CHA
CHICAGO HOUSING AUTHORITY

INFORMATION SECURITY POLICY

Responsible CHA Department(s):	**Information Technology Division**	**Policy No. 102.1**
Effective Date: July 18, 2023	Approved on July 18,2023by CHA Board of Commissioners Resolution No. 2023CHA16	
This policy incorporates and supersedes the Information Security Policy (eff. 03/2008) and Communications Equipment Policy (eff. 01/2001).		

I. Purpose

The Information Security Policy ("Policy") provides a foundation for protecting the Chicago Housing Authority's (hereinafter "CHA" or the "Authority") information resources involving the use of technology; to ensure adequate security for information collected, transmitted, processed, stored, or presented via CHA systems; and to maintain appropriate information confidentiality, integrity, and availability.

Consistent standards for network access and authentication are critical to the Authority's network information security and are often required by regulations or third-party agreements. Any user accessing the Authority's computer systems can affect the security of all users of the network. An appropriate network access and authentication process reduces the risk of a security incident by requiring consistent application of authentication and access standards across the CHA networks and systems.

This Policy and implementing procedures issued by the Chief Information Officer (CIO), are based on standards and best practices defined by the U.S. Department of Housing and Urban Development (HUD), 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 legislation and Illinois state law, including the Federal Information Security Management Act, Computer Fraud and Abuse Act, Electronic Communications Privacy Act, Federal Privacy Act, National Information Infrastructure Protection Act, the Illinois Information Security Improvement Act and the Sarbanes-Oxley Act.

This Policy supersedes any of CHA's previous information security policies and shall be applied and construed consistently with existing organization-wide policies, codes of conduct, standards and procedures.

II. General Provisions.

A. Definitions.

1. A "control" is a protective measure put in place to help mitigate or minimize risk.

2. A "risk" is a probability that a threat will exploit a vulnerability in a system or process.
3. An "application" is a software product or series of programs executed to meet a set of business objectives or user requirements.
4. "Information Assets" is information or data that is of value to and owned by CHA, including such information as tenant records, intellectual property, or customer information. These assets can exist in physical form (on paper or storage media) or electronically (stored in databases, in files, on computers). All CHA issued software, user IDs, and phone numbers remain the intellectual property of CHA.
5. "System Owner" is the person or group having responsibility for the development, procurement, integration, modification, operation, and maintenance, and/or final disposition of an information system. The system owner is usually the primary user of the system.
6. "Sensitive information" is information that can cause substantial harm, including financial loss and/reputational risks for CHA if it is not properly protected. Sensitive information includes but is not limited to: Personally Identifiable Information (PII), Protected Health Information (PHI), Financial Information, and Confidential Business Information.
7. "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 website).
8. 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.
9. "Users" means employees, officials, contractors, volunteers (including residents and resident leaders), and guests who access CHA's corporate network and resources, whether on-premises, by remote access or through cloud-based resources, including CHA-owned or CHA-provided computing devices, such as desktop and laptop PCs, tablets, mobile and desk phones, and other equipment needed to access the corporate network and systems. For purposes of this Policy, Users does not include third parties who access CHA's externally reachable public facing systems, such as CHA corporate website and public web applications and social media.

B. Applicability.

1. This Policy addresses technical, management, and operational requirements for security from the information technology perspective and applies to all Users.
2. This Policy sets requirements for information protection but does not include substantial technical or operational details related to security control implementation. Technical and operational details will be documented in Information Technology (IT) procedure documents issued by the CIO, as amended periodically.
3. This Policy applies to physical security for personnel and IT equipment in locations designated as Data Centers.

III. Roles and Responsibilities

All CHA employees and officials and non-CHA employees who access CHA's information system are responsible for protecting the Authority's information assets. Key personnel responsible for specific information security roles and responsibilities are:

A. **Chief Executive Office.** The Chief Executive Officer (CEO) provides the strategic vision for CHA's information security program, approves strategic goals and ensures information security is integrated in CHA's management processes; and ensures compliance with applicable regulations.

B. **Chief Information Officer (CIO).** The CIO establishes and oversees all aspects of the Information Technology (IT) and network security functions. Duties include but are not limited to:

1. provides guidance and vision for effective, agency-wide information technology services;
2. develops and manages the budget for IT operations and activities, including network information security initiatives;
3. reviews, evaluates and approves information security procedures; establishes oversight procedures to ensure IT activities comply with information technology network security policies and other applicable Board-approved policies and practices; and
4. provides oversight for the enforcement of information technology and network security policies, procedures, and control techniques.

C. **Information Technology (IT) Division.** The IT Division oversees IT operations, the network infrastructure, application development, and system maintenance functions. IT Division's responsibilities encompass the establishment, maintenance and observance of procedures and practices consistent with this Policy and other applicable policies authorized and approved by the Board of Commissioners, and include, but not limited to, the following:

1. Define minimum acceptable parameters for the implementation and use of information technology, communications systems, and data.
2. Review formal information system security procedures that address purpose, scope, roles and responsibilities, management commitment, and operational and technical controls to ensure compliance consistent with applicable state laws and guidance.
3. Monitor technology developments and evaluate their impact upon CHA information resources.
4. Oversee the technical implementation of information technology solutions including but not limited to the IT infrastructure and applications.
5. Design and execute short and long-term strategic plans to assure infrastructure capacity attains current and future needs.
6. Develop, execute, and oversee procedures, policies, and related training plans for project management and infrastructure administration.
7. 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.
8. Monitor infrastructure for security incidents and vulnerabilities, develops monitoring and visibility capabilities, and reports incidents, vulnerabilities, and trends to management.
9. Develop, maintain, and help ensure the enforcement of CHA-wide information security policies, procedures, and controls.
10. Oversee, control, and manage the deployment and integration of new or enhanced security solutions.
11. Ensure the integrity and security of all CHA digital assets and services.
12. Auditing CHA information system by ensuring that it is adequately secured.

13. Ensure compliance and make users aware of CHA information security policies and procedures.

D. **Users' Responsibilities.** All Users of CHA information assets are responsible for helping to maintain confidentiality, availability, and integrity of CHA information. Any person who uses any of CHA systems is considered a User. Users must comply with this Policy and related procedures; take all reasonable measures to protect their accounts and passwords used to access CHA systems; and report any known or suspected information security breaches to appropriate personnel in accordance with procedures developed by the CIO.

IV. Policy Compliance

A. CHA executives and managerial staff will ensure Users' compliance with procedures issued by the CIO to implement this policy.

B. **Enforcement.** This Policy will be enforced by the IT Division and users deemed in violation may be referred to Human Resources to determine if further action is necessary. Violations may result in disciplinary action, which may include suspension, restrictions of access, or more severe penalties, up to and including termination of employment or contractual obligations. Where illegal activities or theft of CHA property (physical or intellectual) are suspected, CHA may report such activities to the applicable authorities. Non-employee Users or guests deemed in violation may be restricted in whole or in part from access to CHA systems and information assets.

V. Information Handling Requirements

Maintaining confidentiality and appropriate distribution standards are paramount in handling the CHA information. Refer to CHA's IT Procedures for current CHA standards and guidance.

VI. Security Violations / Incidents

Refer to CHA's IT Procedures for current CHA standards and guidance.

VII. 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.

VIII. System Access Management

All users who obtain access to CHA systems are required to adhere to CHA information security policies and procedures. Managing system access is paramount in helping to ensure that only authorized users have access to CHA systems. Refer to IT Procedures for current CHA standards and guidance.

IX. User Identification and Authentication

CHA will ensure that any user who accesses CHA systems is properly identified and authenticated in accordance with procedures issued by the CIO. Impersonating, alteration, or sharing may be deemed a violation of this policy and is subject to enforcement. To ensure this, refer to IT Procedures for current CHA standards and guidance.

X. Physical Access Controls

CHA will implement physical controls including protective mechanisms that restrict physical entry into areas containing IT equipment in accordance with procedures issued by the CIO.

XI. System Backup and Recovery

CHA will develop system backup and recovery procedures consistent with its Disaster Recovery Plan and Records Retention Policy to help ensure system availability and integrity to be implemented by Users in accordance with procedures issued by the CIO.

XII. Media Controls

Media controls are designed to protect information stored electronically. Media includes the physical means by which data can be stored, hard drives, cloud-based servers/storage, and removable media such as flash drives, sim cards, etc. Protecting information requires effective safeguards related to media handling including storage and disposal. Refer to IT Procedures for current CHA standards and guidance.

XIII. Social Media

CHA respects the rights of Users to use of social media as a medium of communication. Users are responsible for information posted to social media. CHA's Ethics policy, Employee Handbook, and any other policies governing the conduct of CHA Users apply equally to all social media postings. The Users should seek guidance from the supervisor, the Legal Department and/or the Communications Department if they are uncertain about what is appropriate to share on their personal social media.

XIV. Third-Party Managed Cloud Services

A. **Selection and Contracting** All third-party cloud service providers must undergo thorough security assessment and due diligence before contracting. Contracts with providers should include clear terms regarding data ownership, data security, incident response, and breach notification.

B. **Data Protection** All data stored in the cloud must be protected in compliance with applicable laws, regulations, and CHA's internal policies. This includes, but is not limited to, encryption at rest and in transit, appropriate access controls, and regular data backups.

C. **Vendor Management** CHA will monitor the security practices of the cloud service provider. Regular audits and reviews will be conducted to ensure that the provider is adhering to the agreed-upon security standards and practices.

D. **Incident Response** CHA and the cloud service provider will have a clearly defined incident response plan. The response plan will include the steps to be taken in the event of a security breach, data loss, or service outage.

E. **Exit Strategy** An exit strategy will be outlined in the contract that allows for the secure and complete transfer of data back to CHA or to another provider when the contract ends.

XV. CHA-Issued User Hardware and Software Security

Users are accountable for protecting CHA equipment they use during their work activities, including but not limited to, workstations, multifunction devices, copiers, printers, laptops, tablets, and mobile devices. CHA may restrict use and access to software applications and services.

XVI. Information Technology Code of Conduct

A. CHA systems are to be used for official business purposes in serving the interests of CHA. Users have no expectation of privacy rights related to any information sent, received, or stored in any of CHA systems. Use of CHA systems must be in accordance with CHA policies, including Personnel Policies 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, compromised resources, and legal vulnerability. CHA reserves the right to monitor the network, equipment, and email messages without prior notice.

B. **CHA-Issued Equipment.**

1. CHA may issue Users a computing device for the purposes of fulfilling their job duties and official business activities as a duly authorized CHA employee, officer, staff member, or agent (as applicable). All telephonic, text and related messages sent or received on CHA-issued mobile devices, including any file attachments, are

the property of CHA. CHA may, at its discretion, inspect, use or disclose any electronic communications or data without further notice for any legitimate business, legal or disciplinary purpose.

2. Even to the extent of any limited personal use of CHA-issued devices, there is no reasonable expectation of privacy to information that may be transmitted or stored by or on any CHA-issued device or related system(s). Users' acceptance and use of any CHA-issued device will be deemed their acknowledgement and agreement to observe applicable CHA policies and procedures.

C. Limited Personal Usage.

1. Although acceptable use of internet and e-mail is for CHA business, employees are permitted personal use on a reasonable and limited basis for communication or recreation so long as that use does not interfere with the performance of work duties; violate any CHA policy or procedures, including Personnel Policies; involve the running of a business other than CHA; or cause degradation of system services (e.g., network slowdowns). Managers must impose proper constraints on personal use in their respective areas, and may deny personal use of CHA network, internet, email, or equipment in their discretion.
2. Contractors and other non-CHA employees are not authorized to use CHA's network, email, or information resources for personal use unless it is specifically permitted via applicable contracts.
3. Users must not use CHA-issued equipment or CHA network, email, internet or information resources to:
    a. Intentionally access inappropriate sites (e.g., pornographic web sites);
    b. Perform personal downloads (e.g., personal music, video games, etc.);
    c. Download non-IT approved software from Internet sites; or
    d. Conduct personal financial transactions (e.g., e-commerce transactions).

D. Clear Desk. Users must maintain a "clear desk" practice to ensure that sensitive information and equipment are secured and, to the extent possible, out of open view when desks are unattended.

XV. Risks, Liabilities & Disclaimers

A. While IT will take precautions to prevent the personal data of employees, contractors and affiliates from being lost in the event it must wipe a device, it is the employees, contractors & affiliates' responsibility to take and exercise their own additional precautions and care for personal data, such as backing up emails, contacts, calendar etc.

B. CHA reserves the right to disconnect any device or disable any service provided by the CHA without notification.

C. Lost or stolen CHA devices must be reported to the IT immediately.

D. All employees, contractors & affiliates may be personally liable for all costs associated with loss of or damage to their assigned CHA device.

E. Users may be liable for losses to CHA caused by any usage in violation of this Policy.

XVI. Compliance

Failure to abide by this Policy or procedures issued by the CIO may subject Users, including employees, officers, and contractors, to disciplinary action and/or sanctions up to and including dismissal or termination of contract in accordance with CHA's disciplinary and debarment processes.

References:
Policy History: Approved on 1/16/2001 by 2001CHA6 and 3//2008 by 2008CHA20 Revised and approved on 7/18/2023 by 2023CH16