INFORMATION TECHNOLOGY POLICY

This chapter sets forth the Housing Authority of the City of Los Angeles' (the "Authority") Information Technology Policy (the "Policy").

I. Purpose and Applicability

A. Information Technology enables the Authority to increase public awareness of the Authority's programs, facilitates the Authority's mission and program goals, and allows Users to carry out their duties more effectively and efficiently. The purpose of this Policy is to establish guidelines for the appropriate use of the Authority's IT Resources.

B. This Policy applies to all Users of the Authority's IT Resources.

II. Definitions

A. 3rd Party – Any individual, business, or other entity that is not an Authority employee.

B. E-mail – A system for sending multimedia and text-based messages from one individual to another via telecommunications links between computers or terminals using dedicated software. E-mail is also known as Electronic Mail.

C. Hack – Breaking into or attempting to break into a network and/or server without authorized access.

D. Information Technology – Computer networks, hardware, software, and telecommunication devices and services that allows for the creation, sharing, and storage of electronic files, E-mails and data. Examples of Information Technology include, but are not limited to, computers, laptops, mobile devices, smartphones, and E-mail systems.

E. Internet – A series of globally-interconnected digital networks, communicating through a common communications (Internet Protocol) language, by which data and E-mail may be digitally exchanged in near real-time. The Internet is also known as the World Wide Web.

F. Intranet – The Authority's internal website with departmental links for employee use.

G. ITO – The Authority's Information Technology Department. ITO is

also known as Information Technology Operations.

H. IT Resources – Information Technology owned, licensed, leased or otherwise used by the Authority. IT Resources is also known as Information Technology Resources.

I. Malware – Harmful executable programs such as computer viruses, computer worms, trojans or spyware.

J. P.I.I. – Information that can be used (either alone or in combination with other information) to identify, contact or locate a unique person. Examples include, but are not limited to, name, social security number, address, birth date, telephone number, and account numbers. P.I.I. is also known as Personal Identifiable Information.

K. Portable Storage Devices – Digital storage devices that can be moved between computer systems. Examples of Portable Storage Devices include, but are not limited to, thumb drives, mini drives, memory sticks, digital cameras, and digital video recorders.

L. Retention Policy – The Authority's "Record Retention & Disposition Policy" and the corresponding procedures found in Chapter 116 of the Authority's Manual of Policy and Procedure.

M. Sensitive P.I.I. – P.I.I., which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive P.I.I. is also known as Sensitive Personal Identifiable Information.

N. Server – A computer that provides services to other computers (and their users) on a network.

O. Smartphone – A wireless telephone set with special computer enabled features.

P. Streaming – Downloading compressed, bandwidth-intensive real-time audio and/or video from the Internet to a computer.

Q. Superuser – Users of the Authority's IT Resources who possess special privileges needed to administer and maintain the system. Superusers assist in the training and supervision of employees who use the Authority's IT resources. Superusers approve the levels of system access granted to employees in their respective modules. Superusers are tasked with properly documenting, monitoring,

testing and approving system and set-up changes to their respective modules.

R. User – An Authority employee or 3rd Party who has been authorized access to the Authority's IT Resources.

III. No Expectation of Privacy

A. The Authority's IT Resources, whether used entirely or partially on the Authority's premises, should remain accessible to the Authority and, to the maximum extent permitted by law, will remain the sole and exclusive property of the Authority.

B. Users shall not maintain an expectation of privacy with respect to information created with, transmitted over, received by, or stored in any of the Authority's IT Resources. The Authority retains the right to gain access to any information created with, received by, transmitted by, or stored in any of its IT Resources, at any time, either with or without the User's knowledge, consent or approval. Personal use of the Authority's IT Resources may also be subject to examination under the California Public Records Act (*Government Code* § 6250 *et seq*.)

C. Use of the Authority's IT Resources may be monitored or recorded. Anyone using the Authority's IT Resources consents to monitoring and recording. If monitoring or direct observation reveals evidence of possible misconduct or criminal activity, such evidence may be referred to Human Resources, law enforcement or other officials for appropriate action.

D. While the Authority reserves the right to monitor or record any activity on its IT Resources, the Authority is not obliged to monitor or record such activity.

E. The Authority is not responsible for any adverse consequences resulting from the personal use of the Authority's IT Resources. Users waive any claims against the Authority arising from their personal use of the Authority's IT Resources.

IV. Administrative Privileges

A. Superusers have administrative privileges over the Authority's IT Resources. Superusers may include ITO staff, authorized 3rd Party technical consultants working on behalf of ITO, or qualified

individuals with a legitimate-business purpose who are expressly authorized by the Chief Executive Officer, or his or her designee.

V. Procurement of Information Technology

A. Subject to the Authority's budget constraints and available resources, ITO management is responsible for approving the purchasing of Information Technology for the Authority's operations. Direct purchase of Information Technology by an Authority department must be pre-authorized by ITO management on a case-by-case basis. All purchases of Information Technology must comply with the Authority's Procurement Policy, as it may be amended from time to time.

B. All agreements entered into on behalf of the Authority relating to Information Technology, including but not limited to installation, licensing, maintenance, troubleshooting, consulting, data sharing, subscriptions, web-based services, service contracts and end-user agreements, must be vetted and approved by ITO management.

VI. User Access to the Authority's IT Resources

A. Users are provided access to the Authority's IT Resources on an as-needed basis. Requests for access must be approved by a department director on behalf of the requestor and submitted to ITO in accordance with the Information Technology Procedures ("Procedures"), as may be amended from time to time.

VII. User Responsibility

A. It is the responsibility of all Users of the Authority's IT resources to read and follow this Policy.

B. Users are expected to exercise reasonable judgment and comply with all laws when using the Authority's IT Resources.

C. Users are responsible for all activity performed with their individual user-IDs and passwords. User-IDs and passwords may not be utilized by anyone but the individual to whom it has been issued, except as expressly authorized in the Procedures.

D. Users with concern regarding the security of the Authority's IT Resources should communicate them to ITO management for investigation.

E. Any changes to this policy will require employee notification.

VIII. Acceptable Usage of the Authority's IT Resources

A. Authorized Users are encouraged to use the Authority's IT Resources to perform their work duties and further the Authority's goals and objectives. For limitations on permissible use, see Section X, below. Each User is responsible for ensuring that her or his usage is for an appropriate purpose and is conducted professionally and courteously.

B. Due to their job responsibilities, Users may have access to confidential or proprietary information about individuals or organizations. Users who have a legitimate business reason to electronically access or disseminate Sensitive P.I.I. or other confidential or proprietary information must do so using a secure network connection and/or encryption. Users are strictly prohibited from knowingly disseminating Sensitive P.I.I. or any other confidential or proprietary information that they have access to, unless such dissemination is required by their job responsibilities or is otherwise approved in writing by their department director.

C. Identified bargaining unit officers may utilize the Authority's IT Resources for union/association and labor-relations business, including but not limited to, the meet and confer process, member-related grievances, or other disciplinary matters and other work-related membership concerns.

D. Personal use of the Authority's IT Resources is restricted. For information on restrictions imposed, see Section X.

IX. E-mail Rules and Etiquette

A. Users are provided Authority issued E-mail accounts to facilitate Authority related business. This includes communication with fellow employees and 3rd Parties within the context of a User's assigned responsibilities. Additionally, the Authority often delivers official communications via E-mail. As a result, employees with E-mail accounts are expected to check their E-mail in a consistent and timely manner where feasible.

B. E-mails sent from the Authority's E-mail accounts reflect on the Authority. Users are required to be professional and courteous when composing E-mails.

C. Personalization of Authority issued E-mail accounts could create the appearance of the Authority's endorsement of the User's private activities or beliefs. Users are not permitted to personalize their Authority issued E-mail account or corresponding signature block without authorization from their department director.

D. E-mail use shall comply with all Authority policies, including but not limited to the Retention Policy.

E. Authority issued E-mail accounts may not be used for illegal or unlawful purposes, including but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal activity, and computer tampering (e.g., spreading of Malware).

F. Users should refrain from opening E-mail attachments from unknown or unsigned sources. Note that E-mail attachments are the primary source of Malware and should be treated with utmost caution.

G. ITO is responsible for regulating the maximum permissible size of E-mail attachments to ensure smooth operation of the Authority's E-mail systems.

H. Confidential information, including but not limited to Sensitive P.I.I., shall not be transmitted via unsecured systems without proper encryption.

I. Official Authority files and information contained therein, including but not limited to Sensitive P.I.I., shall not be sent to the User's personal E-mail accounts.

J. Except for those individuals who are expressly authorized to do so, Users may not send Authority-wide E-mails.

K. Users receiving unwanted and unsolicited E-mails shall report it to ITO. ITO will address the matter as soon as practicable.

L. 3rd Party users are not authorized to send email on behalf of the Authority (from hacla.org or other Authority-owned domains) without approval from ITO management. This includes but is not limited to marketing, notifications, alerts, or other information.

M. Deletion of E-mail must comply with the Retention Policy and any applicable legal hold directives. In order to manage the Authority's IT

Resources, the Authority may delete E-mails from the Authority's E-mail system without notice to the User within the retention policy limit.

N. "Bulk saving" of E-mail outside of the Outlook/Exchange email system is not permitted.

X. Unauthorized Usage of the Authority's IT Resources

Unauthorized use of the Authority's IT Resources can impact productivity, cause harm or damage to the systems, or create legal liability for the Authority. Therefore, the following restrictions are imposed on the usage of the Authority's IT Resources.

A. Any level of personal use that interferes with an employee's work duties or productivity is not permitted.

B. The Authority's IT Resources may not be used in a manner that interferes with the Authority's operations, except to the extent authorized in order to conduct Authority business. This includes, but is not limited to, streaming, unauthorized destruction or movement of data, or downloading or sending large personal files.

C. Users may not connect, attach, or plug their personal electronic devices or Portable Storage Devices to the Authority's network or WiFi. This includes, but is not limited, to personal Smartphones, thumb-drives, laptops or tablets.

D. The Authority's IT Resources may not be used in a manner that will result in charges or expenses that are not related to the Authority's operations. Examples of non-permissible charges and expenses include, but are not limited to, non-business related long-distance phone calls and printing/copying personal documents using the Authority's printers/copiers.

E. Access to audio and video streaming websites and services are restricted on the Authority's servers. Users are not permitted to stream audio or video using the Authority's IT Resources except for work-related reasons. Restricted websites include, but are not limited to, websites and services like Netflix, Pandora, YouTube and Hulu. Access may be granted as-needed only for Authority-related business.

F. Users may not store or save non-work related music or videos on the Authority's IT Resources.

G. Access to social media websites is restricted on the Authority's servers. Users may not access social media websites using the Authority's IT Resources except for work-related reasons. These include, but are not limited to, Facebook, Twitter, Instagram and Tumblr. Access may be granted as-needed only for Authority related business.

H. The Authority's IT Resources may not be used to engage in online gaming, gambling or advertising (spamming). Access to gaming, gambling or related websites is prohibited.

I. The Authority's IT Resources may not be used to pursue private commercial business activities or profit-making ventures. This includes, but is not limited to, operating a business, pursing non-HACLA employment activities or opportunities, or engaging in any other form of compensable outside employment.

J. The Authority's IT Resources may not be used in a manner that violates the Authority's Conflict of Interest Policy, as it may be amended from time to time. This includes, but is not limited to, using the Authority's IT Resources to engage in direct or indirect lobbying, matters directed toward the success or failure of a political party/candidate, or in activity in support of political fundraising.

K. The Authority's IT Resources may not be used in a manner that violates the Authority's Anti-Harassment Policy or promotes violence. This includes, but is not limited to, creation, downloading, viewing, storage, copying, or transmission of discriminatory, derogatory, bullying, or sexually explicit material. (In certain circumstances, such as during an administrative investigation, this activity may be work-related and authorized.)

L. The Authority's IT Resources may not be used in a manner that improperly or unlawfully infringes on the intellectual property rights of 3rd Parties. This includes, but is not limited to, unauthorized copying, storing and/or sharing of software or data, including but not limited to peer-to-peer file sharing.

M. The Authority's IT Resources may not be used to hack, gain unauthorized access to, interfere with, or alter the Authority's or 3rd Party's networks or systems. Users shall not attempt to enter any server, workstation or computer (with or without) Internet access without prior authorization.

N. The Authority's IT Resources may not be used in such a manner that

may give the false impression that an individual's otherwise personal communication is authorized by the Authority.

O. The Authority's IT Resources may not be used to engage in unauthorized charitable fundraising or solicitation of volunteers for fundraising.

P. The Authority's IT Resources may not be used in such a manner that introduces Malware into the Authority's or 3rd Party's network or systems.

Q. Users may not move, alter or replace the Authority's IT Resources without authorization from ITO management.

R. The Authority's IT Resources may not be used to engage in any activity that would violate any laws or Authority policies, including but not limited to the Personnel Rules.

Employees with questions regarding the appropriateness of their use of the Authority's IT Resources should contact their department director. All administrative, design, and technical questions regarding the Authority's IT Resources shall be directed to a member of ITO management.

XI. Maintenance

A. The Authority's IT Resources are to be maintained and administered by ITO.

XII. Applicable Laws

A. This Policy is intended to be administered in accordance with all applicable laws, including but not limited to the following:

1. Federal Information Security Management Act ("FISMA"), 44 U.S.C. § 3541, *et seq.*;

2. Federal Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 *et seq*.;

3. The Computer Fraud and Abuse Act, ("CFAA") 18 U.S.C. § 1030;

4. The California Public Records Act ("CPRA") California Government Code § 6250 *et seq*.;

5. California Penal Code section 502 (Computer Crimes);

6. Information Practices Act ("IPA"), Cal. Civ. Code §§1798 *et seq*; and

7. HUD Notice PIH-2015-06 (Privacy Protection Guidance).

XIII. Violations of the Policy

A. Violations of this Policy by an employee may result in progressive disciplinary action, up to and including termination, in accordance with the Personnel Rules and any applicable Memorandum of Understanding.

B. Violation of this Policy by a 3rd Party User of the Authority's IT Resources will be evaluated on a case-by-case basis. Such violations may result in loss of access, contract termination, legal prosecution or other appropriate remedial action.

C. The Authority may notify and cooperate with appropriate authorities upon obtaining knowledge that a User has violated state, federal or local laws.

XIV. Procedures

A. The Authority's President & CEO shall provide for the development, administration and implementation of the Procedures to be adopted in furtherance of this Policy.

XV. Amendments to the Policy

A. This Policy may only be amended by the Board of Commissioners.