

Chapter 84	Information Security Rules for Street Hail Livery Technology System Providers
-------------------	--

Table of Contents

§84-01 Scope of the Chapter..... 2

§84-02 Definitions Specific to this Chapter 2

§83-03 Information Security Requirements..... 3

§84-01 Scope of the Chapter

- (a) To establish the Commission's information security requirements for the collection, transmission, processing, maintenance, and storage of LPEP Data by Street Hail Livery Technology System Providers, their employees, agents and subcontractors.
- (b) The information security requirements set forth in this Chapter apply to LPEPs, all Information System Components, LPEP Data, and all related services provided by Street Hail Livery Technology System Providers, their employees, agents and subcontractors to carry out the activities licensed under Chapter 83 of these Rules.

§84-02 Definitions Specific to this Chapter

- (a) *Application.* A computer program designed for a specific use or task and includes all software applications whether custom or off-the-shelf, including internal and external (web) applications.
- (b) *Database.* An organized collection of data, typically in digital form.
- (c) *Database Management System.* A software package with computer programs that control the creation, maintenance and use of a database.
- (d) *DOITT Standards.* The Department of Information Technology and Telecommunications Citywide Information Security Policy for Service Providers and Encryption Standards.
- (e) *Information System* shall have the same meaning given such term in §83-03 of these Rules.
- (f) *Information System Component* includes any Network Component, Server, or Application included in, or connected to, the LPEP and/or LPEP Data environment.
- (g) *LPEP Data.* All data required to be collected, transmitted and maintained pursuant to §83-31 of these Rules and other information assets related to the LPEP Data. LPEP Data includes, but is not limited to, Trip Data, data related to credit, debit and prepaid card transactions, and text messages and the date and time such messages were sent and received.
- (h) *Network Component* includes all firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- (i) *Non-consumer User.* Any individual, excluding a cardholder, who accesses Database Management System components, including, but not limited to employees, administrators and third parties.
- (j) *Personal Information* shall have the same meaning given such term in §83-03 of these rules.

- (k) *Security Incident or Incident* shall have the same meaning given such term in §83-03 of these Rules.
- (l) *Security Policy*. The information security policy and procedures established by an LPEP Provider that comply with the requirements in §84-03 of these Rules.
- (m) *Server*. A physical computer hardware system dedicated to running one or more services at the requests of other programs and includes web, database, authentication, Domain Name System, mail proxy, and Network Time Protocol.
- (n) *Street Hail Livery Technology System or LPEP* shall have the same meaning given such term in §51-03 of these Rules.
- (o) *Street Hail Livery Technology System Provider or LPEP Provider* shall have the same meaning given such term in §51-03 of these Rules.
- (p) *Trip Data* shall have the same meaning given such term in §51-03 of these Rules.

§84-03 Information Security Requirements

- (a) *Information Security Policy*.
 - (1) *Establish Information Security Policy (Security Policy)*. The LPEP Provider must establish prior to system design, maintain, and disseminate to its employees and relevant third parties such as agents and subcontractors, the information security policy and procedures that:
 - (i) Comply with all of the requirements in this section;
 - (ii) Are reviewed and updated at least annually; any change in information security policy and procedures should be analyzed for breaches before implementation (notification of the review and update of the Security Policy must be provided to the Commission);
 - (iii) Include daily operational security procedures that are consistent with the requirements in this section (e.g., user account maintenance procedures, log review procedures).
 - (2) *Usage Policies*. The Security Policy must include usage policies for critical employee-facing technologies, such as modems and wireless devices, to define proper use of these technologies for all employees, agents and subcontractors of LPEP Providers. Usage policies must include:
 - (i) Explicit management approval;
 - (ii) Authentication for use of the technology;
 - (iii) A list of all such devices and personnel with access;

- (iv) Labeling of devices with LPEP Provider contact information;
 - (v) Acceptable uses of the technology;
 - (vi) Acceptable network locations for these technologies;
 - (vii) A list of products approved by the LPEP Provider.
 - (viii) Automatic disconnect of modem sessions after a specific period of inactivity;
 - (ix) Activation of modems only when needed, with immediate activation after use; and
 - (x) When accessing LPEP Data remotely via modem, disable storage of LPEP Data onto local hard drives, floppy disks or other external media, and disable cut-and-paste and print functions during remote access.
- (3) *Responsibilities of LPEP Providers and Employees.* The Security Policy must clearly define the information security responsibilities of the LPEP Provider and its employees.
- (4) *Management Responsibilities.* The LPEP Provider must assign to an individual or team the following information security management responsibilities:
 - (i) Establish, document, and distribute the Security Policy;
 - (ii) Monitor and analyze security alerts and information, and distribute to appropriate personnel;
 - (iii) Establish, document, and distribute Security Incident response and escalation procedures to ensure timely and effective handling of all situations;
 - (iv) Administer user accounts, including additions, deletions, and modifications; and
 - (v) Monitor and control all access to data.
- (5) *Security Awareness for Employees.* The LPEP Provider must make all employees aware of the importance of information security by:
 - (i) Educating employees (e.g., through posters, letters, memos, meetings, and promotions); and
 - (ii) Requiring employees to acknowledge in writing they have read and understood the Security Policy.

- (6) *Screen Employees.* The LPEP Provider must screen potential employees to minimize the risk of attacks from internal sources.
- (7) *Requirements for Third Party Access.* The LPEP Provider must require all third parties, such as agents and subcontractors, with access to the LPEP, Information System Components, or LPEP Data, or who are involved in any related services provided by the LPEP Provider in carrying out the activities licensed under Chapter 83 of these Rules, to agree in writing to comply with the Security Policy and all security requirements in this section.
- (8) *Incident Response Plan.* The LPEP Provider must implement a Security Incident response plan that, at a minimum, requires the LPEP Provider to respond immediately to a system breach. The plan must:

 - (i) Contain specific Incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies;
 - (ii) Be tested at least annually;
 - (iii) Designate specific personnel to be available on a 24/7 basis to respond to alerts;
 - (iv) Provide appropriate training to staff with Security Incident response responsibilities;
 - (v) Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems; and
 - (vi) Contain a process to modify and evolve the Incident response plan according to lessons learned and to incorporate industry developments.
- (b) *Authentication.* The LPEP Provider must provide a process that verifies a user's identity to ensure that the person requesting access to a system is the person to whom entry is authorized.
- (c) *Change Control.* The LPEP Provider must follow change control procedures for all system and software configuration changes. The procedures must include:

 - (1) Documentation of impact;
 - (2) Management sign-off by appropriate parties;
 - (3) Testing that verifies operational functionality; and
 - (4) Back-out procedures.

- (d) *Copyright Compliance.* The LPEP Provider must comply with the terms of all software licenses and may not use any software in any form that has not been legally purchased or otherwise legitimately obtained.
- (e) *Database Management Systems.* The LPEP Provider must develop and implement appropriate controls and procedures to ensure that the Database Management Systems are adequately protected.
- (f) *Access to LPEP Data and Computing Resources.*
 - (1) *Limit Access.* The LPEP Provider must limit access to LPEP Data and related computing resources to only those individuals whose job requires such access.
 - (2) *Restrict Access.* The LPEP Provider must establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.
 - (3) *Unique ID.* The LPEP Provider is required to assign a unique ID to each person with access to LPEP Data and related computing resources to ensure that action taken on critical data and systems are performed by, and can be traced to, known and authorized users. The LPEP Provider must:
 - (i) Identify all users with a unique username before allowing them access;
 - (ii) To ensure proper user authentication and password management for Non-consumer Users and administrators on all system components, the LPEP Provider must:
 - (A) Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects;
 - (B) Immediately revoke accesses of terminated users;
 - (C) Remove inactive user accounts at least every ninety (90) days;
 - (D) Enable accounts used by vendors for remote maintenance only during the time needed;
 - (E) Distribute password procedures and policies to all users who have access to LPEP Data and related computing resources;
 - (F) Prohibit the use of group, shared, or generic accounts; and
 - (G) Authenticate all access to any database containing LPEP Data, including access by applications, administrators, and all other users.

- (4) *Restrict Physical Access.* The LPEP Provider must restrict physical access to LPEP Data and related computing resources as follows:
- (i) Any physical access to data or systems that house LPEP Data, allows the opportunity to access devices or data, and/or removes systems or hardcopies, must be appropriately restricted.
 - (ii) The LPEP Provider must use appropriate facility entry controls to limit and monitor physical access to systems that collect, transmit, process, maintain or store LPEP Data.
 - (A) The LPEP Provider must use cameras to monitor sensitive areas and audit this data and correlate with other entries, storing for at least three (3) months, unless otherwise restricted by law.
 - (B) The LPEP Provider must restrict physical access to publicly accessible network jacks.
 - (C) The LPEP Provider must restrict physical access to wireless access points, gateways, and handheld devices.
 - (iii) The LPEP Provider must develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where LPEP Data is accessible.
 - (iv) The LPEP Provider must ensure that employees and visitors are authorized before entering areas where LPEP Data is collected, transmitted, processed, maintained or stored.
 - (v) The LPEP Provider must ensure that visitors are given a physical token (e.g., badge or access device) that expires, and that identifies them as non-employees.
 - (vi) The LPEP Provider must ensure that visitors are asked to surrender the physical token before leaving the facility or at the date of expiration.
 - (vii) The LPEP Provider must use a visitor log to retain a physical audit trail of visitor activity, and retain this log for a minimum of three (3) months, unless otherwise restricted by law.
 - (viii) The LPEP Provider must store media back-ups in a secure off-site facility, which may be either an alternate third-party or a commercial storage facility.
 - (ix) The LPEP Provider must physically secure all paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain LPEP Data.

- (x) The LPEP Provider must maintain strict control over the internal or external distribution of any kind of media that contains LPEP Data, including:
 - (A) Labeling the media so it can be identified as confidential; and
 - (B) Sending the media via secured courier or a delivery mechanism that can be accurately tracked.
- (xi) The LPEP Provider must ensure management approves all media that is moved from a secured area (especially when media is distributed to individuals).
- (xii) The LPEP Provider must maintain strict control over the storage and accessibility of media that contains LPEP Data including properly inventorying all media and making sure it is securely stored.
- (xiii) The LPEP Provider must destroy media containing LPEP Data when it is no longer needed for business or legal reasons including:
 - (A) Cross-cut shredding, incinerating, or pulping hardcopy materials; and
 - (B) Purging, degaussing, shredding, or otherwise destroying electronic media so that LPEP Data cannot be reconstructed.

(g) *Firewalls.*

- (1) *Firewall Configuration.* A firewall must control access between internal networks and external networks. All firewalls used in the LPEP Provider's systems must be configured by the LPEP Provider to:
 - (i) Block all data traffic (subject to the protocol limitations of the firewall) except that traffic which is explicitly allowed; direct incoming traffic to trusted internal systems; and protect vulnerable systems;
 - (ii) Prevent disclosure of information such as system names, network topology, and network device types; and
 - (iii) Support network layer authentication, with both the firewall and the network layer authentication to be used in conjunction with standard application authentication methods.
- (2) *External Firewall Connections and Changes.* The LPEP Provider must establish a formal process for approving and testing all external network connections and changes to the firewall configuration.

- (3) *Network Diagram.* The LPEP Provider must provide a current network diagram with all connections to LPEP Data, including any wireless networks.
- (4) *Management Descriptions.* The LPEP Provider must provide a description of groups, roles, and responsibilities for logical management of Network Components.
- (5) *List of Services/Ports.* The LPEP Provider must provide a documented list of services/ports necessary for business.
- (6) *Justification for Protocols.* The LPEP Provider must provide justification and documentation for any risk protocols allowed (e.g., File Transfer Protocol, etc.), which includes reason for use of protocol and security features implemented.
- (7) *Periodic Review.* The LPEP Provider must conduct a periodic review of firewall/router rule sets.
- (8) *Exceptions to Denial of Untrusted Networks/Hosts.* The LPEP Provider must build a firewall configuration that denies all traffic from “untrusted” networks/hosts, except for:
 - (i) Web protocols - HTTP (port 80) and Secure Sockets Layer (SSL) (port 443);
 - (ii) System administration protocols (e.g., Secure Shell (SSH) or Virtual Private Network; and
 - (iii) Other protocols required by the business (e.g., for ISO 8583).
- (9) *Restricting Connections between Publicly Accessible Servers and LPEP Data.* The LPEP Provider must build a firewall configuration that restricts connections between publicly accessible servers and any system component storing LPEP Data, including any connections from wireless networks. This firewall configuration must include:
 - (i) Restricting inbound and outbound Internet traffic to ports 80 and 443;
 - (ii) Securing and synchronizing router configuration files (e.g., running configuration files which are used for normal running of the routers, and start-up configuration files which are used when machines are re-booted, must have the same, secure configuration);
 - (iii) Denying all other inbound and outbound traffic not specifically allowed;
 - (iv) Installation of personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), which are used to access the organization’s network;

- (v) Prohibiting direct public access between external networks and any system component that stores LPEP Data (e.g., databases);
 - (vi) Filtering and screening all traffic to prohibit direct routes for inbound and outbound Internet traffic;
 - (vii) Restricting outbound traffic from sensitive applications to authorized IP addresses; and
 - (viii) Implementing IP masquerading to prevent internal addresses from being translated and revealed on the Internet. The LPEP provider must use technologies that implement RFC 1918 address space, such as Port Address Translation or Network Address Translation.
- (h) *Host and Server Systems.* The LPEP Provider must configure host and server systems with sufficient security features to ensure that LPEP Data are adequately protected from unauthorized use, disclosure, modification, destruction, and denial of service.
- (i) *Local Area Networks.* The LPEP Provider must configure local area networks (“LANs”) with sufficient security features to ensure that LPEP Data are adequately protected from unauthorized use, disclosure, modification, destruction, and denial of service.
- (j) *Network Management.*
- (1) *Appropriate Access.* The LPEP Provider must implement controls over all such devices and platforms so that only appropriate resources and persons may access the network. The LPEP Provider must also implement appropriate architectures, procedures, management assignments, and back-up and recovery plans to provide such controls.
 - (2) *Monitor All Access.* The LPEP Provider must track and monitor all access to network resources and LPEP Data.
 - (3) *Linking Access to System Components.* The LPEP Provider must establish a process for linking all access to system components (especially those done with administrative privileges such as root) to an individual user.
 - (4) *Automated Audit Trails.* The LPEP Provider must implement automated audit trails to reconstruct the following events for all system components:
 - (i) All individual user access to LPEP Data;
 - (ii) All actions taken by any individual with root or administrative privileges;
 - (iii) Access to all audit trails;
 - (iv) Invalid logical access attempts;

- (v) Use of identification and authentication mechanisms;
 - (vi) Initialization of the audit logs; and
 - (vii) Creation and deletion of system-level objects.
- (5) *Record Audit Trails.* The LPEP Provider must record at least the following audit trail entries for each event, for all system components:
- (i) User identification;
 - (ii) Type of event;
 - (iii) Date and time;
 - (iv) Success or failure indication;
 - (v) Origination of event; and
 - (vi) Identity or name of affected data, system component, or resource.
- (6) *Synchronize Times.* The LPEP Provider must synchronize all critical system clocks and times.
- (7) *Secure Audit Trails.* The LPEP Provider must secure audit trails so they cannot be altered, including the following:
- (i) Limit viewing of audit trails to those with a job-related need;
 - (ii) Protect audit trail files from unauthorized modifications;
 - (iii) Promptly back-up audit trail files to a centralized log server or media that is difficult to alter;
 - (iv) Copy logs for wireless networks onto a log server on the internal LAN; and
 - (v) Use file integrity monitoring/change detection software (such as Tripwire) on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added must not cause an alert).
- (8) *Review Logs.* The LPEP Provider must review logs for all system components at least daily. Log reviews must include those servers that perform security functions (like intrusion detection systems) and authentication, authorization and accounting servers (e.g., Diameter).
- (9) *Retain Audit Trail History.* The LPEP Provider must retain audit trail history for a period that is consistent with its effective use, as well as all applicable law, rules and regulations.

(k) *Wireless Networks.* At a minimum, dynamic Wi-Fi Protected Access must be used by the LPEP Provider for any portion of the network or system that includes 802.11x, or similar technology.

(l) *Personal Information.* In addition to complying with §83-26 of these Rules, all LPEP Provider employees, agents or subcontractors or employees of such agents or subcontractors with access to Personal Information are required to maintain the confidentiality of Personal Information. Personal Information:

- (1) Must only be used for the stated purpose for which it was gathered, and
- (2) May not be shared or disclosed, except for lawful purposes.

(m) *Fraud Prevention.* The LPEP Provider must ensure that controls are developed and implemented into the LPEP, Information System Components and any software contained therein to prevent the possibility of fraud, and to ensure that the LPEP Data are adequately protected. This protection must address and prevent both malicious and inadvertent damage by the general user community, as well as authorized users. Controls built into the LPEP, Information System Components and any software contained therein must include:

- (1) Segregating duties so that the initiation of an event must be separated from its authorization to prevent activities that require collusion;
- (2) Fraud detection; and
- (3) Development, test and operational environments that are separated and the roles of those involved in these activities must also be segregated, to prevent the possibility of introducing unauthorized and untested code or altering operational data.

(n) *Security Incident Management.*

(1) *Reporting Security Incidents.* The LPEP Provider must develop a procedure for reporting observed or suspected Security Incidents, threats, weaknesses, or malfunctions that may have an impact on the security of the LPEP, Information System Components and any software contained therein, and LPEP Data. All such observed or suspected Security Incidents, threats, weaknesses, or malfunctions must be reported to the Commission within twelve (12) hours of when the LPEP Provider knows of or should have known of such Security Incidents, threats, weaknesses or malfunctions.

(2) *Security Incident Management Procedures.* The LPEP Provider's Security Incident management responsibilities and procedures must be clearly defined and documented to ensure an immediate, effective, and orderly response to Incidents. At a minimum, these procedures must address:

- (i) Information system failures and loss of service;

- (ii) Denial of service;
 - (iii) Errors resulting from incomplete or inaccurate data;
 - (iv) Breaches of confidentiality; and
 - (v) Loss of integrity of the LPEP, LPEP Data, Information System Components or any software contained therein.
- (3) *Security Incident Response Procedures.* In addition to normal contingency plans designed to recover systems or services, the Security Incident response procedures must also cover:
- (i) Analysis and identification of the cause of the Incident;
 - (ii) Planning and implementation of corrective actions to prevent reoccurrence;
 - (iii) Collection of audit log information;
 - (iv) Communication with those affected by or involved in the recovery from the Incident; and
 - (v) Reporting and escalation (as appropriate) of Incidents.
- (o) *Security Staffing.* The LPEP Providers and their agents or subcontractors must employ staff familiar with generally accepted baseline security practices and methodologies in connection with their performance under this section. These resources must have oversight responsibilities for compliance with this section and be able to articulate and direct secure solutions to protect the infrastructure and the underlying data.
- (p) *Criminal Activity.* The LPEP Provider must report all instances of suspected criminal activity to the Commission and the Agency Inspector General Office at the New York City Department of Investigation within twelve (12) hours of when the LPEP Provider knows of or should have known of such instances of suspected criminal activity.
- (q) *Logging and Administration.* All LPEP, Information System Components and any software contained therein provided by or for the LPEP Provider must enable appropriate logging and auditing capabilities.
- (r) *Anti-Virus Security Policy.*
- (1) *Commercial Anti-virus Software.* Servers, desktops, and laptops must have commercial anti-virus software installed, properly configured and running at all times.
 - (2) *Remove the Virus.* Anti-virus software must be configured to automatically remove the virus.

- (3) *Users Not to Disable Anti-virus Software.* Users must not disable automatic virus scanning on their local machines.
 - (4) *Administrators Not to Disable Anti-virus Software.* Server administrators must not disable anti-virus software on server machines.
 - (5) *Administrators to Validate Files.* The LPEP Provider's administrators are responsible for validating version and signature files for desktop and laptop machines.
 - (6) *Server Administrators to Validate Files.* Server administrators are responsible for validating version and signature files for servers.
 - (7) *Users to Validate Files.* Users are responsible for validating version and signature files for stand-alone computers that are not connected to the network.
 - (8) *Signature Updates.* When possible, signature updates must be installed without user intervention.
 - (9) *Virus Signature Files.* New versions of the virus signature files must be loaded within forty-eight (48) hours.
 - (10) *Affected Devices.* All virus alerts must be followed by an immediate full scan of affected devices performed by appropriate IT personnel.
 - (11) *Root Cause Investigation.* The LPEP Provider's administrators must perform a root cause investigation when a virus is identified to ensure proper containment.
- (s) *Application Development Security Policy.*
- (1) *Security Requirements Analysis.* A comprehensive security requirements analysis must be performed for all new systems and for significant upgrades to existing systems.
 - (2) *Best Practice Standards.* System security requirements and specifications must be compliant with industry best practice standards for technologies and system configuration.
 - (3) *Interoperability.* System security requirements and specifications must ensure interoperability with all information sources and services with which it must interface.
 - (4) *Integration.* System security requirements and specifications must ensure integration with existing security services where applicable.
 - (5) *Production Environment.* The production environment must not be used for development or testing activities.

- (6) *Functionality.* All security functionality must be operational during formal acceptance and operational testing.
 - (7) *Testing of New Application.* Prior to production release of any new application, testing must be done to ensure the new application will not adversely affect any existing systems.
 - (8) *Back Out Plan.* Each application must have a defined back out plan in the unlikely event that its migration to the production environment causes service degradation.
 - (9) *Disaster Recovery Program.* Each new application must create a business continuity and disaster recovery program in accordance with the business significance of the application.
- (t) *Digital Media Re-use and Disposal Policy.*
- (1) *Rendering Information Permanently Unreadable.* Where any equipment containing digital media is to be discarded or re-used, donated, sold or otherwise transferred to an external person, organization or vendor (e.g. at the end of a lease or as an RMA (returned merchandise), the LPEP Provider must use one of the following approved methods appropriate for rendering all information on the media permanently unreadable:
 - (i) A data wiping program that will securely delete all data by methods that irreversibly wipe the physical area of storage (rather than simply removing the disk-directory reference to that information);
 - (ii) Any full disk encryption method which is compliant with the DOITT Standards and in which it can be reasonably expected that no unauthorized person has the ability to decrypt the data; or
 - (iii) Degaussing and/or physical media shredding technology which meets NIST standard 800-88 (or its successor). See http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf
 - (2) *Exception to the Disposal Policy.* The LPEP Provider support staff may evaluate data stored on any equipment transferred *internally* and bypass the requirements of this policy. All such cases must be documented and approved by LPEP Provider management to ensure accountability.
 - (3) *Transfer of Asset for Disposal.* An asset can be transferred for disposal to a vendor who has contractually committed to following one or more of the above methods.
- (u) *Encryption Policy.*
- (1) *Approved Algorithms.* Only approved cryptographic algorithms and supporting processes as described in the DOITT Standards found at

<http://www.nyc/html/doitt/html/business/security.shtml> must be used to protect business critical information.

- (2) *Confidential Data at Rest.* Where technology permits, private or confidential data at rest must be protected by encryption. The use of password protection instead of encryption is not an acceptable alternative to protecting sensitive information.
- (3) *Private or Confidential Data.* Data categorized as private or confidential must not be transitioned to removable media without management approval.
- (4) *Removable Media.* Removable media including CDs, backup tapes, and USB memory drives that contain private or confidential data must be encrypted and stored in a secure location.
- (5) *Transfer of Removable Media.* When transferring removable media, the receiver must be identified to ensure the person requesting the data is a valid recipient.
- (6) *Emails.* All emails containing data classified as private or confidential must be encrypted.
- (7) *Unencrypted Transmission.* Unencrypted transmission of private or confidential data through the use of web applications is not allowed.
- (8) *Wireless Networks.* Wireless networks must be encrypted in accordance with DOITT Standards.
- (9) *Storage of Private or Confidential Data.* Private or confidential data may only be stored on portable devices such as laptops, smart phones and personal digital assistants (PDAs) when encrypted.
- (10) *Portable Devices.* Portable devices must not be used for long-term storage of private or confidential data.
- (11) *Remote Wipe.* Where it is technologically feasible, portable devices must have the capability to be remotely wiped in the event of theft or accidental loss.
- (12) *Protections for Portable Devices.* Portable devices must have proper protections in place.
- (13) *Approved Encryption Algorithms.* Approved encryption algorithms must be a minimum key length of 128 bits.
- (14) *Private Keys.* Private keys must be kept confidential.
- (15) *Key Management.* Key lifecycle management must be implemented.
- (16) *Keys in Storage and Transit.* Keys in storage and transit must be encrypted.
- (17) *Key Choice.* Keys must be chosen randomly from the entire key space.

- (18) *Encryption Keys*. Encryption keys must allow for retrieval for administrative or forensic use.
- (v) *Password Policy*.
- (1) *Passwords and PINs*. Passwords and PINs:
- (i) Must never be shared or displayed on screen;
 - (ii) Must be classified; and
 - (iii) Must be changed when there is any indication of system or password compromise.
- (2) *Screen Lock*. A password-protected screen lock must be activated within fifteen (15) minutes of user inactivity.
- (3) *Encryption of Passwords and PINs*. Passwords and PINs:
- (i) Must be encrypted when transmitted electronically with a protocol which complies with the DOITT Standards located at http://cityshare.nycnet/html/cityshare/downloads/it_wireless/info_security_policies/Encryption_Standard.pdf; and
 - (ii) Must be encrypted or hashed when held in storage. When embedded in configuration files, source code or scripts, passwords and PINs must be either encrypted or secured with compensating controls which provide a comparable level of protection.
- (4) *Change Password*. A user wishing to change his or her password/PIN must be positively identified by demonstrating knowledge of the current password/PIN or by other comparable methods. Passwords must be changed every ninety (90) days. Passwords cannot be changed more than once a day.
- (5) *Password Delivery*. Passwords must be delivered securely to the recipient (authorized user) with an approved transmission method. Although passwords and PINS must never be shared, initial passwords may be delivered to the recipient's manager. In all cases, the recipient or manager must be positively identified before the password is delivered.
- (6) *Sensitive Accounts*. All accounts which provide access to sensitive, private or confidential information must be automatically disabled after a maximum of five (5) sequential invalid login attempts within a fifteen (15) minute period. After being disabled, the account must remain locked out for a minimum of fifteen (15) minutes.

- (7) *Use of PINS.* PINs may only be used where a numeric method for authentication is required, such as a telephone keypad. In all other cases, passwords or pass-phrases must be used for authentication.
- (8) *Number of Password and PIN Characters.* Passwords and PINs must have a minimum length of eight (8) characters with the exception of voice mail systems, and Blackberry and PDA devices issued by the LPEP Provider, its agents or subcontractors must use a password or PIN of at least 4 alphanumeric characters.
- (9) *Type of Password Characters.* Passwords must be constructed using at least one alphabetic character and at least one character which is either numeric or a special character:
- (10) *Derivation of Passwords.* Passwords must not be derived from easily guessed, common words or phrases such as those found in dictionaries (English and non-English), nor should they be constructed from user IDs, proper names or other names, words, numbers or dates readily associated with the individual user (e.g., telephone extension, Social Security number, or zip code).
- (11) *Temporary or Initial Passwords.* Temporary or initial user account passwords and PINs must be set to expire after initial use. Default passwords and PINs must be changed immediately upon the completion of the installation process and/or first login.
- (12) *Expiration Requirements.* Additional password/PIN expiration requirements and related guidelines and restrictions are provided as follows for three account types.
 - (i) User Accounts.
 - (A) User account passwords and/or PINs must expire at least every ninety (90) days.
 - (B) There are no exceptions for User account passwords and/or PINs.
 - (ii) Administrative Accounts.
 - (A) Administrative account passwords must expire at least every ninety (90) days.
 - (B) Administrative accounts must be restricted to logging in from specified IP addresses.
 - (C) When a staff member who knows an Administrative account password leaves the LPEP Provider or changes his or her job function, that password must be changed.
 - (D) Administrative accounts need not expire provided they use two-factor authentication and be either randomly generated or highly complex.

- (E) Where feasible, the use of password management software and/or certificate-based authentication is recommended as an additional control for non-expiring Administrative accounts.

(iii) Service Accounts.

- (A) Service account passwords must expire at least every ninety (90) days.
- (B) Service accounts must be known only by a limited number of staff members on a need-to-know basis.
- (C) The names of staff who know the password for any Service account must be documented and the list of names/service accounts must be kept current.
- (D) Service accounts must be restricted to logging in from specified IP addresses.
- (E) When a staff member who knows a Service account password leaves the LPEP Provider or changes his or her job function, that password must be changed.
- (F) Service accounts need not expire provided they have a minimum length of fifteen (15) characters and be either randomly generated or highly complex.
- (G) Where feasible, the use of password management software and/or certificate-based authentication is recommended as an additional control for non-expiring Service accounts.

- (13) *Reuse of Passwords and PINs.* Users cannot re-use any of the past four (4) passwords.
 - (14) *Automate Enforcement or Establish Equivalent Controls.* Where possible, the system must automate the enforcement of these requirements. Where this is not possible, equivalent controls must be established through alternative methods or procedures. For example, as an alternative to enforcing password complexity, the administrator could periodically use tools to detect weak passwords and require users with weak passwords to change them.
- (w) *Access Policy.*
- (1) *Authenticated Users.* Users must be positively and individually identified and authenticated prior to being permitted access to any LPEP Data or related networking and computing resource.
 - (2) *Connection to Only One Network.* A computer or computing device must not be connected simultaneously to more than one network.
 - (3) *Fax Modem Function.* The fax modem function must be appropriately configured on all network resources to not answer any incoming call requests.
 - (4) *Disconnect from Remote Access.* Users must disconnect from the remote access connection when not actively in use.
 - (5) *One Hour Limit.* Users must be disconnected after a maximum of one (1) hour of no user input or activity. This does not apply to application program inactivity. The application time-out period will be determined by the application owner. Users must not use any method acting in their absence to avoid the inactivity disconnect.
 - (6) *Confidentiality of Passwords and Authentication Mechanisms.* Users are responsible for maintaining the confidentiality of passwords or other authentication mechanisms that are assigned in conjunction with the remote access service. A user's credentials must be classified as restricted information. Individual passwords must never be shared.
 - (7) *Confidentiality of Data Remotely Accessed.* Users must protect the confidentiality and integrity of data that is accessed remotely. This includes, but is not limited to ensuring that LPEP Data is either erased from the remote device after use or appropriately protected based on the level of sensitivity of the information.
- (x) *User Responsibilities Policy.*
- (1) *Safeguard.* The LPEP Provider is responsible and accountable for safeguarding LPEP Data from unauthorized modification, disclosure, and destruction.

- (2) *Protect Critical Data.* Critical data and removable data devices (USB drives, CDs, external drives, etc.) must be protected by appropriate physical means from modification, theft, or unauthorized access.
 - (3) *Faxing Sensitive Information.* When faxing sensitive information, the recipients must be called in advance to ensure the fax is properly managed upon receipt.
 - (4) *Remove Documents.* When faxing, copying or printing is completed, all documents must be removed from the common area.
 - (5) *Screen Lock Workstations.* Users must screen lock their active workstations when left unattended.
 - (6) *Protect PDA Devices.* Users must utilize passwords to protect PDA devices and voice mail systems.
 - (7) *Protect Credentials.* Individual users must properly protect credentials for their accounts. Individual credentials must never be shared.
 - (8) *Group IDs.* The use of group IDs is prohibited.
 - (9) *Written Passwords.* Writing down passwords is strongly discouraged. Passwords that are written must be appropriately stored to prevent disclosure to anyone other than the individual user. Passwords that are written must not reference the account or data store they protect.
 - (10) *PINs for Blackberry.* PINs for Blackberry, PDA, and voicemail must be a minimum of four (4) digits.
- (y) *Vulnerability Management Policy.*
- (1) *Inventory Computing Resources.* All computing resources must be inventoried to determine the types of hardware, operating systems, and software applications that are used within the organization.
 - (2) *Review and Update Inventory.* The computing resource inventory must be periodically reviewed and updated in order to accurately reflect the environment. The inventory must be updated whenever new resources, hardware, operating systems, or software are added to the environment.
 - (3) *Monitor Sources of Threat and Vulnerability.* The LPEP Provider must continuously monitor sources of threat and vulnerability information from internal and external security sources.
 - (4) *Review Vulnerability Information.* The LPEP Provider must perform a timely review of vulnerability information received from reputable sources.

- (5) *Perform Analysis.* The LPEP Provider must perform proper analysis to confirm applicability of identified vulnerabilities in comparison to system inventory.
- (6) *Categorize Vulnerabilities.* The LPEP Provider must categorize applicable vulnerabilities according to a vulnerability classification. At a minimum, classification must consist of urgent, routine, or not applicable.
- (7) *Remediate Vulnerabilities.* The LPEP Provider must have a process to remediate vulnerabilities based on significance.
- (8) *Automated Patch Management Tools.* The LPEP Provider must use automated patch management tools to expedite the distribution of patches to systems.
- (9) *Action Plan.* The LPEP Provider must maintain a process that develops an action plan to remediate all verified vulnerabilities.

