the results from submission of a quote as a part of any commercialadvertising. CHA does not permit the use of CHA's relationship with an entity of purposes of marketing efforts unless CHA specifically agrees otherwise.

- ## Government Restrictions

  In the event any governmental restrictions may be imposed which would necessitate alteration of the material, quality, workmanship or performance of the goods or the material, quality, workmanship or performance of the goods or services offered, it shall be the responsibility of the successful Respondent to immediately notify CHAin writing specifying the regulation which requires an alteration. CHA reserves the right to accept any such alteration, including any reasonable price adjustments occasioned thereby, or to cancel the contract at no expense to CHA.

- ## Compliance & Law

  The Respondent shall comply with all applicable Federal, State and local laws, regulations, ordinances and requirements applicable to the work described herein including, but not limited to, those applicable laws, regulations and requirements governing equal employment opportunity programs, subcontracting with small and minority firms, women's business enterprise, and labor surplus area firms, equal opportunity for businesses and unemployed and underemployed persons (as referenced in Section 3 of The Housing and Urban Development Act of 1968, as amended, 12 U.S.C. 1701u (Section 3), the Americans with Disabilities Act, Section 504 of the Rehabilitation Act of 1973, the Davis-Bacon Act, and those laws and regulations concerning the abatement and remediation of asbestos and lead-based paint, and shall provide for such compliance in the contract documents.

  To the extent the work required under this contract is related to development, Respondentshall further comply with the applicable Annual Contributions Contract (ACC) related to such development. To the extent such work is related to a mixed finance development, Respondent shall comply with the provisions of 24 CFR ' 941.208. The Respondent shall obtain, at Respondent's expense, such permits, certificates and licenses as may be required in the performance of the work specified.

Vendor Name	M/W/DBE and/or Section 3 Status	Certification Attached (Y/N)

Chicago Housing Authority
Contract Requirements

CHA is committed to contracting with vendors who share our values for inclusive and equitable contracting opportunities. CHA strives to be fair, transparent and practical, and to optimize the use of public funds through purchasing decisions.

1. Summary of Contract Requirements

Type of Contract	M/W/DBE	HUD Section 3 (Labor Hours)	S3 Business subcontracting (> $250,000)	Davis Bacon
Construction	Yes	Yes	Yes	Yes
Professional Service (licensure required)	Yes	No	Yes	No
Professional Service (non-licensure required)	Yes	Yes	Yes	No
Professional Services (direct services to residents)	Yes	Yes	No	No
Material & Supply	Yes	No	Yes	No

* if not self-performing

Minimum Contract Requirements:

Minority/Women/Disadvantaged Business Enterprises (M/W/DBEs)

Certified Minority, Women, and Disadvantaged Business Enterprises (M/W/DBEs) shall have the maximum opportunity to participate in the performance of contracts financed in whole or in part with federal funds. Vendors and their subcontractors or suppliers must take all necessary and reasonable steps to ensure that M/W/DBEs have the maximum opportunity to compete for and perform contracts financed in whole or in part by federal funds. CHA establishes minimum thresholds for all contracts over $50,001. Vendors unable to meet the requirement may propose indirect participation subject to CHA's written approval.

Section 3 Business Subcontracting – For contracts >$250,000**,** vendors are required to subcontract to Section 3 Businesses, unless self-performing. To locate a Section 3 Business, visit the Workforce Opportunity Resource Center (WORC) site. Professional Services that directly provide social support services for CHA residents are not required to sub-contract to Section 3 Businesses but are encouraged to sub-contract when feasible. Vendors unable to meet the requirement may propose indirect participation subject to CHA's written approval. These may include, but are not limited to mentorship programs,

internships, training, and employment opportunities for non-CHA funded projects, or payment into CHA's Workforce & Education Fund.

Section 3 Labor Hours

CHA supports HUD's Section 3 requirement which counts labor hours. All applicable contracts **require at least 25% of the labor hours** performed on a project are done so with Section 3 workers and businesses, of which 5% of those hours must be performed by Targeted Section 3 workers (i.e. CHA residents and HCV participants).Vendors will report these hours via B2Gnow and/or LCPtracker or through required affidavits based on the contract type (HUD Section 3 24 CFR part 75).

Davis Bacon and Minimum Wage Requirements:

The Davis-Bacon & Related Acts apply to construction contracts over **$2,000** and ensures that all construction employees are paid under the US Department of Labor's wage decision. Union contractors must ensure that Davis-Bacon wages are met, in accordance with the contract.

All CHA contracts must comply with the current local Minimum Wage requirement. The Minimum Wage Requirements shall be specifically incorporated as a contractual requirement in any award and agreement resulting from this solicitation for any of the Selected Respondent's covered employees. The Respondent must consider the Minimum Wage Requirement in determining its fees for services to be performed or provided by the Respondent under its fee proposal and other submittals. Note that Federal wage determinations (either Davis-Bacon or HUD-Determined Wage Rates) preempt any conflicting State prevailing wage rate or the Minimum Wage Requirement when the State prevailing wage rate or the Minimum Wage Requirement is higher than the Federally imposed wage rate (24 CFR 965).

The following chart indicates the goals set by the CHA for each type of contract.

Type of Contract	Contract Amount	MBE/WBE/DBE Participation	Section 3 Business Subcontracting (>$250,000)	Section 3 Labor Hours (25% of which 5% is through CHA resident hires)***
Construction	$50,001+	30%	10%	25%
Supply & Delivery	$50,001 +	20%	3%*	N/A
Professional Services	$50,001 +	20%	3%**	25%

*Or indirect **excludes direct support service providers *** Required regardless of contract amount

2. Utilization Plan:

This chart is a list of items needed to evaluate a full utilization Plan (UP). All respondents to CHA solicitations must submit a UP which enables CHA to evaluate how they will fulfill contract requirements.

Document Name	To be Completed By	Details
Utilization Plan (UP) M/W/DBE and Section 3 Businesses	Prime Contractor	This Excel worksheet will include all M/W/DBE and Section 3 Businesses subcontracting as well as proposed indirect, etc.
Letter of Intent	Each M/W/DBE and Section 3 subcontractor listed on the UP including a self-performing Prime Contractor	If a Prime is a M/W/DBE and they are self-performing, they must submit a Letter of Intent. A Letter of Intent for each sub-contractor that is MWD/BE or Section 3 Business must also be submitted. The information outlined in the UP must correspond with the Letters.
Letter of M/W/DBE Certification	Each M/W/DBE listed on UP, including a self-performing Prime Contractor	This form must be submitted with every UP and Letter of Intent and include current certification letters. Applications are not accepted.
Waiver Request- M/W/DBE	Prime Contractor	This form is only to be used if a vendor cannot meet their subcontracting requirements and all good-faith efforts, including indirect participation, have been exhausted. The form must include (1) the scope of work and (2) the reason the Prime cannot meet the commitments outlined.
Other Economic Opportunities (OEO)	Prime Contractor	If vendor is unable to subcontract to a Section 3 Business in full or in part, they will need to propose indirect participation through the OEO section on the UP, or make commensurate payment upfront into the Workforce and Education Fund, subject to approval by CHA.

3. Reporting Requirements:

Contract Requirement	System	Details
Construction Contracts	LCPtracker	Certified Payroll Reports must be entered into LCPtracker weekly. This system also tracks compliance with Davis Bacon and Section 3 hours.
Professional Services	B2GNow	Payments must be entered into B2Gnow for every pay application monthly. This system tracks and verifies Prime and Subcontractor payments made and received.

Additional Information:

(a) COUNTING M/W/DBE AND SECTION 3 BUSINESS (S3B) CREDIT: A business that is both self-identified /certified as a Section 3 Business and certified as a M/W/DBE will count towards subcontracting requirements for both the M/W/DBE and Section 3 sub-contracting requirements.

(b) PROVIDING OPPORTUNITIES TO SECTION 3 WORKERS: In accordance with 24 CFR part 75.9, Prime and sub-contractors (including Section 3 Businesses) on CHA/HUD-funded contracts must ensure that Section 3 workers are provided economic opportunities with the following preference when applicable: a) residents of the project where the assistance is being provided; b) residents of other public housing or Section 8; c) Youthbuild participants; and d) resident of the metropolitan area.

(c) SUBSTITUTION/REMOVAL OF SUBCONTRACTOR: A prime contractor that needs to remove or substitute a subcontractor on its approved utilization plan must submit a written request for the removal or substitution of the subcontractor concerned. Only when Department of Procurement and Contracts (DPC) approves such a request in writing can the removal or substitution of the subcontractor be done by the prime contractor. Under no circumstance should a prime contractor unilaterally remove or substitute a subcontractor on its CHA/HUD-funded contract without prior approval by DPC.

Definitions

Section 3 Business are defined a business that either is a) 51% owned by public housing or housing choice voucher participant(s); b) 51% owned by a low-income person(s); or c) 75% of the labor hours are performed by low-income workers.

Davis-Bacon and Related Acts directs the US Depart of Labor to determine prevailing wage for construction projects.

Indirect Participation refers to the value of payments made to MWD/BE firms for work that is done outside of the proposed project or commensurate value to S3 Business or CHA residents/participants in other economic opportunities.

Additional information on CHA's contract requirements and forms can be found at https://www.thecha.org/how-do-business-cha

EXHIBIT I.

INFORMATION TECHNOLOGY SERVICES
INFORMATION SECURITY POLICY

2015-2024

TABLE OF CONTENTS

1.0 INTRODUCTION

The Chicago Housing Authority (CHA) relies heavily on information technology to achieve its mission:

> *To leverage the power of affordable, decent, safe, and stable housing to help communicated thrive and low-income families increase their potential for long-term economic success and a sustained high quality of life.*

To ensure continuous achievement of the CHA's mission and solidify its commitment to quality service, the Information Technology Services (ITS) department has established its internal mission:

> To be an excellent customer service-oriented team that supports and maintains the essential infrastructure and applications that implement information and communication technology services for the Chicago Housing Authority and its stakeholders.

Information security policies are essential to protect assets and ensure high quality service delivery as the CHA continues to execute its mission. All departments across the CHA are required to adhere to this policy. Each department must also determine its need for any additional controls.

1.10 Purpose

The purpose of this document is to establish a clear, concise set of information security policies for the Chicago Housing Authority, subsequently referred to as the CHA. The document provides a foundation for protecting the organization's information resources. The policy is designed to help assure adequate security for information collected, transmitted, processed, stored, or presented via the CHA's systems. It is established to ensure appropriate information confidentiality, integrity, and availability.

This policy also describe what steps must be taken to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with company standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

The CHA's information security policies and procedures are based on standards and best practices defined by the U.S. Department of Housing and Urban Development, National Institute for Standards and Technology (NIST), International Standards Organization (ISO), the Information Systems Audit and Control Association (ISACA) and the System Administration Networking and Security Institute (SANS). It is also consistent with federal legislative directives, including: Federal Information Security Management Act, Computer Fraud and Abuse Act, Electronic Communications Privacy Act, Federal Privacy Act, National Information Infrastructure Protection Act, and the Sarbanes-Oxley Act.

This policy supersedes any of the CHA's previous information security policies and is consistent with existing organization-wide policies, codes of conduct, standards, and procedures.

1.20 Scope

This policy encompasses information security policies for the Chicago Housing Authority. It addresses technical, management and operational requirements for security from an information technology (IT) perspective.

The scope of this policy also includes all users who have access to company-owned or company provided computers or require access to the corporate network and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the corporate network. Public access to the company's externally reachable systems, such as its corporate website or public web applications are specifically excluded from this policy.

(1) Inclusions: Policy provisions apply to all the CHA's employees and officials and nonemployees who access the CHA's information, including:

- CHA personnel, contractors acting on behalf of the CHA, and all users who access the CHA's networks, applications, and support facilities.
- Non-CHA organizations (or their agents), including other government agencies, who are granted access to the CHA's resources.

(2) Exclusions: This policy is intended to provide a set of basic information protection goals. However, it does not include substantial technical or operational details related to security controls implementation. Technical and operational details are documented in Information Technology Services (ITS) procedure documents and respective departmental documentation. Also, physical security for personnel and non-ITS equipment is excluded from this policy.

Additional policies and procedures may be issued as supplements to this document, as necessary.

1.30 Definitions

Some common terms are used throughout this policy. Many of these terms contain various meanings. To establish a consistent understanding of terms for the context of this policy, the following is a list of definitions.

1.30.10 Control

A control is a protective measure that should be put in place to help mitigate or minimize risk.

1.30.20 Risk

A risk is the probability that a threat will exploit vulnerability in a system or process.

1.30.30 Application

An application is a software product or series of programs executed to meet a set of business objectives or user requirements.

1.30.40 Sensitive Information

As defined by the Computer Security Act of 1987, "sensitive information" is information that requires that access be controlled and restricted "in order to protect the national interest, the conduct of federal programs, and the privacy to which individuals are entitled under the Privacy Act". For the purposes of this policy, sensitive information is information that can cause substantial harm, including financial loss and/or embarrassment to the CHA if it is not properly protected.

1.30.50 Public Information

Public information is information that can be disclosed to the public without restriction, but should be protected against erroneous alteration (e.g., a public Internet web site).

1.30.60 Principle of Least Privilege

The "principle of least privilege" also known as the "principle of least authority" requires granting users' minimal access to systems. It requires that users receive no more than the access necessary for the execution of their job responsibilities.

1.40 Acronyms

The following are commonly used acronyms used throughout this document.

CEO – Chief Executive Officer

CFO – Chief Financial Officer

CHA – Chicago Housing Authority

COS – Chief of Staff

CIO – Chief Information Officer

DCIO – Deputy Chief Information Officer

SDIR – SR Director, Information Technology

MGRINFR – MGR Infrastructure Information Technology

ITS – Information Technology Services

1.50 Overview of Network Access

Consistent standards for network access and authentication are critical to the company's Network information security and are often required by regulations or third-party agreements. Any user accessing the company's computer systems can affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduces risk of a security incident by requiring consistent application of authentication and access standards across the network.
• Network (on-site or remote) Access: All requests for network accounts must be approved by a manager or supervisor before submittal to ITS for implementation.

2.0 ORGANIZATION AND USE OF THIS DOCUMENT

2.10 Document Organization

This document is organized in sections by content area. Early sections of the document provide foundational elements of the policy. As the document progresses, actions are specified based on the earlier defined foundation (e.g., roles and responsibilities).

Sections 3.0 through 5.0 give general information on roles and responsibilities of key parties and how policy compliance and information classification is handled.

Section 6.0 describes how information should be handled based on its classification level.

Section 7.0 defines requirements for reporting security incidents (e.g., policy violations).

Sections 8.0 and 9.0 primarily apply to System Owners and managerial staff. These sections illustrate segregation of duties requirements and role-based security.

Sections 10.0 through 12.0 define system access requirements for all users.

Sections 13.0 through 16.0 describe specific action-oriented processes that all users must adhere to for the daily use of information resources.

2.20 How to Use this Document

This document should be read in its entirety. Security awareness training is given as a supplement. All users are responsible for knowing and complying with the CHA's information security policy.

Each section is numbered and identified via a title designating the section's subject area. A subsection is identified by the general section it falls under and appended increments of 10. For example, Section 3.0 identifies the general section on Roles and Responsibilities. Each role is

identified by a subsection number (e.g., Chief Executive Officer is described in section 3.10). Increments of 10 are used for the easy addition of future sections.

3.0 ROLES AND RESPONSIBILITIES

The responsibility of protecting the Authority's information assets is shared by all CHA employees and officials and non-CHA employees who access the CHA's information. Specific duties are associated with key personnel responsible for upholding the policy. This section defines specific information security roles and responsibilities.

3.10 Chief Executive Officer

The Chief Executive Officer directs all aspects of the operations of the Chicago Housing Authority. The Chief Executive Officer, along with key executive office personnel (i.e., Chief of Staff), is responsible for establishing and articulating the Authority's security stance. Key responsibilities include:

- Provide the strategic vision for the CHA's information security program.
- Approve strategic goals and ensure information security is integrated in the Authority's management processes.
- Ensure the CHA complies with applicable regulatory directives.

3.20 Chief Information Officer

The Chief Information Officer (CIO) establishes and oversees all expects of the Information Technology Services and network security function and has the following responsibilities:

- Provide guidance and vision for an effective, agency-wide information technology services.
- Develop and manage the budget for all ITS operations and activities, including network information security initiatives.
- Review, evaluate and approve information security policies and procedures.
- Establish oversight procedures to ensure all IT activities comply with information technology network security policies and procedures.
- Provide oversight for the enforcement of information technology and network security policies, procedures, and control techniques.

3.25 Deputy Chief Information Officer

The Deputy Chief Information Officer directs and oversees ITS operations, the network infrastructure, application development and system maintenance functions. The Deputy Chief IT Officer responsibilities include:

- Monitor technology developments and evaluate their impact upon the CHA's information resources.
- Oversee the technical implementation of information technology solutions including but not limited to the IT infrastructure and applications.
- Maintain and enforce effective policies and procedures across ITS functions.
- Assist the CIO in meeting agency wide ITS responsibilities.

3.30 SR. Director, Information Technology Services

The SR Director, Information Technology Services directs and oversees ITS operations, including the network infrastructure, application development and system maintenance functions. The SR. Director, Information Technology Services responsibilities include:

- Monitor technology developments and evaluate their impact upon the CHA's information resources.
- Oversee the technical implementation of information technology solutions including but not limited to the IT infrastructure and applications.
- Maintain and enforce effective policies and procedures across ITS functions.
- Assist the DCIO in meeting agency wide ITS responsibilities.

3.40 MGRINFR – MGR of Infrastructure Information Technology

The MGR of Infrastructure is responsible for managing all aspects of the Organization's Network Infrastructure. This includes Network Security, Server, Storage, Telephony, Security Cameras and LAN\WAN. The MGR of Infrastructure responsibilities include:

- Design and execute short plus long-term strategic plans to assure infrastructure capacity attains current and future needs.
- Develop, execute, and oversee procedures, policies and related training plans for project management and infrastructure administration.
- Manage and establish priorities for maintenance, design, development, and analysis of entire infrastructure systems inclusive of LANs, WANs, internet, security, telephony, security cameras, and wireless implementations.

3.50 Network Security Architect

The Network Security Architect is responsible for handling network security across the Authority. S/he is responsible protecting for developing and coordinating activities related to the CHA's. Network information security program. Responsibilities include:

- Develop, maintain, and help ensure the enforcement of Authority-wide information security policies, procedures, and controls.
- Oversee the deployment and integration of new or enhanced security solutions.
- Serve as an advisor on IT security-related issues across the Authority.
- Develop and execute an ongoing training and awareness program on matters related to information security.
- Assess ITS procedures and activities to ensure appropriate controls are in place for system related activities.

- Ensure the integrity and security of all CHA digital assets and services.

3.60 Inspector General

The CHA's Inspector General's Office investigates potential fraud and waste of the CHA's resources. For information security issues, the Inspector General is responsible for investigating possible fraud or other unscrupulous pursuits resulting from suspicious system activity.

3.70 Department of Procurement and Contracts

The CHA's Department of Procurement and Contracts is responsible for procuring goods and services for the Authority. Information security requirements must be included in procurement activities involving the CHA's information assets. The department's responsibilities include:

- Ensure all solicitation documents and applicable contract components document information security requirements, including how sensitive information is to be handled.
- Monitor vendors' compliance with contractual obligations.

3.80 General Counsel

The CHA's General Counsel oversees the Authority's legal affairs. The Office of the General Counsel provides legal assistance and direction on the CHA's policies, contractual agreements, and regulatory requirements. It also provides guidance on the legal activities related to information security breaches and violations.

3.90 System Owner (Business/Application/Information Owner)

System Owners, also known as Business, Application or Information Owners are information managers and stewards. They are typically management personnel who head functional areas accountable for data in the CHA's systems. System Owners are responsible for ensuring appropriate security, management, and technical controls for their respective systems. Their activities are typically accomplished in partnership with the Information **Network Security Architect.** In accordance with information security guidelines, their responsibilities include:

- Maintain compliance with all the CHA's information security policies and procedures.
- Classify the information they own according to the CHA's information classification system (Page 12).
- Define and communicate the rules for the appropriate use and protection of their systems to users.
- Ensure that users who access their system(s) receive appropriate training.
- Ensure proper segregation of duties in the execution of system-related activities.
- Ascertain who should have access to their respective information system(s) and determine and authorize access rights based on users' job roles.
- Provide timely notification of access modifications (i.e., user account deletions for terminated users).

- Manage system risk and develop and implement any necessary additional controls and procedures beyond this manual.

3.100 Executive Management / Management & Supervisory Personnel

Management personnel include all levels of the CHA's management structure. This includes "C" level personnel (CEO, CFO, COS, CIO), managing directors, directors, managers, and supervisors. Management is responsible for overseeing personnel and / or they are responsible for a functional area in or associated with the Authority. They are accountable for implementing and administering controls in their respective areas. They oversee compliance of the CHA's information security policies and procedures. Responsibilities include:

- Ensure compliance and make users aware of the CHA's information security policies and procedures.
- Handle the information they access according to the CHA's information classification system (Page 13).
- Enforce rules for appropriate use and protection of the CHA's systems.
- Ensure proper segregation of duties in their operational areas.
- Follow appropriate procedures and provide first-line authorization for system access requests.

3.110 Users

All users of the CHA's information assets are responsible for helping to maintain confidentiality, availability, and integrity of the Authority's information. Any person, (including one who falls in any of the roles), who uses any of the CHA's systems is considered a user. Users' responsibilities include:

- Adhere to all the CHA's policies and procedures.
- Protect all user accounts and passwords used to access the CHA's systems.
- Report any known or suspected IT security breaches to appropriate personnel.
- Follow the CHA's incident response process for system-related problems.
- Treat all information with the sensitivity necessary in accordance with the CHA's information classification system (Page 12).
- Safeguard and maintain the accuracy and integrity of data that is accessed, collected, transmitted processed or stored.

4.0 POLICY COMPLIANCE

The CHA's executives and managerial staff are responsible for ensuring compliance with policies and safeguards. To assure policy compliance, the following applies:

- **Responsibility:** Executives and managerial staff are required to implement controls consistent with this policy.

- **Non-compliance:** Parties who do not abide by information security policies and safeguards are subject to disciplinary action, including termination of employment or contracts. Incidents of non-compliance should be reported to the Information **Network Security Architect**.
- **Exceptions:** In rare cases in which policy compliance is not immediately possible, written requests for policy exemptions must be submitted to CHA's Chief Information Officer.
- **Compliance reviews:**

  o Executives and managerial staff may conduct periodic compliance reviews in their respective areas. o The ITS **Network Security Architect** may perform periodic reviews to assess policy compliance.

4.5 Enforcement

This policy will be enforced by the Network Security Architect and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restrictions of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report Such activities to the applicable authorities. property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

5.0 INFORMATION CLASSIFICATION

All the CHA's information must be treated with care. Classifying information by sensitivity and risk is essential in providing a secure environment. The CHA's classification system provides a framework for information handling.

All System Owners are responsible for classifying the information for which they have responsibility. Anyone who handles the CHA's information is accountable for treating information according to its classification. This classification system refers to the sensitivity of data handled. It does not include the time requirements for retention, but it is coordinated with the CHA's Records Retention Schedule.

5.10 Classification Categories

The CHA's classification categories are consistent with Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information, and Information Systems*.

The CHA's Information Classification Categories

Category	Description	Examples	Rules	Potential Impact [1]
Public	Information that can be made available to the public.	• Public press releases • Board resolutions • Responses to FOIA (Freedom of Information Act) requests	• Public information can be released according to the CHA's public release guidelines. However, before information is released to the public, releasers should make sure, that it is in fact public information, and that any request or disclosure is properly undertaken and documented.	Low
Potential	impact refers to the extent to which information mishandling can result in financial loss, disruption, or embarrassment to the organization.	•	•	

Confidential	Confidential information represents the highest level of sensitivity for information resources. It is information that should be protected based on regulatory requirements, CHA policies and/or contractual obligations.	• Social security numbers • Academic records • Certain protected personally identifiable records (PII)	• Disclose to individuals on a need-to know basis. • Disclosure to external parties must be explicitly authorized by executive management (CEO, CFO, COS, CIO General Counsel or a Managing Director). • When stored electronically, this information must be: - stored on protected media - protected with strong passwords and encryption • Hardcopies of confidential data must be protected via strong physical controls (e.g., locked, authorized entry areas)	Extremely High

The Information **Network Security Architect** must be notified immediately if confidential data has been lost or disclosed to unauthorized parties.

5.20 Reclassification

When the risk associated with information changes, it may be subject to reclassification. System Owners are responsible for administering and communicating reclassification to users, as necessary.

6.0 INFORMATION HANDLING REQUIREMENTS

The CHA's information must be handled in accordance with the Authority's information classification system (Page 13). Maintaining confidentiality and appropriate distribution standards are paramount in handling the CHA's information.

6.10 Data Confidentiality

All the CHA's employees, non-CHA employees (including contractors) and organizations (or their agents) who have access to the CHA's information resources are required to maintain the confidentiality of non-public information. A signed data confidentiality agreement is required for all users who access the CHA's data. This agreement must be a part of the following processes:

- Employee and contractor new hire process
- Vendor contracts
- Government, Institutional or other authorized data sharing agreements

6.20 Distribution

To effectively protect information, its distribution must adhere to appropriate security standards. Users must appropriately protect information being distributed internally and externally. The following requirements are designed to help secure the CHA's information:

- Private and confidential information must be appropriately labeled (e.g., "Official Use Only") before distribution.
- Private and confidential data must be encrypted for electronic transmission.
- Private and confidential data must not be transmitted to external (non-CHA) parties without a binding arrangement (e.g., data sharing agreement).

7.0 SECURITY VIOLATIONS / INCIDENTS

All users are required to immediately report security incidents to the CHA Helpdesk or the Information **Network Security Architect**. An incident includes a violation or threat of violation of the CHA's security policies and procedures. Incidents can involve intentional or unintentional infringements. When incidents are reported, corrective action will be taken. Corrective action can include non-disciplinary action (e.g., training). However, it should be noted that violations are subject to disciplinary action, up to and including termination or disassociation with the CHA and/or criminal prosecution. When reported to or discovered by ITS, incidents will be treated with the highest level of sensitivity.

Security violations include, but are not limited to:

- Unauthorized user login attempts
- Sharing or misusing user accounts and passwords
- Revealing passwords to unauthorized parties
- Causing computer virus infections intentionally or negligently

Incidents that are not necessarily violations include:

- Accidentally causing computer virus infections
- Unintentionally exploiting a system vulnerability

8.0 SEGREGATION OF DUTIES

Segregation of duties is essential in maintaining security. It requires that no one person can perform all functions of a business process. Segregating duties also requires preventing one from altering a process without detection. All managers and System Owners are required to ensure appropriate segregation of duties in their respective areas and systems.

9.0 SYSTEM ACCESS REQUEST FORM

System Owners are responsible for defining and enforcing standards for access to and within their systems. System Owners, along with managers must establish the guidelines for appropriate access based on users' job responsibilities. System Access Request Forms (SARF), also known as role-based security, is how user access is maintained according to the specific requirements of his or her function. Access to the CHA's systems must be managed using role-based security standards, which shall occur via the following requirements:

- System Owners must define access levels according to job function, using the principle of least privilege.
- All access to systems must be authorized by respective System Owners.
- When users' job functions change, managers are responsible for requesting and receiving authorization for system access changes.
- System Owners are required to periodically review access to respective systems for accuracy.
- Access logs must be reviewed on regular internals (quarterly, bi-yearly) based upon the criticality of the system

10.0 SYSTEM ACCESS MANAGEMENT

All users who obtain access to the CHA's systems are required to adhere to the CHA's information security policies and procedures. Managing system access is paramount in helping to ensure that only authorized users have access to the CHA's systems.

10.10 Access Authorization

Access authorization processes are as follows:

- ITS Personnel: Network and applications support personnel are responsible for maintaining the CHA's systems. An ITS manager or designee must approve access to system resources on an as needed basis.

- Network (on-site or remote) Access: All requests for network accounts must be approved by a manager or supervisor before submittal to Information Technology Services (ITS) for processing.

- Application Access: All requests for access to applications must be approved by the applicable user's manager and requested application's System Owner (or designee) before submittal to ITS for processing.

10.15 Account Termination Cont.

When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at the company, that employee's account can be disabled. Human Resources must create a process to notify the IT

Manager in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.).

10.20 Modifications to Existing Access

Modifications to user access may be required due to a variety of circumstances, including promotions, transfers, demotions, etc. When modifications are needed, the affected user's sponsoring department is required to notify ITS via the CHA's access modification procedures (documented in the ITS Information Security Procedures document).

10.30 Disabling and eliminating (revoking) System Access

When a user account must be disabled, a request must be immediately submitted to the ITS Helpdesk. Disabling user accounts is necessary under any of the following conditions:

- Upcoming termination of a user's employment or contractual relationship.
- A user's employment or contractual relationship has been terminated.
- System-related suspicious activity has been detected.
- A user's account has been inactive for an extensive time (over 60 days).

Once appropriate post-incident activities have been done, disabled accounts are either reactivated or eliminated (i.e., deleted or permanently disabled) as necessary.
When a request for disabling or deleting an account is made, the requestor must indicate whether files or emails associated with the account should be retained. Otherwise, all files, mailboxes, etc. are deleted when the account is deleted. Deciding whether emails, files, etc. should be retained must be based on the CHA's Records Management Policy.

10.40 Remote Access

Remote access encompasses access to the CHA's information technology resources from a location other than the CHA's central office. Remote access users are required to adhere to the same requirements used for all network and application access. Due to the increased exposure of remote access, the following additional rules apply:

- MFA (Multi-Factor) authentication method must be used when accessing systems whether internally or remotely.
- Users with remote access privileges must protect their connection from non-CHA users (e.g., family members, etc.).
- Remote access users are fully responsible for all activity associated with their remote access connection.
- All hosts that connect to the CHA's network remotely must use the most recent version of CHA-approved anti-malware (anti-virus and anti-spyware) software.
- Equipment that connects remotely to the CHA's network must meet the CHA's standard hardware and software specification requirements.

10.50 Wireless Access

All wireless communications must adhere to the CHA's information security policies and procedures. Requirements specifically related to wireless access include the following:

- Users are not allowed to implement access points on the CHA's network. Only ITS installed access points are permitted on the CHA's network.
- All wireless access must be configured by the CHA's ITS department. Non-ITS wireless configurations are not allowed.
- All wireless configurations must include the CHA's ITS-approved authentication mechanisms.

10.60 Creation of Contract users

Prior to the creation of contract user accounts, access will only be granted after the completion of a System Access Request Form. This form can only be initiated by the appropriate department head, and must be signed by the department head, and by the appropriate personnel. These guidelines include before given rights to access any resources (I-Files, Yardi, Lawson etc.).

This guideline satisfies the "need to know" requirement of the Authority regulations, since the supervisor or department head is the person who most closely recognizes an employee's need to access data. Users may be added to the information system, network **only** upon the signature of the appropriate personnel who is responsible for adding the employee to the network in a manner and fashion that ensures the employee is granted access to data only as specifically requested.

11.0 USER IDENTIFICATION AND AUTHENTICATION

11.10 Identification and Authentication Requirements

Any user who accesses the CHA's systems must be properly identified and authenticated. To ensure this, the following requirements apply:

- A user must have her / his own, unique user account(s) to access the CHA's systems.
- Users must not share user accounts.
- Users are personally responsible for maintaining their user accounts and passwords.
- Users must adhere to the CHA's password policy when creating their passwords.
- Network (on-site or remote) Access: All requests for network accounts must be approved by a manager or supervisor before submittal to ITS for implementation.

11.20 Network Password Policy and Management

Strong password standards are required for access to the CHA's systems. Network passwords must adhere to the following requirements:

- **Password Format -** Network passwords must:

o Contain upper- and lower-case characters o Include digits as well as alphabetic characters o Have a length of at least six characters o Password should not contain common words. (example: Password 1, CHA123)

- **Account Lockout -** An account lockout process is instituted for network user accounts, which disables accounts after six login attempts.

- **Password History -** Network account password history is set to prevent excessive reuse of a password. A user must not use any of his/her previous six passwords when s/he is prompted to change a password.

- **Password Changes -** Users are required to change their passwords every 60 days.

11.30 Application, Telecommunication and Other Passwords

Passwords for applications, voice mail and other systems (e.g., cell phone locks) should adhere to strong password standards to the extent possible. The CHA's identification, authentication and privacy standards are required for all passwords including those for applications, telecommunications, and other systems.

11.40 Password Privacy

Passwords must be treated as confidential information. They must NOT be revealed to anyone. If someone demands a password reveal, they should be referred to the **Network Security Architect** or ITS Helpdesk. If an account or password has been compromised, the affected user should change all passwords and report to the Information **Network Security Architect** or ITS Helpdesk immediately. To help ensure password privacy, users must adhere to the following guidelines:

- Do not insert passwords in electronic communication (e.g., emails).
- Avoid writing passwords down.
- Avoid storing passwords in files or Personal Digital Assistants unless encrypted.
- Never share your password with anyone.

11.50 Password Resets

Password reset should be done via self-service password reset tool. However, if the utility is not available, password should be reset by contacting ITS Helpdesk. Further, password reset requests are tracked and analyzed to determine excessive password resets for a user. Users that have excessive password resets are assessed for user training or other corrective action.

12.0 PHYSICAL ACCESS CONTROLS

Physical controls include protective mechanisms that restrict entry into areas containing IT equipment. The following access controls apply to all CHA and CHA-related (CHA contractor facilities) locations.

- Access to areas must be limited to authorized personnel.
- Access to locations that contain IT equipment must require appropriate identification (e.g., entry access card).
- Visitors must be identified and authorized for entry.
- Unattended equipment (e.g., laptops) should be physically secured (via locking cables, locked cabinets, etc.).

All users are responsible for physically protecting sensitive (private and confidential) information.

13.0 SYSTEM BACKUP AND RECOVERY

To help ensure system availability, users are responsible for maintaining appropriate backups for information. Users must maintain their backups in accordance with their respective area's backup and recovery standards and / or Business Continuity Plan. The CHA's ITS resources must be backed up in accordance with its Disaster Recovery Plan.

Retaining information must be done in accordance with the CHA's Records Management Policy.

14.0 MEDIA CONTROLS

Media controls are designed to protect information stored electronically or as hardcopy. Media includes the physical means by which data can be stored, including paper, hard drives, and removable media such as flash drives etc. Protecting information requires effective safeguards related to media handling including storage and disposal.

14.10 Media Handling

- Users must physically protect media in their possession to avoid damage.
- Users are responsible for creating their own backups of media in their possession.
- Media containing sensitive information (classified as private or confidential) must be treated according to the following requirements. Sensitive media:
    - Should be labeled with its classification and associated special handling instructions.
    - Must be secured when not in use (e.g., kept in a locked cabinet). o Should be appropriately sealed and specially marked when transported by courier or special mailing service.
    - Should include delivery confirmation procedures when transmitted by courier or special mailing service.
- When users' employment or contract is terminated, their respective manager(s) must make sure any media with the CHA's information is returned to the CHA's possession.

- Lost media containing sensitive information must be reported immediately to the Information **Network Security Architect**.

14.20 Media and Information Disposal

Before destroying media or associated information, users must refer to the CHA's Records Management Policy to ensure that disposal is appropriate. The following requirements must be followed when destroying media pursuant to authorized procedures, practices, and methods:

- Media containing private or confidential information must be sanitized before disposal.
- Before computers or storage media are transferred from an original user to another party, the equipment must be sanitized.

14.30 Portable (Removable) Media

Portable media is media that can be easily moved and transported (e.g. Flash drives, etc.). Portable media should not be removed from the CHA's sites unless explicit approval from a manager has been given. Managers should give this approval only in cases that require it for the performance of assigned job duties. The following additional requirements apply for portable media:

- Private or confidential information should only be stored on portable media when it is encrypted.
- **Cloud Storage (CHA OneDrive) is the only approved cloud storage for company owned assets).**
- Any media attached to the CHA's computers must be scanned for malware (viruses and spyware).

15.0 USER HARDWARE AND SOFTWARE SECURITY

Users are accountable for protecting the equipment they use during their work activities. User equipment includes workstations, laptops, and mobile devices.

15.10 General Requirements for Computer Equipment and Software

To ensure proper security for the CHA's systems, users must adhere to the following rules for computing equipment and software:

- All users are required to log off or lock unattended workstations.
- The CHA's equipment must not be removed from CHA sites without management approval.
- All the CHA's equipment must be returned to the CHA upon request or upon employment termination or disassociation from the Authority.
- Only licensed and approved software (applications and operating systems) can be used on CHA or CHA ITS supported equipment.

- Users must not install software (e.g., freeware downloads) unless expressly approved by the CIO.
- Users must not use personally owned equipment and/or software to process or store sensitive CHA information (classified as private or confidential).

15.20 Laptop Security

Laptop use must meet the CHA's information security policies and procedures, including those detailed in 15.10 General Requirements for Computer Equipment and Software. Given the portable nature of laptops, specific laptop protection requirements include the following:

- Sensitive data stored on laptops must be encrypted.
- Protect against physical theft by using anti-theft mechanisms (e.g., laptop locks).
- Laptop damage, theft or loss must be reported to the ITS Helpdesk immediately.
- To ensure appropriate malware protection and patch management, laptops must be connected to the CHA's network at least once a week.

16.0 INFORMATION TECHNOLOGY CODE OF CONDUCT

All CHA systems are to be used for official purposes in serving the interests of the Authority. The CHA's system users have no expectation of privacy for information sent, received, or stored in any of the CHA's systems. Systems must be used in accordance with the Authority's policies, including the communications policy, the employee code of conduct and the ethics policy. It is the responsibility of all system users to know applicable policies and conduct themselves accordingly. Inappropriate use of system resources exposes the organization to the risk of viruses, compromise of resources and legal vulnerability.

16.10 Limited Personal Use

Although Internet and e-mail access are to be used for the CHA's business, employees are permitted personal usage on a very limited basis. Managerial staff is responsible for ensuring that proper constraints on personal use are established in their respective areas. Managers reserve the right to deny personal use as deemed necessary. Any limited personal use must adhere to the following requirements:

Limited personal use must NOT:

- Interfere with the performance of work duties.
- Violate any of the CHA's policies, including those written in the employee handbook.
- Involve running a business.
- Cause degradation of system services (e.g., network slowdowns).

- Contractors and other non-CHA employees are not authorized to use the CHA's information resources for personal use unless it is specifically permitted via applicable contracts.

- Users have no expectation of privacy rights related to the use of the CHA's information resources. The CHA reserves the right to monitor use without prior notice.

16.20 Network Usage

Network use requirements apply to all users who access the CHA's network resources. The following requirements apply:

- The CHA's network is to be used for Authority business. Limited personal use requirements are found in section 16.10 of this policy.
- Users may only connect to the CHA's network via ITS-approved equipment (e.g., computers, printers, or other end-point devices) and ITS-approved connectivity media (e.g., cabling).
- Users must not connect non-ITS approved cables to the CHA's network jacks.
- Network (on-site or remote) Access: All requests for network accounts must be approved by a manager or supervisor before submittal to ITS for implementation.
- Users must not, in any way, attempt to extend or modify the network by installing infrastructure devices, such as hubs, switches, bridges, or routers.
- Network users have no expectation of privacy rights related to anything they store, send, or receive on the CHA's network. The CHA reserves the right to monitor network traffic without prior notice.

16.30 Email Usage

Email use requirements apply to all users who send and receive email on behalf of the CHA.

- The CHA's email system is to be used for Authority business. Limited personal use requirements are found in section 16.10 of this policy.
- The CHA's email system must not be used to create or distribute disruptive or offensive messages, including, but not limited to, offensive statements regarding race, gender, age, disabilities, religious beliefs, political beliefs, sexual orientation, or national origin.
- Transmitting inappropriate items such as chain letters and/or pornographic images is forbidden.
- Email users have no expectation of privacy rights related to anything they store, send, or receive on the CHA's email system. The CHA reserves the right to monitor email messages without prior notice.

16.40 Internet Usage

The Internet can be a valuable resource for the CHA's users. However, misusing it can expose the CHA to various risks. For example, using the Internet to download personal music can expose the CHA to malicious code and it can slow down the network for the entire organization. Internet usage requirements apply to all users who access the Internet from the CHA's network.

- The Internet is to be used for Authority business. Limited personal use requirements are found in section 16.10 of this policy.
- Users must not intentionally access inappropriate sites (e.g., pornographic web sites).

- Users must not use the Internet for personal downloads (e.g., personal music, video games, etc.).
- Users must not download non-ITS approved software from Internet sites.
- Users should not use the Internet for personal financial transactions (e.g., e-commerce transactions).
- Users who access the Internet via the CHA's network have no expectation of privacy rights. The CHA reserves the right to monitor Internet usage without prior notice.

16.50 Social Media Usage

Social Media is defined as any online tool or application that goes beyond simply providing information, instead allowing collaboration, interaction and sharing. Example of social media include, blogs, microblogs, wikis, photos, videos, podcasts, virtual worlds, social networking, social newsrooms, web conferencing, webcasting etc.

Social Media can be a valuable resource for the CHA's users if utilized properly. However, misuse of social media may expose CHA to various risks. For example, using social media to download files may expose the CHA computer assets to malicious code. It can also slow down the network for the entire organization. Consequently, posting confidential and non-public information to social media can lead to the leak of propriety information of the agency.

Official use of Social Media:

- Only officially approved accounts be used to communicate via social media.
- Official social media accounts be administered & maintained by the authorized individuals only.
- No administrator can share the password of any social media account to any unauthorized individual or entity.
- Social media communication in connection with the transaction of public business should be posted solely from a CHA social media account and not from a personal social media account.
- Social Media account must be clearly identifiable by using the appropriate naming conventions and consistently used design elements (i.e. background colors, images, and link back to the official and relevant section of the CHA website.
  To establish a new social media account or new social media channel, prior appropriate approval must be sought.
- The CHA authorities may review & observe contents and information made available by the employee, contractor, or other affiliates through social media.
- Employee, contractors, and all affiliates should get appropriate permission before referring or posting of image or images of a current or former employees, members, vendors, or suppliers. Additionally, appropriate permission to be sought to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- Configure social media accounts to encrypt sessions whenever possible. This is extremely important for roaming users who connect via the CHA WI-FI networks.
- If mistakenly posted information on social media, contact Ethic Officer immediately and fully informed the incident.

- In the event of hacking of a social media account, administrator must notify the appropriate parties immediately.
- Do not use the same passwords for social media that you use to access the CHA's computing resources.
- Follow all privacy and confidentiality guidelines in employee's handbook. As well as all applicable laws such as copyright, fair use, and financial disclosure laws.
- Adhere to the Ethics Policy of CHA while using social media.

Personal Use of Social Media:

- Ensure NOT to post any confidential material (text, picture, video, or another form of information) which may cause harm to the reputation of the CHA.
- Ensure NOT to represent CHA in any form or shape as an official or employee of CHA.
- Configure social media accounts to encrypts sessions whenever possible. This is extremely important for roaming users who connect via the CHA WI-FI networks.
- Do not use the same passwords for social media that is used to access the CHA's computing resources.
- If mistakenly posted information on social media, contact Ethic Officer immediately and fully informed the incident.
- Follow all privacy and confidentiality guidelines in employee's handbook. As well as applicable laws such as copyright, fair use, and financial disclosure laws.
- Adhere to the Ethics Policy of CHA while using social media.
- The CHA reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Acceptable Use:

- Acceptable use defines business use activities that directly or indirectly support the business of the CHA.
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing during breaks or lunch hours.
- Employees may use their mobile devices to access the following company-owned resources:
    - Emails o Calendars o Contacts o Non-Confidential Documents & Data o Any related material to perform one's job
- Devices may not be used at any time to:
    - Store or transmit illicit materials o Store or transmit proprietary information to Harass others to Engage in outside business activities

- CHA has a zero-tolerance policy for texting or emailing while driving to conduct CHA business, only hands-free talking while driving is permitted.
- Only connectivity issues are supported by ITS, employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.
- Devices must be available for inspection b ITS for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the CHA network.

Security of devices & Data:

- To prevent unauthorized access, devices must be password protected using the features on the devices and a strong password is required to access the company network.
- The device must lock itself with a password or PIN if idle for more than five minutes.
- Rooted (Android) or jailbroken (iOS) devices are forbidden from accessing the CHA network.
- Employees' access to company data is limited based on user profiles defined by ITS and 'need to know' basis.
- The employee's device may be remotely wiped by the CHA data if:
    - The device is lost or stolen
    - The employee terminates his or her employment
- ITS detect a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure
- Without any visible cause based upon ITS risk determination

Risks, Liabilities & Disclaimers:

- While ITS will take every precaution to prevent the employees, contractors & affiliates personal data from being lost in the event it must wipe a device, but it is the employees, contractors & affiliates' responsibility to take additional precautions, such as backing up emails, contacts, calendar etc.
- CHA reserves the right to disconnect any device or disable any service provided by the CHA without notification.
- Lost or stolen devices must be reported to the ITS within 24-hours. Employees, contractors & affiliates are responsible for notifying their mobile carrier immediately upon loss of devices.
- All employees, contractors & affiliates are always expected to use their devices in ethical manners and adhere to the CHA acceptable user policy as outlined above.
- All employees, contractors & affiliates are personally liable for all costs associated with their device.
- All employees, contractors & affiliates assumes fully liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, error, bugs, viruses, malware, and / or other software or hardware failures, or programming errors that render the device unusable.
- The CHA reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

16.70 Clear Desk

All the CHA's users must maintain a "clear desk" policy. Users must make sure that sensitive information and equipment is secured and out of open view (if possible) when desks are unattended.

References

City of Chicago, Department of Innovation and Technology (Do IT), Social Media Policy, 2014,2015

Chicago Police Department, General Order G09-01-06 – Use of Social Media Outlets, 2014 CHA Board Approved Ethics Policy. The Chicago Housing Authority, April 21, 2015.

Chan, Jason. Essentials of Patch Management Policy and Practice. Patchmanagement.org. January 31, 2001. < http://www.patchmanagement.org/pmessentials.asp>

Chew, Elizabeth, Marianne Swanson, Kevin Stine, Nadya Baratol, Anthony Brown and Will Robinson. Performance Measurement Guide for Information Security. National Institute of Standards and Technology, US Department of Commerce. NIST, SP 800-55, Gaithersburg, MD, September 2007. <http://csrc.nist.gov/publications/drafts/800-55-rev1/Draft-SP800-55r1.pdf>

Communications Equipment Policy. The Chicago Housing Authority.

Computer Security Act of 1987. 40 USC 759, 101 STAT 1724. PL 100-235, Washington, DC. 01/08/1988.

Computer Fraud and Abuse Act of 1986. 18 USC 1030, PUBLIC LAW 99-474, Washington, DC, 10/16/1986.

Electronic Communications Privacy Act. 18 USC 2510, 100 STAT 1848, PUBLIC LAW 99508, Washington, DC. 10/21/1986.

Employee Handbook. The Chicago Housing Authority. 1 April 2007.

Federal Information Security Management Act of 2002. 44 USC 3541, 116 STAT. 2899. PUBLIC LAW 107-347, Washington, DC. 12/17/2002.

Information Systems Security Policy. The Chicago Housing Authority. Office of Information Technology Services, Systems Security Division. December 2003.

Information Technology Security Policy. U.S. Department of Housing and Urban Development. May 2005.

Media Management. The SANS Security Policy Project. 8 December 2004. <csrc.nist.gov/groups/SMA/fasp/documents/production_io_controls/Media-Management.pdf>

National Information Infrastructure Protection Act of 1996. PUBLIC LAW 104-294, Washington, DC. 10/04/1996.

Privacy Act of 1974, As Amended. 5 USC 552a, PUBLIC LAW 93-579, Washington, DC. 07/14/87

Records Management Policy. Chicago Housing Authority. 13 July 2004.

Sarbanes-Oxley Act of 2002. 117 STAT. 745. PUBLIC LAW 107-204, Washington, DC. 07/30/2002.

U.S.A. Patriot Act. 115 STAT. 272, PUBLIC LAW 107-, Washington, DC. 10/26/2001.

Reviewed by Chief Information Officer: Anna Chen Anna Chen (Nov 18, 2024 14:28 CST) Date: 11/18/2024

Reviewed by Director, Infrastructure & Security: Trish Domask Date: 11/18/2024

EXHIBIT II. INVESTMENT & CASH MANAGEMENT POLICY

I. Policy.

Through the primary role of providing and sustaining affordable, decent, safe and stable housing, Chicago Housing Authority (CHA) is committed to empowering low-income families and residents served throughout Chicago to achieve long term economic success and empower Chicago's communities to thrive.

This policy approved by the Board of Commissioners (BOC) is intended to establish criteria that will protect CHA 's financial integrity while setting forth general guidelines for the treasury management practices. Treasury management activities include, but are not limited to, the management of cash and investments, liquidity, debt, banking relationships and financial risks.

Investment Management

II. General Provisions.

CHA invests funds of CHA, its affiliates, and instrumentalities to maximize financial capacity and community impact as a return on investment. CHA funds are to be invested in a manner that will meet the objectives of ensuring the safety of principal, provide sufficient liquidity to meet anticipated expenditures, and maximize the return on investment.

Excess funds of the CHA shall be invested in accordance with this policy, while fulfilling the following objectives:

1. Safety of principal is the primary objective. CHA investments shall be undertaken in a manner that seeks to ensure the preservation of capital. To attain this objective, diversification is required to ensure that market, interest rate, and credit risks are managed.

2. The investment portfolio must be sufficiently liquid to meet anticipated operating expenditures when such expenditures become due, based on daily, weekly, quarterly, and annual cash flow projections.

3. The investment portfolio should achieve the highest yield possible, consistent with the above stated objectives of safety of principal and liquidity and allowing for risk factors such as market fluctuation in price and interest rate trends.

A. Definitions.
   1. "BOC" means the Board of Commissioners of the CHA.
   2. "CEO" means the Chief Executive Officer of the CHA.

3. “CFO” means the Chief Financial Officer of the CHA.
4. “ICMC” means the Investment and Cash Management Committee.
5. “HUD” means the United States Department of Housing and Urban Development.

B. Investment Authority.

The BOC will review and approve the policy on an annual basis. The BOC Finance and Audit committee has authority and responsibility to monitor adherence to the policy and recommend policy changes to the BOC for approval.

The CEO and the CFO have the authority to appoint one or more appropriate staff members to manage the CHA’s portfolio of investments in a manner consistent with this policy.

The Treasurer is the primary manager of the investment portfolio and, in consultation with the CEO and CFO, may form an Investment & Cash Management Committee (“ICMC”) to oversee compliance with this policy.

The Treasurer and/or Treasury Directors are authorized to make day-to-day investment decisions within this policy and as guided by the Investment and Cash Management Committee.

1. Trade Dollar Limits.

The maximum single security purchase is limited to $10,000,000. The sale of securities as recommended by the Treasurer requires CFO and CEO approval on a case-by-case basis.

2. Portfolio Maturity.

Management shall monitor and adjust the duration of the portfolio in consideration of the following factors:

a. The current level of, and anticipated changes in, interest rates and shape of the yield curve. The Investment & Cash Management Committee shall decide appropriate duration and benchmark performance comparisons for each portfolio no later than Jan 30th. The determinations will be based upon liquidity and budgetary requirements by fund while considering economic conditions.
b. Size, indicated by Individual bonds in excess of $10 million by CUSIP[1] number.

3. Portfolio Benchmarking.

The yield performance benchmark of the portfolio will be the 12-month rolling average of the US Treasury Constant Maturity (CMT) 1-year plus 10 basis points.

[1] A CUSIP is a nine-digit numeric or nine-character alphanumeric that identifies a North American financial security for the purposes of facilitating clearing and settlement of trades.

Duration and benchmark determinations will be presented to the Audit and Finance Committee at the first meeting of the Board of Commissioners of each fiscal year. Throughout the year, any actual duration changes greater than 25% of target duration will be reported to the Audit and Finance Committee as well.

a. Core Portfolio – This represents those funds received in the CHA's normal and recurring course of business. Typically, grants and other funds received from HUD used in the operation and management of the CHA's housing portfolio.

Examples: Performance Funding System (PFS) (Operating), Housing Choice Voucher (HCV), and any other HUD funds; Agency program income, or operating funds which are derived from other sources.

Maximum Duration Limit - 6 to 24 months OAS (Option Adjusted Spread) Basis
Performance Benchmark - 6-to-12-month Treasury Bill (or similar comparative index)

b. Restricted Portfolio - Restricted Portfolio funds are typically restricted, or reserve funds held and invested for identified use for periods exceeding one year. These funds may also be considered fund/program equity resulting from revenues, which exceed expenses on any given fund/program.

Examples: Insurance Reserve, Project Bond Funds, HOPE VI, non-federal funds, and various program operating reserves and/or collateralized lending programs.

Maximum Duration Limit - 1-to-5-year OAS (Option Adjusted Spread) Basis
Performance Benchmark 1-to-2-year Treasury Note (or similar comparative index)

c. CHA LLC Portfolio - Funds required for the operation of properties and administration of Rental Assistance Demonstration (RAD) -PBV funds may consist of operating, administrative, capital escrow, security deposit and replacement reserve funds.

Duration for operating, administrative & security deposits – 6 to 24 OAS (Option Adjusted Spread) Basis
Performance Benchmark - 6-to-12-month Treasury Bill (or similar comparative index)

Duration for Capital Escrow - 1-to-5-year OAS (Option Adjusted Spread) Basis
Performance Benchmark 1-to-2-year Treasury Note (or similar comparative index).

Duration for Replacement Reserve - 1-to-5-year OAS (Option Adjusted Spread) Basis.
Performance Benchmark 1-to-2-year Treasury Note (or similar comparative index).

d. Special Purpose Portfolios – Special purpose portfolios may consist of non-federal grants, funds and/or other funding revenue which are received from alternative sources, such as bond proceeds, project and payment funds, debt service reserve, etc. Some sources may have restricted uses and timing. Additionally, any portfolio defined as special purpose upon reaching $5 million total balance can be established and reported to the Board of Commissioners Audit and Finance Committee.

Maximum Duration Limit - 1-to-5-year OAS (Option Adjusted Spread) Basis. Performance Benchmark 1-to-2-year Treasury Note (or similar comparative index).

4. Other Requirements:

All demand deposits in excess of the FDIC insured deposit limit (currently $250,000) must be 100% collateralized with U.S. government securities or FHLB Public Unit Deposit Insurance for non-Low Rent Public Housing. All duration and performance benchmarks subject to market conditions.

III. Reporting and Monitoring Governance.

Management will prepare at least quarterly reports for the Audit and Finance Committee's review. The reports shall include the following information:

- Total portfolio size in dollars
- Asset class breakdown in percentage terms
- Portfolio yield
- Unrealized gain or loss
- Asset class balances
- Asset class balances compared to policy concentration limits.

The Treasurer is responsible for developing an Annual Cash Flow Forecast derived from the BOC-approved CHA's Comprehensive Budget for the fiscal year beginning January 1st through December 31st. The Annual Cash Flow Forecast for the fiscal year should be completed no later than March 1st of that year. It shall be approved by the ICMC during the first quarter meeting and presented to the Audit and Finance Committee of the BOC.

On an annual basis, or more frequently, if necessary, the CFO and/or Treasurer will update the CHA's overall Investment Plan and present it to the Audit and Finance Committee.

IV. Account Classification for Securities Purchased.

CHA is required to prepare and report its financial statements in accordance with GAAP and GASB standards.

V. Eligible Investments and Limits.

A. US Government Securities:

- United States Treasury Bills
- United States Treasury Notes and Bonds
- United States Treasury Strips
- Tennessee Valley Authority (TVA) Notes, Bonds, and Strips
- Overseas Private Investment Corp (OPIC) - Sovereign Agency US
- Money Market Deposit & Super Now Accounts that are 100 % backed by US Gov't Securities
- Interest-Bearing Savings Accounts and Time Deposits or Certificates of Deposits issued by financial institutions which are insured and/or collateralized 100% by Government Securities
- Repurchase Agreements. The securities, unless registered or inscribed in the name of the CHA, shall be purchased through banks or trust companies authorized to do business in the State of Illinois. The term "repurchase agreements" as used herein shall include flexible repurchase agreements that permit the CHA to withdraw funds as needed and master repurchase agreements that permit the deposit, withdrawal and redeposit of funds over time and do NOT exceed 30-day maturities.
- Mortgage-backed Securities and CMOs issued by GNMA.
- HUD Project Notes
- Housing (HUD) Government Sponsored Enterprises (GSE)

B. Federal Agency Securities:

- Farm Credit Consolidated System (FFCB) Discount Notes, Notes and Bonds
- Federal Home Loan Bank (FHLB) Discount Notes, Notes and Bonds
- Federal National Mortgage Association (FNMA) Discount Notes, Notes and Bonds
- Federal Home Loan Mortgage Corporation (FHLMC) Discount Notes, Notes and Bonds
- Farmer Mac (FRM) Discount Notes
- Financing Corp (FICO) Notes, Strips
- Private Export Funding Corp (PEFCO)
- SBA (Asset Based Product is Guaranteed by Lender)
- Mortgage-backed Securities and CMOs issued by FHLMC & FNMA

C. State of Illinois Securities:

- Interest-Bearing Savings Accounts and Time Deposits or Certificates of Deposits issued by financial institutions which are insured and/or collateralized 100% by FHLB Public Unit Deposit Insurance for all other programs
- State/Municipal Obligations
- Illinois Housing Development Authority Mortgage Participation Certificate
- Public Treasurer’s Investment Pool – section 17 State Treasurer’s Act Non-amortizing US

- Commercial Paper – short term obligations of corporations

Note – see appendix for full list of eligible investments

D. Concentration:

Government Securities are limited to a maximum maturity of 5 years.

The aggregate total of all guaranteed US Government Securities and Agencies by issuer may not exceed 25% of the investment portfolio assets. All other security types by issuer may not exceed 5% of the total portfolio's value and may be invested in securities issued by a single entity, except for securities issued or guaranteed by the U.S. Government or U.S. Government agencies and U.S. Government money market funds with same day fund availability.

VI. Prohibited Investments.

The following transactions are not deemed in compliance with current applicable policy/statute and are prohibited:

- When Issued Trading – trading of security prior to issuance
- Reverse Repurchase Agreements – the loaning of CHA securities for cash proceeds
- Securities Lending – the loaning of CHA securities for other cash and/or securities
- Short Selling – the sale of a security the CHA does not own.

VII. Safekeeping.

The CHA has approved the following list of safekeeping agents for the investments:

- Federal Reserve Bank
- BMO Harris Bank
- Bank of New York
- Fifth Third Bank
- Bank of America
- J.P. Morgan Chase Bank

All banks will be examined by net capital, financial strength, and reputation in the industry.

VIII. Authorized Broker/Dealers.

A. The CHA will transact investment securities with broker/dealers who are registered with the SEC.

B. For each securities dealer with which the CHA does business, the following information will be kept on file:

1. Company Name
2. Company Address
3. Contact person name, number, and email address
4. Annual audited financial statements
5. Part 2 for National Association of Securities Dealers (NASD)
6. Any debt ratings from security agencies or any related disclosure statements

C. All documentation concerning approved broker/dealer/financial institutions must be maintained in accordance with CHA document retention policies.

D. The following parties are approved to conduct investment transactions with the CHA:

(hidden)

E. All brokers and dealers and anyone conducting investment transactions will be examined by net capital, financial strength, and reputation in the industry. A Request for Information (RFI) process will be used for identifying and selecting the most qualified parties that will best match and serve the CHA's investment needs.

IX. Internal Controls and Documentation.

A. The CHA shall conduct an annual review of the earnings performance, capital level, credit rating and operational results of any institution or entity that has a concentration of 5% or more of the CHA's total investment portfolio assets which include cash and cash equivalents.

B. Internal Audit shall conduct a bi-annual audit and review including:
   1. Sample of transactions during prior 12-months
   2. Authorized staff members who approved each transaction

C. There will be an adequate division of responsibilities among those who execute investment transactions and those who perform trade confirmation and settlements as well as accounting procedures or reporting and control activities. Such arrangements reduce the risk of undetected error and limit opportunities to misappropriate assets or conceal intentional misstatements in the financial statements.

X. Investments Falling Outside Policy.

If an investment falls outside board policy or fails a requirement within 30 days after purchase, the Treasurer must notify the CFO/ICMC and the Audit and Finance Committee within 45 days with a recommendation and timeframe to bring the portfolio back in line.

Cash and Liquidity Management

XI. General Provisions.

A. CHA manages cash to achieve its liquidity management goals that include providing sufficient liquidity to support the cash flow needs of the annual operating cycle, investments, remarketing risk for put-able debt and optimal credit ratings. The cash and liquidity management activities are guided by principles and requirements stated by the U.S. Department of Housing and Urban Development (HUD); Cash & Investment Guidelines & Procedures Notice PIH 2002-13 (HAs).

B. Efficient cash management strategies, techniques, and procedures will be used to achieve the following objectives:

    1. Liquidity – maintain the ability to pay obligations when they become due

    2. Cash Optimization – establish systems and procedures that minimize investment in non-earning cash resources while providing liquidity and security

    3. Financing – obtain both short- and long-term borrowed funds in a timely manner at an acceptable cost

    4. Financial Risk Management – monitor and assist in the control of exposure to interest rates and other financial risks

    5. Coordination - ensure that cash management goals are communicated and integrated with the strategic objectives and policy decisions of all areas of the CHA that impact cash flows

C. The Treasurer shall authorize the opening and closing of any checking and savings accounts. The Treasurer is authorized to appoint Treasury Director to make day-to-day management decisions and reporting related to cash and liquidity management activities. The Treasurer must maintain oversite and ensure adequate tracking and reporting of transactions and trades in line with this policy and Treasury procedures. The Treasurer shall monitor the lines of credit usage to ensure liquidity needs are met. For any line of credit, prior to draws, Treasurer must obtain approval from the ICMC and approval from the chair of the BOC Audit and Finance Committee.

D. Cash related duties, such as maintenance of accounts receivable, cashiering, accounting, disbursing, and collecting funds shall be segregated. The accessibility to funds and fund records shall be restricted and administratively controlled.

E. CHA must designate a bank account for the deposit of payments that are received from HUD through Direct Deposit-Electronic Funds Transfer (DD-EFT). A Standard Form 1199A must be submitted to designate this account. A signed General Depository Agreement [HUD Form 51999] will be maintained with each bank as required by HUD.

F. The Treasury Director develops an Annual Cash Flow Forecast derived from the Board-approved CHA's Comprehensive Budget for the fiscal year, which must be reviewed and approved by Treasurer. Diversification may be achieved via various sources of liquidity, in order to effectively manage liquidity risk.

XII. Banking Relationship Management.

Banking services will be secured through competitive solicitation to assure CHA receives the highest quality of banking services at the lowest possible cost.

Banking services are currently provided by the following parties:

- BMO Harris Bank NA
- J.P. Morgan Chase Bank
- Fifth Third Bank
- Federal Home Loan bank
- Bank of New York (Mellon)

Treasury shall conduct an annual review of the banking relationships and performance and will submit the internal Annual Bank Review Summary to the ICMC.

Counterparty credit risk shall be closely monitored and proactively managed. A minimum credit rating of A- is required for establishing and maintaining a banking relationship with CHA. Counterparty credit ratings should be reviewed and updated as part of the quarterly treasury reporting activities.

Debt Management

XIII. General Provisions.

The use of debt plays a critical role in ensuring adequate and cost-effective funding for CHA's capital plan. The CHA's debt issuance activities and procedures shall be aligned with the CHA's vision and goals.

The policy commits CHA to manage the financial affairs so as to minimize financial and legal risks and maximize future debt capacity, while providing for public accountability and transparency.

CHA will not issue long-term debt to finance current operations.

A. Legal Authority.

   CHA will adhere to the requirements of the Illinois Housing Authorities Act 310 ILCS 10/1, et seq., (the "Act") and the Local Government Debt Reform Act, 30 ILCS 350/1 et seq., (the "Debt Reform Act"), which govern CHA's ability to borrow money to issue bonds, notes, debentures, or other evidence of indebtedness, and to secure the same by pledges of its revenues, or in any other manner.

B. Purposes and Uses of Debt Proceeds.

   The Illinois Housing Authorities Act 310 ILCS 10/8.4, et. seq., (the "Act") states that a public housing authority for a municipality having a population in excess of 1,000,000 may borrow, lend and issue revenue bonds for the purposes of financing the construction, equipping, or rehabilitation or refinancing of multifamily rental housing.

The CHA may issue debt for any of the purposes set forth in the Act, including but not limited to, to finance in whole or in part the cost of acquisition, purchase, construction, reconstruction, improvement, alteration, extension or repair of any project or undertaking, to acquire and dispose of improved or unimproved property, to remove unsanitary or substandard conditions, to construct and operate housing accommodations and to regulate the maintenance of housing developments.

C. Governance.

The CHA's Board of Commissioners shall approve any and all debt financing of federal or non-federal funds in excess of $250,000. As applicable, HUD approval for debt financing transactions shall be obtained.

The CFO has overall responsibility for debt management. The CFO and General Counsel coordinate their activities to ensure that all debt is in compliance with applicable federal and state laws and resolutions of the various governing bodies.

The CEO and the CFO may appoint one or more appropriate staff members to perform the duties of debt management in a manner consistent with this policy.

The Treasurer is the primary manager of the debt portfolio and is authorized to appoint staff to assist in making day-to-day debt management decisions and performing other debt-related duties with this policy.

D. CHA will:

1. Manage capital structure and planning and assess borrowing needs and debt capacities.

2. Maintain access to financial markets and ensure funds are available to meet funding requirements.

3. Manage CHA's credit rating and attain the best possible credit worthiness for cost-effective borrowing while preserving financial flexibility.

4. Minimize debt service and issuance costs as well as financial risks to operations.

5. Ensure full and timely repayment of debt.

6. Optimize overall funding and portfolio management strategies (e.g. fixed/floating rate mix, average life, weighted average cost of capital, liquidity objectives, etc.) and identify metrics to monitor debt capacity and affordability.

7. Establish a control framework for approving and managing debt portfolio.

8. Ensure compliance with applicable State and Federal laws.

Debt may be publicly issued or privately placed and may be issued on either a long-term basis ("Long-term Borrowing") or short-term basis ("Short-term Borrowing") with the types of debt that are consistent with the provisions of this Policy and regulatory requirements.

E. Debt Limits

CHA will maintain guidelines that ensure a balance between debt service and all other housing authority expenditures. These guidelines are to be reviewed annually to determine applicability and appropriateness.

F. Debt Structuring

When structuring a debt issue, consideration should be given to any contractual, statutory, or regulatory conditions or restrictions governing the funds that are anticipated to serve as the source of repayment for the debt issue and/or as collateral, such as in any relevant grant agreements, the Annual Contributions Contract (ACC), the MTW Agreement, and/or applicable state and federal statutes and regulations. Analysis and consideration of the following topics should be part of any debt structuring effort.

1. Term - The term of the debt shall match the expected useful life of the projects or purpose of the program being financed.

2. Interest Rate – Interest rates may be variable or fixed but may not exceed the maximum rate set forth in the Bond Authorization Act, as now or hereafter amended (30 ILCS 305/0.01 et. seq.).

3. Maturities - The date the principal of a municipal security or a loan becomes due and payable to the bondholder or loan issuer.

4. Level Debt – Relates to the debt service schedule in which the combined annual amount of principal and interest payments remains relatively constant over the life of the issue of bonds.

5. Bond Insurance – A guarantee by a bond insurer of the payment of the principal and interest on municipal bonds as they become due should the issuer or obligated person fail to make required payments.

6. Capitalized Interest – A portion of the proceeds of an issue that is set aside to pay interest on the securities for a specified period of time.

7. Credit Enhancement – credit enhancement shall be used only when a significant savings is produced through its use or when necessary for marketing reasons.

At this time, CHA does not allow the use of derivatives as part of its debt management structure.

XIV. Debt Issuance Practices

A. Method of Sale.

CHA shall issue debt through competitive sale wherever feasible. CHA may elect to sell debt obligations through an invited or negotiated sale provided such sale brings significant benefits to CHA that would not be achieved through a competitive sale. For negotiated sales, CHA should seek to include qualified minority and women-owned firms on the

underwriting team.

B. Professional Service Providers and Fees.

CHA shall utilize the services of bond counsel on all debt financings as well as the services of independent financial advisors when deemed appropriate. CHA will issue a Request for Proposal (RFP) to periodically select service providers as needed, under the direction of the CFO. Such services, depending on the type of financing, may include bond counsel, financial advisory, underwriting, trustee, remarketing agents, arbitrage consulting, Letter of Credit (LOC) providers and special tax consulting. The goal is to achieve an appropriate balance between service and cost regardless of a competitive process or single-source selection.

The fees will vary depending on the complexity of the issuance. In general, all fees incurred in undertaking a bond financing will be payable from bond proceeds and shall be disclosed prior to the transaction closing.

C. Ratings and Rating Agency Communication.

CHA will make all reasonable efforts to maintain the highest possible credit ratings for all categories of short and long-term debt.

CHA will maintain good communications with the rating agencies and timely inform them about CHA's financial position including the Annual Comprehensive Financial Report (ACFR) and the Comprehensive Operating Budget.

D. Structural Features.

The CEO and CFO, with guidance from professional service providers, shall be responsible for determining the appropriate structure for the debt financing considering factors including, but not limited to, the long-term benefit of the financing and current market conditions.

1. Debt Repayment – the maturity of the debt issue should be consistent with the economic or useful life of the capital project to be financed.

2. Variable-rate Debt – CHA may issue bonds in a variable rate mode. Such issuance must be consistent with applicable law and covenants of pre-existing bonds, and in an aggregate amount consistent with CHA's creditworthiness objectives. Such use shall be evaluated on a case-by-case basis to determine whether the potential benefits are sufficient to offset any potential costs.

3. Tax Structure – CHA may choose to issue securities on a taxable or tax-exempt basis. Such use shall be evaluated on a case-by-case basis to determine which structure will be most effective and beneficial.

XV. Debt Administration Activities.

The Treasurer shall be responsible for managing and coordinating all activities related to the issuance and administration of debt, particularly the timely payment of debt, investment of bond proceeds, monitoring compliance for tax-exempt debt. Treasury is also responsible for the

implementation of internal control procedures to ensure that the proceeds of debt are directed to the intended use.

In order to avoid arbitrage earnings on bond proceeds, CHA shall recommend issuance of debt based upon the cash flow needs of the capital plan. CHA shall maintain, or cause to be maintained, an appropriate system of accounting to calculate bond investment arbitrage earnings in accordance with the Tax Reform Act of 1986, as amended or supplemented, and applicable United States Treasury regulations related thereto.

XVI. Internal Controls and Compliance.

This policy shall be presented to the Audit and Finance Committee as part of the annual debt report to ensure its consistency with respect to the CHA debt management objectives. Any modification to this policy shall be presented for approval by the BOC.

On at least an annual basis, the Treasurer will review CHA's debt capacity and affordability analysis and will report to the CFO and ICMC.

XVII. Conclusion.

CHA's Investment & Cash Management Policy constitutes a dynamic and living document and as such will be subject to periodic review and/or amendment to comply with applicable law and to ensure that CHA's financial and operational flexibility is maintained.

In the case of any conflict between applicable law and this policy, applicable law shall prevail.

CHA Investment Policy—APPENDIX
Approved Securities

All Funds	**Listed Under:**	
Security	**HUD Guidelines**	**State of IL Guidelines**
United States Treasury Bills	x	x
United States Treasury Notes and Bonds	x	x
United States Treasury Strips	x	x
Farm Credit Consolidated System (FFCB) Discount Notes, Notes and Bonds	x	x
Federal Home Loan Bank (FHLB) Discount Notes, Notes and Bonds	x	x
Federal National Mortgage Association (FNMA) Discount Notes, Notes and Bonds	x	x
Federal Home Loan Mortgage Corporation (FHLMC) Discount Notes, Notes and Bonds	x	x
Sallie Mae (SLMA) Obligations	x	x
Farmer Mac (FRM) Discount Notes and MTNs	x	x
Financing Corp (FICO) Notes, Strips	x	x
Tennessee Valley Authority (TVA) Notes, Bonds, and Strips	x	x
Private Export Funding Crp (PEFCO)	x	x
Inter-American Development Bank (IADN) Discount Notes	x	x
Overseas Private Investment Crp (OPIC) - Sovereign Agency US	x	x
Government Aid Bonds (AID) - Agency for Int'l Development	x	x
Housing Government Sponsored Enterprises (GSE)	x	x
Security Issued by any other agency created by an Act of Congress	x	x
Money Market Deposit & Super Now Accounts that are 100 % backed by US Gov't Securities	x	x
Interest-Bearing Savings Accounts and Time Deposits or Certificates of Deposits issued by financial institutions which are insured and/or collateralized 100% by Government Securities for the Low-Rent Public Housing and Home Ownership Programs	x	x
Repurchase Agreements pursuant to the Act. The securities, unless registered or inscribed in the name of the Authority, shall be purchased through banks or trust companies authorized to do business in the State of Illinois. The term "repurchase agreements" as used herein shall include flexible repurchase agreements that permit the Authority to withdraw funds as needed and master repurchase agreements that permit the deposit, withdrawal and redeposit of funds over time and do NOT exceed 30 day maturities.	x	x
Mortgage backed Securities and CMOs issued by GNMA, FHLMC & FNMA	x	x
SBA (Asset Based Product is Guaranteed by Lender)	x	x
HUD Project Notes	x	x
Title 11 Merchant Marine	x	x
Housing (HUD) Government Sponsored Enterprises (GSE)	x	x
Non Low Rent Public Housing or Homeownership Programs (subject to established credit criteria)		
Interest-Bearing Savings Accounts and Time Deposits or Certificates of Deposits issued by financial institutions which are insured and/or collateralized 100% by FHLB Public Unit Deposit Insurance for all other programs		x
State/Municipal Obligations		x
Illinois Housing Development Authority Mortgage Participation Certificate		x
Commercial Paper – short term obligations of corporations		x
Credit Unions – state of Illinois only		x
Public Treasurer's Investment Pool – section 17 State Treasurer's Act		x