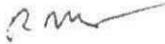
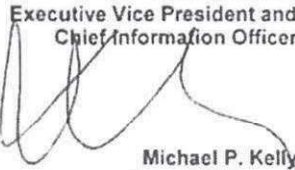


# NYCHA STANDARD PROCEDURE MANUAL

## SP 003:01:5, INTERNET POLICY

### TABLE OF CONTENTS

I. PURPOSE .....	1
II. POLICY.....	1
III. APPLICABILITY .....	1
IV. DEFINITIONS .....	1
V. REVIEW CYCLE.....	3
VI. RESPONSIBILITIES .....	3
A. The Information Technology Infrastructure Department.....	3
B. Enterprise Technology Portfolio Management Department.....	4
C. NYCHA Chief Privacy Officer .....	4
D. Department Directors/Location Supervisors.....	4
E. Users.....	5
VII. PROCEDURE.....	5
A. Internet Access .....	5
B. Internet Access/Removal/Reinstatement Request .....	6
C. Users Guidelines .....	6
D. Unauthorized Use of Computer Programs or Hardware.....	9
E. Security Monitoring.....	9
F. NYCHA Information Systems and Users Privacy .....	9
G. Private and Confidential Information .....	10
H. Data Breach Incidents and Reporting.....	10
I. Users Problems and Questions.....	10
VIII. OUTPUTS, REPORTS, AND RECORDKEEPING .....	11
A. Outputs.....	11
B. Reports.....	11
C. Recordkeeping .....	11
IX. TRAINING REQUIREMENTS .....	12
X. PERFORMANCE METRICS.....	12
XI. NON-COMPLIANCE .....	12
XII. FORMS.....	12
XIII. WORKFLOW .....	14
XIV. REVIEW/REVISION HISTORY PAGE.....	15
XV. APPENDICES.....	17

SUBJECT	PROCEDURE OWNER	APPROVED DATE	APPROVED BY	INDEX NO.
INTERNET POLICY	INFORMATION TECHNOLOGY INFRASTRUCTURE	Issued May 15, 2001 Revised November 20, 2002 Revised May 2, 2012  Date: <u>9/10/15</u>	  Robert Marano Executive Vice President and Chief Information Officer   Michael P. Kelly General Manager	003:01:5

## I. PURPOSE

This Standard Procedure establishes the New York City Housing Authority's (NYCHA) internet policy. It provides specific instructions for the appropriate use, monitoring, and management of the internet. It explains the responsibilities of all NYCHA employees, consultants, and contractors/vendors for safeguarding NYCHA's information systems from unauthorized access and protecting NYCHA's confidential and sensitive information.

## II. POLICY

It is NYCHA's policy to provide internet access to all authorized employees, consultants, and contractors/vendors to assist them in performing their job responsibilities. All Users shall comply with all other applicable NYCHA and internet policies; federal, state, and local laws and regulations; as well as Standard Procedures 002:12:1, *NYCHA Privacy Policy*, and 004:12:1, *Social Media Policy*.

## III. APPLICABILITY

This Standard Procedure applies to all NYCHA employees, consultants, and contractors/vendors authorized to access, use, or manage the internet.

## IV. DEFINITIONS

### A. Access

The specific permissions that NYCHA grants to Users to read, write and erase files within NYCHA's information systems. Users are granted access only to the information necessary for the performance of their official duties, and may have their access revoked or restricted at any time.

### B. Bandwidth

The transmission capacity of an electronic pathway such as a communication line that an electronic device or system (e.g., a computer network) can handle in a given period of time.

## NYCHA STANDARD PROCEDURE MANUAL

### C. Data Breach

An unauthorized dissemination of information. It may be due to an attack on the network or outright theft of paper documents, portable disks, USB drives or laptops. Sensitive information can also be found in trash cans when reports are carelessly discarded.

### D. Information Systems

NYCHA's systems composed of hardware, software, and computer networks for collecting, storing, and processing data.

### E. Internet Protocol Security (IPSEC)

The internet protocol security system that provides authentication and encryption over the internet and secures everything in the network.

### F. Network

A group of computer systems and other computer hardware devices that are linked together to facilitate communications and resource-sharing among a wide range of users.

### G. Personally Identifiable Information

Information that can be used to distinguish or trace an individual's identity. For more information, see the Privacy Portal at <http://connect/PRI>.

### H. Private and Confidential Information

Information created and maintained within NYCHA's information systems that requires a greater level of protection to prevent loss or inappropriate disclosure. For more information on IT security, see the IT Security Portal at <http://connect/IT/Pages/IT-Security.aspx>.

### I. Proprietary Information

Confidential information that is not public knowledge and that is viewed as the property of the holder.

### J. Shareware

A commercial software that is provided to users for a limited trial basis until it is paid for and registered.

### K. User

A person with authorized access to NYCHA's information systems including permanent or temporary employees, contractors, consultants, clients, vendors, agents, volunteers, any

## NYCHA STANDARD PROCEDURE MANUAL

other outsourced third parties, and service or resource providers.

### V. REVIEW CYCLE

The Enterprise Technology Portfolio Management Department shall review this Standard Procedure every two (2) years and revise as needed.

### VI. RESPONSIBILITIES

#### A. The Information Technology Infrastructure Department

1. The Information Technology Infrastructure Department 's staff responsibilities include, but are not limited to, the following activities:
  - a. The chief technology officer shall:
    - (1) Ensure that internet access is provided to all authorized NYCHA employees, consultants, and contractors/vendors as needed.
    - (2) Ensure that NYCHA keeps up with technological changes and best practices.
    - (3) Ensure that the Information Technology Infrastructure Department provides technical and operational control for the internet access process.
    - (4) Ensure that visits by Users to restricted sites are blocked and logged automatically by the system.
  - b. The technical queue administrators shall process all requests to add, remove, or reinstate internet access within five (5) business days upon receipt of the completed and approved NYCHA eForm 130.042, *IT Services Request*.
  - c. The Wide Area Network (WAN) chief shall ensure that the WAN group supports its responsibilities as required by this Standard Procedure.
  - d. The WAN group shall:
    - (1) Monitor the transmission of information throughout NYCHA.
    - (2) Review the monthly reports, listed in section VIII.B.1.a. through d., for internet services received from NYCHA's internet service providers (ISPs).
  - e. The Local Area Network (LAN) manager shall:
    - (1) Ensure proper and secure internet access for Users.

## NYCHA STANDARD PROCEDURE MANUAL

- (2) Ensure that the LAN group generates and provides department directors/ location supervisors with the internet usage activity report upon receipt of a written request.

### B. Enterprise Technology Portfolio Management Department

1. The Enterprise Technology Portfolio Management Department's staff responsibilities include, but are not limited, to the following activities:
  - a. The vice-president for the Enterprise Technology Portfolio Management (ETPM) Department shall ensure compliance with this Standard Procedure.
  - b. The chief IT auditor shall:
    - (1) Evaluate and investigate, immediately, in collaboration with the chief privacy officer, all reported privacy or data breach security incidents upon notification.
    - (2) Provide authorization to Users as needed.
  - c. The Enterprise Technology Portfolio Management Department security group shall:
    - (1) Administer NYCHA's internet policy.
    - (2) Review and monitor all information that is distributed through the internet and via email.
    - (3) Distribute Information Technology security awareness newsletters to all employees, as required, to reinforce and support the practices within this procedure to remind them of NYCHA's appropriate and inappropriate internet use.

### C. NYCHA Chief Privacy Officer

The chief privacy officer shall notify the chief IT auditor immediately of all reported, suspected, or confirmed privacy breaches or violations.

### D. Department Directors/Location Supervisors

1. Department directors or location supervisors shall:
  - a. Monitor compliance with this procedure within their location.
  - b. Submit requests for adding, removing, or reinstating internet access for employees from their location.

## NYCHA STANDARD PROCEDURE MANUAL

- c. Submit written requests to the LAN manager for the internet User activity report, as needed.

### E. Users

#### 1. The Users shall:

- a. Take responsibility for activities they initiate using the internet through any NYCHA network.
- b. Notify their supervisors immediately of the arrival time of any inappropriate images/materials.
- c. Notify their supervisors of any suspected or confirmed data or security breach.
- d. Comply also with the following two NYCHA procedures:

(1) Standard Procedure 002:12:1, *NYCHA Privacy Policy*, listed at <http://connect/sites/FRL/Library/SP002121.pdf>

(2) Standard Procedure 004:12:1, *Social Media Policy*, listed at <http://connect/sites/FRL/Library/SP004121.pdf>.

## VII. PROCEDURE

Users may utilize NYCHA's information systems to access the internet to support the timely communication and sharing of information related to NYCHA services and functions, once the Information Technology Department provides them with access.

### A. Internet Access

1. All Users receive internet access upon creation of their LAN identifications. Location directors/supervisors may specially request that the Information Technology Department deny internet access to Users who do not require the use of the internet to perform their job duties when submitting NYCHA eForm 130.042, *IT Services Request*, to the technical queue administrators for LAN access.

<b>NOTE:</b>	Department directors/location supervisors may revoke or restrict the internet access privilege of a User, at any time, with a written justification.
--------------	--

#### 2. Processing LAN Access Request

The Information Technology Department's technical queue administrators process all requests received from department directors/ location supervisors on NYCHA eForm

## NYCHA STANDARD PROCEDURE MANUAL

130.042, *IT Services Request*, for LAN access. Upon receipt of the request, the Information Technology Department's technical queue administrators create the required LAN identification for the applicable employee, consultant, contractor/vendor and also provide them with internet access, unless otherwise mandated by the requesting department director/ location supervisor.

### B. Internet Access/Removal/Reinstatement Request

1. Department directors/location supervisors shall submit NYCHA eForm 130.042, *IT Services Request*, to the Information Technology Department's technical queue administrators to either add, remove, or reinstate internet access.
2. IT Processing Request

Upon receipt of the request, the Information Technology Department's technical queue administrators perform one of the following actions:

- a. Add internet access for authorized employees, consultants, contractors/vendors who were originally denied internet access when the LAN identification was created for them.
  - b. Remove internet access from authorized employees, consultants, contractors/vendors who knowingly violate this Standard Procedure.
  - c. Reinstate internet access for employees, consultants, contractors/vendors whose previous internet access has been revoked.
3. Accessing Internet Via ISPs

Only NYCHA's authorized ISPs can be used to access the internet through a NYCHA LAN or WAN. Accessing the internet through NYCHA LAN or WAN via any other internet service provider or backdoor accounts is prohibited.

### C. Users Guidelines

1. Appropriate Use of the Internet

Users shall use NYCHA's information systems to access the internet for authorized purposes only.

Appropriate use of the internet includes, but is not limited to, the following activities:

- a. Using the internet for work-related information research.
- b. Accessing and distributing information that is in direct support and relation to NYCHA's business.

## NYCHA STANDARD PROCEDURE MANUAL

- c. Distributing information about topics that are relevant to NYCHA.
- d. Providing authorized information to city, state, and federal agencies.
- e. Informing other employees of new laws, rules, or regulations that may impact NYCHA.
- f. Sharing resources with other city agencies when working on collaborative projects.

<b>NOTE:</b>	Limited personal use of NYCHA's information systems, including NYCHA's email and internet services, is appropriate and expected; however, such use should be kept to a minimum to ensure that it does not interfere with work assignments, and/or job performance, or cause any degradation of network services. For more information, see Standard Procedure 003:15:1, <i>User Responsibilities Policy</i> .
--------------	---

### 2. Inappropriate Use of the Internet

Users shall refrain from using the internet for activities that are unauthorized by this Standard Procedure and all other applicable NYCHA policies.

Inappropriate use of the internet includes, but is not limited to, the following activities:

- a. Using the internet in ways that may negatively affect network performance (e.g., watching videos).
- b. Using the internet knowingly to violate any applicable laws and regulations.
- c. Attempting to circumvent NYCHA's security features which protect NYCHA's network from internet threats and other unauthorized access.
- d. Sharing your log-in user identification (ID) or password with someone else to allow an unauthorized user to access the internet.
- e. Modifying security settings, including Operating System (OS) or Antivirus settings, to allow unauthorized web access or applications.

<b>NOTE:</b>	Users who require access to a specific website or application that is blocked shall contact their immediate supervisors who shall notify the Information Technology Department for authorized access, as appropriate.
--------------	---

- f. Installing any hardware or software on the computer without supervisory permission and prior authorization from the Information Technology Infrastructure Department.



## NYCHA STANDARD PROCEDURE MANUAL

- g. Transmitting proprietary or confidential NYCHA information or information received from third parties on a private/confidential basis, to any unauthorized person.
- h. Using an unauthorized computer program or hardware that may intercept and log traffic passing over NYCHA's network without prior authorization.
- i. Installing any software that may degrade the performance of the entire network.
- j. Distributing copyrighted software programs or documents without proper authorization.
- k. Creating, sending, or disseminating discriminatory, harassing, or threatening messages or images to any employee, resident, contractor, any other person, or entity.
- l. Creating or forwarding chain mail.
- m. Interfering or disrupting network services or equipment by distributing unsolicited advertisements.
- n. Spreading computer worms and viruses through unauthorized entry to any database accessible via the internet or NYCHA's information systems.
- o. Using the internet to conduct private or commercial work for personal gain.
- p. Displaying inappropriate images, documents, or related web sites.
- q. Archiving, storing, distributing, editing, or recording inappropriate materials using NYCHA's network or computing resources.
- r. Visiting gambling sites.
- s. Hyperlinking or pointing NYCHA's websites deliberately to other internet sites containing information or materials that may be inconsistent with or in violation of NYCHA's Privacy Policy.
- t. Downloading any unauthorized shareware programs or files for use without prior authorization from a supervisor.

<b>NOTE:</b>	Unauthorized shareware (freeware) games, movies, music, file sharing programs, and file conversion programs are known as malware attack vectors that may allow Users to gain access to a computer with a malicious code that can infect the computer.  Malware attack vectors may result in systems failure, wasting computer resources, corrupting data, and increasing maintenance costs.
--------------	---

## NYCHA STANDARD PROCEDURE MANUAL

- u. Using too much bandwidth within NYCHA and when connecting to the internet which is a shared finite resource.

Any other use that may interfere with any NYCHA internet user's job responsibilities.

<b>NOTE:</b>	Users who observe others violating this Standard Procedure shall contact IT security at <a href="mailto:itsecurity@nycha.nyc.gov">itsecurity@nycha.nyc.gov</a> .
--------------	--

### D. Unauthorized Use of Computer Programs or Hardware

The use of any unauthorized computer programs or hardware that may adversely affect NYCHA's network is not allowed. Information Technology Department Users who need access to a particular computer program or software for troubleshooting purposes shall obtain prior approval/authorization from the chief technology officer

### E. Security Monitoring

NYCHA has implemented several monitoring systems to prevent unauthorized access to NYCHA's information systems and to detect inappropriate activities.

### F. NYCHA Information Systems and Users Privacy

All the data and information processed, stored, and presented on any NYCHA information system are considered vital property of NYCHA and are maintained in a secure environment. Therefore, Users shall understand that the use of NYCHA's information systems is not private and or/anonymous.

#### 1. Right of Privacy

Users do not have any right of privacy when using NYCHA's information systems, whether for NYCHA's business or personal purposes, at any time.

<b>NOTE:</b>	If Users want their personal activities to remain private, privileged, or confidential, they shall refrain from using NYCHA's information systems for such activities.
--------------	--

#### 2. Files and Information Disclosure

By using NYCHA's information systems, Users consent to the following:

- a. The contents of any file or information that is maintained on any NYCHA information system may be disclosed at any time.
- b. Time spent visiting any sites on the internet is monitored and recorded.

## NYCHA STANDARD PROCEDURE MANUAL

- c. Any information that is distributed through the internet and via e-mail may be monitored and subject to review by the Information Technology Department's Enterprise Technology Portfolio Management security group.

### G. Private and Confidential Information

Information that is created and maintained within NYCHA's information systems including Personally Identifiable Information (PII) is considered private, confidential, and protected. It is essential that all Users comply with all current NYCHA policies regarding the handling, safeguarding, and disclosure of PII.

Confidential information about NYCHA residents, employees, or contractors, including their PII such as social security number, driver's license number, or date of birth may not be transmitted outside of NYCHA (via e-mail, file transfer, or any other method) without an authorized business purpose. Certain authorized transfers are allowed only with the use of proper encrypted channels. Privacy violations, issues, and questions may be reported immediately to the Office of Privacy via e-mail at [Privacy@nycha.nyc.gov](mailto:Privacy@nycha.nyc.gov) or call the Privacy Hotline at (212) 306-3737. Refer to the Privacy and Information Technology Security Portal on the intranet for more information @ <http://connect/PII>.

### H. Data Breach Incidents and Reporting

A data breach incident may be intentional or unintentional. Data breach incidents may include an attack on the network, the careless disposal of used computer equipment, theft of paper documents, portable disks, USB drives, or laptops. Users shall use due diligence when discarding of reports containing sensitive information to avoid the unauthorized disclosure of sensitive, protected, or confidential data.

Refer to the following additional documents for more information regarding NYCHA's policy on handling and safeguarding private/confidential information and protecting NYCHA's information systems.

1. Standard Procedure 003:04:1, *Baseline Information Security Policy*.
2. Standard Procedure 003:04:2, *Virtual Private Network Policy*.
3. Standard Procedure 003:05:1, *Access Control Policy*.
4. Standard Procedure 003:11:1, *Portable Data Device Issuance, Acceptable Use and Security*.
5. Standard Procedure 003:78:1, *Public Access to NYCHA Records*.
6. NYCHA Human Resources Manual.

### I. Users Problems and Questions

## NYCHA STANDARD PROCEDURE MANUAL

If Users have any questions about this procedure, issues, including internet-related problems/questions, they can contact the NYCHA Service Center by email at [svctr@nycha.nyc.gov](mailto:svctr@nycha.nyc.gov) or by telephone at (212) 306-7000. Users can also contact the NYCHA Service Center and/or IT security at [itsecurity@nycha.nyc.gov](mailto:itsecurity@nycha.nyc.gov) to report security violations.

### VIII. OUTPUTS, REPORTS, AND RECORDKEEPING

#### A. Outputs

1. Internet access is provided, removed, or reinstated as requested by department directors or location supervisors.
2. Users are utilizing the internet in an appropriate and safe manner.

#### B. Reports

1. NYCHA's ISPs provide the Information Technology Department WAN's chief with the following four monthly reports:
  - a. Technical performance report.
  - b. Time Warner average and peak traffic rates report.
  - c. Verizon weekly utilization report.
  - d. Verizon FiOS average and peak traffic rates report.

<b>NOTE:</b>	These reports may not be distributed due to the confidential and restricted information that they contain.
--------------	--

#### 2. Internet Usage Activity Report

The Information Technology Department's LAN group shall generate and submit the internet usage activity report to department directors/location supervisors upon request.

#### C. Recordkeeping

##### 1. The Process and Information Management Department

The director of the Process and Information Management Department (PIMD) shall maintain the internet transactions log for one (1) year for audit purposes within the Information Technology Department's backup archives. This log contains all internet – related activities/transactions.

## NYCHA STANDARD PROCEDURE MANUAL

2. The chief of the Information Technology Department LAN shall:
  - a. Maintain records of the internet technical performance reports issued by NYCHA's ISPs.
  - b. Archive internet performance metrics on average uptime, average utilization, and peak usage time for a thirty (30) day period.
3. The Information Technology Wide Area Network

The chief of the WAN shall retain information about performance metrics of the 90 Church Street overall circuit usage including NYCHA's field offices uptime, average utilization, and peak usage time within a shared directory in the WAN folder.

### IX. TRAINING REQUIREMENTS

Training is not required to implement this procedure.

### X. PERFORMANCE METRICS

- A. Average uptime versus average utilization and peak usage time.
- B. Performance metrics of the 90 Church Street overall circuit usage which tallies the traffic sustained by the IPSEC tunnels that connect the NYCHA field offices uptime, average utilization, and peak usage time.

### XI. NON-COMPLIANCE

- A. Failure to comply with the requirements of this Standard Procedure may result in the following:
  1. Restrictions in the use of NYCHA's information systems.
  2. Loss of internet access privilege.
  3. Disciplinary action that may result in suspensions and/or terminations.

Due to the sensitivity of the data contained on various NYCHA computing platforms, NYCHA evaluates each incident on a case-by-case basis.

### XII. FORMS

The following form is referenced in the procedure:

## NYCHA STANDARD PROCEDURE MANUAL

A. NYCHA eForm 130.042, *IT Services Request*.