INFORMATION TECHNOLOGY PROCEDURES

I. In accordance with the Information Technology Policy adopted by the Board of Commissioners on __12/22/2016_____, Resolution __9322___, the following Information Technology Procedures (the "Procedures") set forth the requirements for the issuance and use of the Housing Authority of the City of Los Angeles ("Authority") IT Resources.

II. Definitions

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

B. Cloud-Based Applications – Applications that are used by the Authority but are not hosted on the Authority's premises or equipment. Cloud-Based Applications that are currently used by the Authority include, but may not be limited to, Yardi and Office 365.

C. Cloud-Based Storage – 3rd Party storage providers that allow individuals, companies, and government entities to store data on their servers to be accessed and shared via the Internet. Examples of Cloud-Based Storage include, but are not limited to, DropBox, One Drive, GoogleDrive, and Box.com.

D. Desktop Computer – A computer that is not portable, often consisting of a CPU, monitor, keyboard and mouse.

E. Drive – A storage device on a local access Network where files can be saved.

F. 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.

G. G Drive – An Authority department's shared Drive where data is saved.

H. H Drive – An Authority employee's dedicated Drive where data is saved.

I. Information Technology – Computer Networks, hardware, software, and Telecommunication Devices and Services that allow 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.

J. 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. The Internet is also known as the World Wide Web.

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

L. ITO – The Authority's Information Technology Department. ITO is also known as Information Technology Operations.

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

N. I.T.R.F – The form that must be used when requesting IT Resources from ITO. The I.T.R.F. can be accessed from the 'Information Technology' section of the Authority's Intranet. The I.T.R.F. is also known as the Information Technology Request Form.

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

P. Mobile Devices – Small, portable computing devices, such as laptops, tablets, netbooks, smart phones, cell phones and successive technologies.

Q. M.R.F. – The form that must be used when requesting a move of Desktop Computers, printers, telephones and office furniture. The M.R.F. is also known as the Move Request Form. The M.R.F. can be accessed from the 'Information Technology' section of the Authority's Intranet.

R. Network – A group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

S. Network Management Tools – Applications used by ITO staff to oversee the Authority's computer and network processes.

T. Online Meetings/Web Conferencing – Meetings and conferences that are conducted on computers over the Internet using websites and applications such as GoToMyPC, Webex, TeamViewer, and Lync.

U. 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.

V. 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.

W. Peripheral Device – Any auxiliary device that connects to and works with the computer in some way. Examples of Peripheral Devices include, but are not limited to, printers, speakers and all-in-ones.

X. Retention Policy – The Authority's "Record Retention & Disposition Policy" and the corresponding procedures found in Chapter 116:1 of the Authority's Manual of Policy and Procedure.

Y. RSA – A centrally managed authentication system that uses 'two-factor authentication' (i.e. password-protected log-on and a security access token) to allow secure remote access to the Authority's servers.

Z. POETA/Charge Account – The payment codes assigned by Finance to each Authority department for cost allocations and inventory.

AA. 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.

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

CC. Software Systems/Applications – Computer programs designed to perform a group of coordinated functions, tasks, or activities.

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

EE. Telecommunication Devices & Services – Devices and services that permit communication at a distance. Examples of Telecommunication Devices & Services include, but are not limited to, Mobile Devices, telephones and two-way radios.

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

III. Certification of IT Policies and Procedures

A. All Authority employees who have access to the Authority's IT Resources are required to acknowledge receipt of the Information Technology Policy and Procedures by executing an Employee Certification of IT Policies and Procedures form. The form will be filed and maintained in the employee's Personnel file.

B. Users of the Authority's IT Resources who are not Authority employees are required to acknowledge receipt of the Authority's Information Technology Policy and Procedures using an Authority issued form.

IV. Required Notice

A. Authority Desktop Computers must post the following or similar notice when Users log on:

> "This computer system is the property of the Housing Authority of the City of Los Angeles (HACLA). Do not attempt to log in unless you are an authorized user. Users agree to abide by the terms of the HACLA I.T. Policy. Any access or use may be monitored and violations of the IT Policy or misuse of HACLA's IT Resources may result in criminal or civil prosecution under applicable law. Users have no explicit or implicit expectation of privacy in the use of HACLA's IT Resources. By accessing and/or using this computer system, you agree to and acknowledge these terms of use."

This notice may also be posted on other IT Resources, to the extent appropriate.

V. Access to and Use of the Authority's IT Resources

A. **Network Access** – Access or changes to the Authority's Network must be approved by an Authority director, or his or her designee. Requests for such access or changes to a Network must be submitted to ITO using an approved I.T.R.F.

If the request is the result of an employee transfer, the requesting department shall review all access levels in coordination with ITO management to ensure proper access is requested and unnecessary access is properly removed.

Requests for Network access for 3rd Parties will be reviewed on a case-by-case basis and evaluated by ITO management. In determining whether access will be granted to the 3rd Party, ITO management will consider the type of Network sought to be accessed, sensitivity of the information sought to be accessed including whether the information includes P.I.I. or Sensitive P.I.I., the level of screening that the 3rd Party has undergone, any potential risk to the Authority's operations, and any other factors that may be relevant.

Network access accounts may be disabled if unused for three or more consecutive months. Reactivation of these accounts will not require a formal I.T.R.F.

All Authority employees shall save Authority-related data and files to their department's H Drive or their G Drive. Authority-related data shall not be saved to the C drives of Desktop Computers or laptops. ITO cannot secure or recover data and files saved to a C Drive.

Storage of non-work related personal files on the Authority's Network is restricted. For further information regarding such restrictions, see the Information Technology Policy.

B. **Software Systems/Applications** – Access to the Authority's Software Systems/Applications must be approved by an Authority director, or his or her designee. Requests for access to the Authority's Software Systems/Applications must be submitted to ITO using an approved I.T.R.F.

If the request is the result of an employee transfer, the requesting department shall review all access levels to ensure proper access is requested and unnecessary access is properly removed.

Requests for access to the Authority's Software Systems/Applications for 3rd Parties will be reviewed on a case-by-case basis and evaluated by ITO management. In determining whether access will be granted to the 3rd Party, ITO management will consider the type of Software Systems/Applications sought to be accessed, sensitivity of the information sought to be accessed including whether the information includes P.I.I. or Sensitive P.I.I., the level of screening that the 3rd Party has undergone, any potential risk to the Authority's operations, and any other factors that may be relevant.

User access to Software Systems/Applications may be disabled if unused for three or more consecutive months. Reactivation of these accounts will not require a formal I.T.R.F.

C. **Desktop Computers** – Resources permitting, all Desktop Computers used on the Authority's premises shall be a standard model (i.e. a model previously vetted and approved by ITO), unless a special need can be demonstrated to vary from the standard model. Such variations include, but are not limited to, a computer with greater memory, computing power, or specialized software.

Issuance of a Desktop Computer must be approved by an Authority director, or his or her designee. A request for Desktop Computer must be submitted to ITO using an approved I.T.R.F. as well as a POETA/Charge Account.

Users are strongly encouraged to shut down Desktop Computers at the end of each workday, unless otherwise instructed by ITO.

D. **Mobile Devices** – Issuance of Mobile Devices (and similar successive technologies) must be approved by an Authority director, or his or her designee. A request for a Mobile Device (and similar successive technologies) must be submitted to ITO using an approved I.T.R.F. Issuance of certain Mobile Devices may also require a POETA/Charge Account.

All Authority-issued Mobile Devices shall be pass-code or password protected and encrypted at all times, on or off Authority premises. All Users shall cooperate with ITO to enable their devices to be pass-code or password protected. Users of Authority-owned mobile devices must not disable or bypass security controls implemented by ITO.

Handheld Mobile Devices issued by the Authority must be designed and configured to allow for hands-free listening and talking. Handheld Mobile Devices issued by the Authority may not be used while operating a motor vehicle, unless the hands-free function is utilized.

E. **Peripheral Devices** – Issuance of a Peripheral Device, such as a personal printer or other non-networked device, must be approved by an Authority director, or his or her designee. A request for a Peripheral Device must be submitted to ITO using an approved I.T.R.F. as well as a POETA/Charge Account.

F. **Telecommunications Devices & Services** – Issuance of Telecommunications Devices and Services, such as land lines, some Mobile Devices, long distance service, fax lines, and DSL service, must be approved by an Authority director, or his or her designee. A request for telecommunications equipment and services must be submitted to ITO using an approved I.T.R.F. Under some circumstances, a POETA/Charge Account may be required.

ITO may terminate or disable Telecommunications Devices and Services without notice and without the User's knowledge or consent. Unless otherwise approved in writing by the Chief Operating Officer or his or her designee, Authority issued cell phones shall not be enabled for internet, texting, file download, unless necessary to carry out official duties. Any loss or theft of Authority-owned cell phones must be reported to ITO immediately upon notice of loss.

G. **Cloud-Based Applications** – Access to standard Cloud-Based Applications (i.e. those that have been previously vetted and approved by ITO), such as Voyager and Office 365, must be approved by an Authority director, or his or her designee. Requests for standard Cloud-Based Applications must be submitted to ITO using an approved I.T.R.F. ITO will administer User access to these applications in a manner similar to on-premise applications.

Use of non-standard Cloud-Based Applications must be coordinated with ITO after the business need is established and before any planning or use begins. Access to non-standard Cloud-Based Applications will be evaluated on a case-by-case basis by the ITO management, and will require an approved I.T.R.F. and POETA/Charge Account.

H. **Cloud-Based Storage** – Use of 3rd Party Cloud-Based Storage services must be approved by an Authority director, or his or her designee. Requests for Cloud-Based Storage must be submitted to ITO using an approved I.T.R.F. Access to 3rd Party Cloud-Based Storage services will be evaluated on a case-by-case basis by the ITO management after the business need is established and before any planning or use begins. Such evaluation will include, but may not be limited to, vetting the 3rd Party's security system and end-user agreement. Approval must be obtained by ITO management before any Authority-related data is stored on a 3rd Party's Cloud-Based Storage.

I. **Online Meetings/Web Conferencing** – Use of 3rd Party Online Meetings/Web Conferencing services must be approved by an Authority director, or his or her designee. Requests for standard (i.e. those that have been previously vetted and approved by ITO) Online Meetings/Web Conferencing must be submitted to ITO using an approved I.T.R.F. Access to non-standard Online Meetings/Web Conferencing services will be evaluated on a case-by-case basis by ITO management, and will require an approved I.T.R.F. and POETA/Charge Account.

J. **Portable Storage Devices** – Only Authority-issued Portable Storage Devices will be allowed for use on the Authority's IT Resources. All Authority-issued Portable Memory Devices except digital cameras, digital video recorders, digital media players, and MP3 players shall be encrypted to prevent unauthorized users from accessing data. All Authority-issued Portable Storage Devices must be registered with ITO. Any loss or theft of Authority-owned Portable Storage Devices must be reported to ITO immediately upon notice of loss.

Removing Authority-issued Portable Storage Devices from the Authority's premises without the approval of the User's department director is prohibited.

The loading of P.I.I. or other proprietary or confidential information onto Portable Storage Devices, including but not limited to CDs, floppy discs and external drives, is strictly prohibited.

Use of personally purchased portable storage devices on Authority premises is prohibited.

K. **Remote Access** – Remote Access (from locations not on the Authority's network) to the Authority's network must be approved by an Authority director, or his or her designee. Requests for Remote Access must be submitted to ITO using an approved I.T.R.F. Remote access shall be granted on a case-by-case basis.

Remote access shall require at least a two-step authentication process, using an RSA (remote access) token and a password, and/or other security techniques.

L. **Network Management Tools** – Network Management Tools are to be used by ITO and authorized designees only. Security flaws are not to be tested by anyone other than members of ITO and authorized designees. Security concerns shall be forwarded to ITO management for investigation.

M. **E-Mail Systems** – The Authority's E-mail systems are not designed to be 'file storage systems'. All E-mail more than three-years old shall be purged from Authority E-mail servers on a daily basis except as required by any pending legal hold notices or other Authority authorized preservation requests.

"Bulk saving" of E-mail outside of the Outlook/Exchange email system is not allowed. Any individual E-mails saved must adhere to the Authority's Retention Policy.

Sending or forwarding "Chain E-mails" using the Authority's E-mail system is not allowed.

N. **Internet** – Access to restricted websites on the Internet must be approved by an Authority director, or his or her designee. Requests for access to restricted websites on the Internet must be submitted to ITO using an approved I.T.R.F. Requests must also describe the desired level of access as well as the intent (business case) for the access.

VI. Passwords, User-IDs, and Log-Ins

A. Users are responsible for all activity performed with individual User-IDs and passwords. User-IDs and passwords may not be utilized by anyone but the individual to whom it has been issued. Sharing passwords is prohibited in all Authority internal systems, including but not limited to ORACLE, Elite and Outlook. Passwords for access to external non-Authority systems and Internet websites (including use of login name and passwords) that are being used for Authority-related business may be shared with written approval from the Department director or his or her designee, unless it violates end-user agreements.

The guidelines below shall be followed in the selection and maintenance of passwords:

1. Unique User-IDs and password are required. Passwords must meet the following complexity requirements:

a) Password must be at least 8 characters long.

b) Password shall not contain three or more characters from the User-ID.

c) Password must contain characters from at least three of the following four categories:

i. English uppercase characters (A-Z);

ii. English lowercase characters (a-z);

iii. Base 10 digits (0-9); and

iv. Non-alphanumeric characters (e.g. !, $, #, or %).

2. Systems shall not be set to remember passwords.

3. Password reminders such as notes shall not be placed anywhere they can be easily found, such as under or on phones, keyboards, PCs, monitors, mouse pads, or desktops.

4. Users should refrain from using the same passwords on multiple systems to avoid compromise of other systems when one system is compromised.

5. After three incorrect login attempts, employee's account will be locked out.

6. Password change requests submitted to ITO shall be processed over the telephone. Managerial verifications must be provided for password changes to be made.

7. Password expiration period shall be 90 days.

8. Passwords cannot be reused until 4 cycles have elapsed.

9. Multiple concurrent network logins from different Desktop Computers, virtual desktops, and laptops is not recommended because there is a risk of data and profile corruption. In some cases multiple logins is restricted.

VII. Relocation or Removal of IT Resources

A. Requests to move, alter or replace any of the Authority's IT Resources must be submitted to ITO using a MRF. Moving, altering, or replacing the Authority's IT Resources without authorization from ITO management is prohibited.

VIII. Return of IT Resources By Employees and 3rd Parties

A. Human Resources shall notify ITO management when an individual's employment with the Authority ends. ITO shall disable the departing employee's access to the Authority Network and Servers. Human Resources shall coordinate with the employee's department director to retrieve any IT Resources that have been issued to the departing employee (e.g. Mobile Devices, RSA tokens).

B. The Authority director who approved access for a 3rd Party to use the Authority's IT Resources must notify ITO management when the use is no longer required. ITO shall disable the 3rd Party User's access to the Authority's Network and Servers. Any IT Resources that have been issues to the 3rd Party User must be retrieved by the Authority director who approved issuance of such IT Resources, or his or her designee.