LANSING HOUSING
LHC
COMMISSION

419 Cherry St., Lansing, MI 48933 Telephone: (517) 487-6550 Fax: (517) 487-6977

Lansing Housing Commission
Policy No. 2009-11
Computer and Electronic Equipment

Introduction

The purpose of this IT Security Policy and Security Procedure manual is to establish a comprehensive program to protect the security of sensitive information collected, stored, received, or transmitted by LHC. LHC has an obligation to protect its confidential and proprietary data; protect its clients' interests; and comply with various federal, state, and industry regulations.

The policies and procedures included in this manual apply to all members of LHC's workforce —including both employees and independent contractors who perform work under the supervision of LHC.

Access Authorization

Staff members receive authorization to access proprietary data and to use LHC's network, devices, and cloud services, to conduct transactions, and to run software applications based on their job responsibilities and qualifications. Authorization enables staff members to use the information resources of the company. Staff members should not access information for other staff members who lack appropriate authorization, or for anyone outside the company, unless expressly authorized by company management. Only authorized staff members are allowed to use workstations (computer terminals, personal computers, and other devices) that can access company data. A unique user ID and password are required to use LHC's information systems.

Assigned Security Responsibility

LHC will appoint a security official who is responsible for:

- Establishing LHC's security program and overseeing its implementation
- Ensuring compliance with federal, state and industry security regulations and standards
- Reviewing all purchases or acquisitions of information technology for consistency with LHC's security policies and standards
- Investigating security incidents (i.e., known or suspected violations of security policies and procedures, breaches in security measures and the security of LHC's protected health information)
- Reviewing information system activity to ensure compliance with LHC's security policies and procedures
- Developing and implementing security training and awareness program for LHC's employees and staff

- Reviewing and approving the security provisions of contracts with business partners
- Reviewing annually compliance with security requirements, policies, and standards
- Complying with the HIPAA requirements for an assigned HIPAA Security Officer

Authorization/Supervision
All employees and other members of LHC's workforce must be specifically authorized to use the information resources or to access company data.

Automatic Locking for Windows and Mac OS computers
All workstations are configured to lock the user’s screen after 15 minutes of inactivity. After being automatically locked, a user must re-enter his or her user name and password to resume the interrupted activity. Users may not disable this automatic screen locking feature.

Automatic Locking for iPhone, iPad, and Android mobile devices
All mobile devices are configured to lock the user’s screen after two (2) minutes of inactivity. After being automatically locked, a user must re-enter his or her screen unlock code to resume the interrupted activity. Users may not disable this automatic screen locking feature.

Business Continuity Plan
LHC will develop a comprehensive written plan to continue business during, or resume business immediately after a disruption or disaster. This plan must go beyond the tasks required to recover LHC’s IT infrastructure, and include a:

- Risk Analysis identifying potential risks and mitigation strategies
- Business Impact Analysis to identify LHC’s functions and the effect of critical functions
- Communications Plan to contact employees, customers, and vendors
- Alternate site plan if the company facilities are not available
- Ability to redirect incoming phone calls; e-mail; access to company on-line resources
- Ability to continue critical services to customers
- Ability to continue critical technology functions
- Recovery strategies based on the Risk Assessment and Business Continuity Plan

The plan must be tested with a simulated disaster at least once per year. Testing may be as little as proving that critical IT infrastructure can be recovered to a full-scale drill where employees work from an alternate site.

Client Security

Only employees authorized by LHC management may access client systems, and only for authorized purposes. LHC employees are required to maintain confidentiality of client information as if it were LHC information.

LHC users of information systems must never require the provision of private Customer information, which is unnecessary for the completion of a transaction or for the provision of services. No service provided by LHC may be denied to any Customer if they refuse to provide unnecessary private information. The LHC Executive Director will resolve all disputes about necessary private information.

Any client information protected by federal, state, or industry regulations must be managed in accordance with those regulations. Specifically,

- No protected information may be removed from client site by physical or electronic means without specific authorization by LHC management.
- All protected information must be protected with the encryption standards set forth in the applicable regulation(s).
- No information overheard or seen at customer sites may be shared for purposes other than those authorized by LHC
- Employees will be trained on all regulations appropriate to their work with clients
- Employees will be subject to all civil and criminal penalties for non-compliance with regulations required of clients

Data Classification

The security official must develop a process to classify and secure company data. Classifications must include:

- Criticality for prioritized recovery after a disruption or disaster
- Sensitivity of company data that is proprietary, including customer lists, designs and plans, employee records, pricing, etc.
- Protected information including Social Security numbers, health information, financial information; credit card information, and all other information protected by state, federal, or industry compliance regulations

Access to data must be controlled so that it may be accessed only by those with an approved need. Data must be stored in secure location on the network or in structured software environments. Data may not be removed from LHC's local network without specific authorization and may only be stored on secured devices.
Data may only be accessed for authorized purposes. Snooping into company or employee data or communications is expressly prohibited.

Disposal

Before sale or disposal, all computer hardware is examined and certified as containing no company data or information enabling security features of LHC's information system, including information that would enable a user to access the company's information system.

All storage devices and media are to be given to the security official for disposal. Storage devices and media may be disposed of only by an authorized staff member. Prior to disposal, the storage media is sanitized either by means of degaussing, triple overwriting, or physically dismantling and destroying the storage media.

All software and data are removed from all computer equipment prior to sale or disposal of the equipment. Disk drives are sanitized by degaussing or triple overwriting. Logs are maintained of all computer equipment and storage media that have been disposed of. These logs include the date on which storage media were sanitized and a description of the sanitizing method used.

E-Mail

The LHC e-mail system is for authorized business purposes only.

- No personal messages; harassing messages; sexually explicit material; or jokes may be sent through the company system.
- No sending of unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- No form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- No unauthorized use, or forging, of email header information.
- No solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

- No creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- No company information may be sent to/from employee personal accounts without specific management authorization.
- No company information may be sent to anyone outside of the company unless for authorized business purposes
- Only administrators authorized by LHC may manage the e-mail system and have access to others' messages. Snooping into others' e-mail is expressly forbidden and grounds for immediate dismissal.
  Unified communications systems convert phone messages into e-mail making them subject to all e-mail controls and regulations.

Encryption and Decryption

The security official identifies any circumstances under which information transmitted by the company must be encrypted to prevent its use by unauthorized recipients.
The security official ensures that staff members responsible for transmitting information are familiar with encryption requirements and the use of encryption software.
Staff responsible for transmitting information must encrypt it when directed to do so by the security official.

When determined necessary by the security official, information transmitted outside the company is encrypted to prevent use by unauthorized individuals.
Data should be encrypted when it is transmitted over a network that might be accessible by unauthorized individuals. Information that can be used to alter or defeat LHC's security measures also should be encrypted.
The technical methods used to implement encryption and decryption are determined by the security official.

Facility Access Controls

The security official develops and implements policies and procedures that allow only authorized staff members and contractors to physically access LHC's electronic information systems. The areas of the company's facilities in which components of its information systems are housed are physically secure and deny access to all but properly authorized staff members.

Facility Security Plan

All computer equipment and devices that are used to access, transmit, or store company data are protected from unauthorized physical access, tampering, and theft.

Lansing Housing Commission
Policy No. 2009-11
Computer and Electronic Equipment

Network servers and storage devices must be housed in a secure location that cannot be accessed by visitors to the company. The equipment closet, office, or room in which such equipment is located must be locked at all times.

Back-up copies of company data are stored in a secure location. Back-up media stored on-site are kept in locked cabinets. Back-up media stored off-site are stored in a manner that prevents physical access by anyone lacking proper authorization.

Information Access Management

The security official is responsible for developing and implementing procedures to authorize staff members' use of LHC's information resources. This includes establishing access to company data, based on the staff member's job responsibilities and qualifications.

Authorization is limited to the information the individual needs to fulfill his or her job responsibilities.

Information System Activity Review

The security official periodically reviews records of information system activity, such as audit logs, access reports, and security incident tracking reports.
The security official must review all security incident reports and ensures that any breaches in security have been corrected.

The security official must regularly review records of system activity to identify any patterns of activity that suggest LHC's security policies and procedures have been breached, either by members of its workforce or by outside individuals or organizations. The security official determines whether security has been violated and takes appropriate corrective action, including changes in security policies and procedures. The security official maintains records of all reviews of security incidents and system activity, and reports any findings to other members of LHC's management.

Log-in Monitoring

Log-in procedures limit the number of unsuccessful log-in attempts to five (5), after which a user must contact the information system administrator to have his or her password reset.

The security official must review log-in monitoring records and investigate patterns that suggest the possibility of security breaches or attempted penetration of security measures by unauthorized users.

Lansing Housing Commission
Policy No. 2009-11
Computer and Electronic Equipment

Operating systems must be configured to monitor log-in attempts. The security official maintains a record of any investigations of suspected efforts to penetrate security measures by unauthorized users.

Media Re-use

All storage media, including removable disks, rewritable CD-ROMs, and back-up tapes, must be "sanitized" before re-use.

Mobile Device Encryption Policy

This policy applies to any mobile device issued by LHC or used for LHC business which contains stored data owned by LHC.
All mobile devices containing stored data owned by LHC must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, tablets, phablets, and mobile phones.

Users are expressly forbidden from storing LHC data on devices that are not authorized by LHC, such as storing LHC email on a personal cell phone or PDA.Owners of any personal device that contains LHC data shall give LHC explicit authorization to utilize remote wipe technology to remotely disable and delete any data stored on a cell phone or other portable device which is reported lost or stolen.

The loss or theft of any mobile device containing LHC data must be reported immediately.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

It is the policy of LHC that mobile computing and storage devices containing or accessing the information resources at LHC must be approved prior to connecting to their information systems, this pertains to all devices connecting to the LHC network, regardless of ownership.

Monitoring

LHC reserves the right to monitor all computer use. There should be no expectation of privacy when using a company-owned device. Users may be subject to electronic monitoring (i.e. closed-circuit TV, other camera systems, Intercoms, etc.) of their activities while on LHC premises.

This monitoring may be used to measure a user's performance as well as to protect user private property, user safety, and LHC property. In areas where there is a reasonable expectation of privacy, such as bathrooms no electronic monitoring will be performed.

Password Management

This section applies to all personnel who have or are responsible for an LHC network account, email account, cloud-based service account, or has been granted any form of access that supports or requires a password. This policy applies to any system or cloud service that resides at any LHC facility, has access to the LHC network, or stores any nonpublic information.

Policy

1. Users must create “complex” passwords that are a minimum of 10 characters in length, if the system they are logging into will allow it. Complex passwords include both upper and lower-case letters, and one or more numbers and/or special characters.
2. Where possible, users must use a unique password for all account logins held by that user, including any website passwords.
3. Users are prohibited from using LHC account passwords for any non- LHC accounts, such as personal email, banking, Facebook, Twitter, etc.
4. Passwords must never be reused. When passwords are changed, a unique (new) password should be selected and used rather than recycling a previously used password, or incrementing a number in the password.
5. Users are required to use the LHC administered global password management database, LastPass, to record all production passwords.
6. Users are prohibited from sharing passwords with anyone, even co-workers. All passwords are sensitive, confidential LHC information.
7. Users are prohibited from inserting passwords into email messages or other forms of electronic communication, unless the message or communication is encrypted.
8. Users must change all user-level passwords (Office 365, Windows Network/Computer Login, Box) at least every 120 days.
9. System Administrators are required to change all system-level passwords (e.g., administrator, admin, application administration accounts, etc.) at least every 120 days.

10. If a user suspects an account or password has been compromised, they must report the incident to the designated Cybersecurity Officer and change the password in question as soon as possible.
11. The Security official or their delegate may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it immediately. All user-level and system-level passwords must conform to the Strong Password sub-section under the General Password Construction Guidelines shown below.

General Password Construction Guidelines

LHC uses passwords for various purposes. Some of the more common uses include: user-level accounts, Web accounts, email accounts, screen saver protection, voicemail passwords, and network device logins.

Strong passwords have the following characteristics:

1. Contain both upper and lower-case characters (e.g., a-z, A-Z).
2. Include digits and punctuation characters as well as letters, e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
3. Are at least ten alphanumeric characters long.
4. Are not a word in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, etc.
6. Are never written down or stored on-line unless within an encrypted password storage system, such as with LastPass.

Poor, weak passwords have the following characteristics and should be avoided:

- They contain less than ten characters.
- They are a word found in a dictionary (English or foreign).
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms, names, commands, sites, companies, hardware and software.
- The words “LHC,” and geographical indicators such as “San Jose,” “San Fran” or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns such as aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- The use of the word ‘Password’ in any variation with numbers.

Password Protection Standards – List of Don'ts

A. Don't reveal a password to anyone over the phone.
B. Don't reveal a password in an email message.
C. Don't reveal a password to your supervisor.
D. Don't talk about a password in front of others.
E. Don't hint at the format of a password (e.g., "my family name").
F. Don't reveal a password on questionnaires or security forms.
G. Don't share a password with family members.
H. Don't reveal a password to a co-worker when you go on vacation.
I. Don't write down a password and store it anywhere in your office.
J. Don't store passwords in a file on any computer, including a handheld computer, phone, or tablet without encryption.
K. Don't use the "Remember Password" feature of any website or browser.
L. If someone demands a password, DO NOT give it to them.

The security official or their delegate must review password policies with a user when he or she first receives his or her user ID.

The security official must monitor password usage and identify any patterns that suggest password policies and guidelines are not being followed.

The security official must require staff members who frequently lose or forget their passwords to complete retraining on the correct use of passwords.

Person or Entity Authentication

All users must use their passwords when logging on to LHC's information system.
Passwords should not be written down or disclosed to other members of the staff, friends, family, or anyone else.
A staff member may not use another staff member's user name and password to access LHC's information system.
Staff members may not give their passwords to other staff members.
Users must change their passwords once they become known to others.
Users should change their passwords at least once every six months, but not so frequently that they are likely to be forgotten.

Client Access Passwords

LHC employees who access client networks must use a unique identifier for logging purposes. This may be either a unique logon and password or a shared logon and password plus a second method of authentication that can be tracked back to a specific user. Sharing network account passwords or allowing others to gain access to your network account is a violation of this policy. Both the user who owns the account, as well as the user not officially authorized to use the account, have violated this policy.

Protection from Malicious Software

Anti-malware software must be installed on all endpoint devices and servers to protect LHC and its information from attack by malicious software such as computer viruses, worms, and Trojan horses. This software must be maintained with current subscriptions and regularly updated; must be turned on; and must be installed to prevent users from disabling or removing the software.

Staff members must not disable anti-virus software and must immediately take action to report virus infections and remove viruses from affected machines when the anti-virus software identifies an infection.

The security official must maintain a log of virus infections and detections that includes a record of successful eradication of viruses and cleaning of affected files and computer applications. Staff members are responsible for reporting all viruses detected by anti-virus software. The security official must confirm that the viruses have been successfully removed from the affected machines.

Social Media

Staff members with access to the Internet should not open e-mail messages and e-mail attachments from unknown senders, or any message with links to banks, the IRS, credit card companies, etc.

Risk Analysis

The security official must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of company data. A comprehensive analysis of security threats must be conducted at least every three years. It must be reviewed annually and updated as needed.

The risk analysis must comprehensively describe LHC’s information system, including the following components:

- The computer hardware and software that make up LHC's information systems
- The categories and qualifications of staff members who use the systems
- The functions and activities that are supported by the information systems

Lansing Housing Commission
Policy No. 2009-11
Computer and Electronic Equipment

- The data and information that are collected, processed, and stored by the information systems
- The physical environment that houses information system components
- On-site and off-site storage of information
- The organizations to which information is transmitted
- The data and information that are transmitted to other organizations
- The internal and external connections between LHC's information systems and the information systems of other organizations

The risk analysis must identify threats to the security of LHC's company data, including natural, human, and environmental threats. The risk analysis must identify the nature of each threat or vulnerability and how each may damage information security.

The risk analysis must indicate the preventive measures that LHC has implemented (or is planning to implement) to limit the damage that might be caused by each threat or vulnerability.

The risk analysis must evaluate the likelihood that each security threat or vulnerability might occur.

The risk analysis must describe the nature and extent of the damage each threat might cause to the integrity, availability, and confidentiality of LHC's information resources.

The risk analysis must identify high-priority threats that are the focus of risk-management efforts.
The risk analysis must recommend controls or actions to lessen the risk associated with high-priority threats.

The risk analysis must be reviewed and approved by the security official. The results of the risk analysis must be shared with other members of LHC management team.

Risk Management

The security official must implement a comprehensive risk-management program based on the results of the risk analysis.

The risk-management program must include the security measures identified by the risk analysis at least every three years. The purpose of these security measures is to reduce risks and vulnerabilities to a reasonable and appropriate level.

Lansing Housing Commission
Policy No. 2009-11
Computer and Electronic Equipment

The risk-management plan must identify the specific actions that will be taken to implement the security measures identified in the risk analysis, including a timetable for implementation of each measure.

The risk-management plan clearly must describe the magnitude of the risks that will be accepted if the plan is adopted.

The plan must include documentation that the accepted risks are reasonable. Risks are considered reasonable if they cannot be reduced, can only be reduced by adopting measures that would severely impair the ability of the information system to perform its intended functions, or can be reduced only by implementing measures whose cost substantially exceeds the anticipated costs of any security failures that would be prevented.

The risk-management plan must be reviewed with and approved by the governing body of LHC annually.

Sanction Policy

Employees and other members of LHC’s workforce are subject to sanctions for violating LHC's security policies and procedures. Violations should be reported, in writing, to the HR Manager.

Violations of security measures and the penalties associated with them include the following:

Minor Security Breaches

This category of breaches consists of minor or unrepeated violations of security policies.

> S*anction*: A minor infraction such as this will result in brief counseling and, if necessary, additional security training.
>
> *Example:* A staff member briefly leaves her workstation unattended without logging off.

Significant Security Breaches

This category includes any documented violation of the security of company data that could easily have been avoided had the staff member exercised due care.

Sanction: A pattern of repeated, significant violations of security policy may be grounds for suspending an employee and may lead to termination of the employee.

Example: A staff member attaches a note to his workstation monitor that gives his user ID and password.

Severe Security Breaches

This category includes any deliberate violation of security policies and procedures or confidentiality requirements that are not justified by considerations of employee safety or were not necessary or unavoidable during an emergency.

Sanction: A deliberate violation of security policies will result in the immediate suspension of the employee or other workforce member and the termination of all access to information resources.
Example: A staff member makes a copy of company data and gives it to a vendor without obtaining required authorizations.

Criminal Security Breaches

This category includes any deliberate violation of security policies and procedures or confidentiality requirements for harm or personal gain.

Sanction: A deliberate violation of security policies for harm or personal gain will result in the immediate referral of the situation to criminal authorities for investigation and prosecution.

It is the responsibility of an employee's supervisor to identify security breaches and apply appropriate sanctions.

An employee or other workforce member who believes that he or she has been wrongly charged with a security violation may appeal the imposition of sanctions to the security official.

Security Awareness and Training

The security official is responsible for developing and implementing a security awareness and training program for all members of LHC’s workforce, including professional staff, company partners, and management. The training program covers:

- ➢ The definition of security (availability, integrity, confidentiality)

- Threats to security (natural, human, and environmental)
- Methods of safeguarding security
- Security features of LHC's information system and applications
- Use of major applications
- Policies on installation and configuration of software
- Controls on access to information
- Correct use of anti-malware software
- Contingency plans and disaster procedures
- Workstation policies
- Good security practices (workstation use policies)
- Security incident reporting procedures
- User ID and password policies
- All staff members, including management and professional staff, are required to complete security training before they can use LHC's information systems or are permitted to access company data.

New staff members receive security training as part of their orientation.
Contractors and consultants receive training and/or information on LHC's security policies and procedures.

Security Incident Procedures

Security incidents must be reported promptly to the security official. Incidents, including attempts to discover someone’s password, should be reported by the staff members responsible for the incident or staff members who identify the incident.

No sanction or penalty is imposed for simply reporting a security incident.
The security official must investigate security incidents and determine:

- Whether a breach of security has occurred
- The appropriate actions to take to repair any damage or potential damage to security that the incident might have caused
- The security official must ensure that actions needed to repair any damage caused or potentially caused by a security incident are taken.

The security official must document the report of a security incident, the findings of the investigation, and any actions taken in response to those findings.

Lansing Housing Commission
Policy No. 2009-11
Computer and Electronic Equipment

Security Policy

This security policy must be reviewed by company management each year and updated as necessary. The policy and any changes must be communicated to all employees.

Social Media

Use of social networking sites and/or that are opinionated, pornographic, discriminatory, inflammatory, or otherwise Inappropriate for a standard business enterprise is strictly prohibited. Internet users have individual responsibility to report any violations of this policy of which they may become aware. Violations should be reported to the HR Manager

Sharing information about the company in social media without expressed authorization from management is expressly prohibited. Employees must remove any references to company information immediately upon request.

Termination Procedures

A staff member's authorization to use information resources and to access company data ends immediately upon termination or suspension of employment. Staff members must turn in keys or key cards that give access to computer equipment or facilities upon termination of their relationship with LHC.

The security official should be notified of the effective date of any employee termination or of the date on which a staff member’s authorization to use LHC's information resources will terminate. The staff member's user account on LHC's information system must be disabled or deleted upon termination of the relationship with LHC.

The staff member will surrender any protected information, including information contained on storage media (e.g., a CD-ROM or removable disk, data storage key, etc.) that may be in the staff member's possession at the time the relationship with LHC ends.

Workforce Clearance

A staff member will be authorized to access company data and to use information resources if the following are true:

1. They meet the minimum professional or technical qualifications for the position they occupy,
2. They have not been disciplined for serious infractions of security in previous jobs.

Lansing Housing Commission
Policy No. 2009-11
Computer and Electronic Equipment

Staff members who have been disciplined for infractions of security policies and procedures may be granted restricted access until their trustworthiness has been established to the satisfaction of the security official.

When verifying credentials and checking references, the staff member responsible for hiring should determine that the candidate has not been sanctioned or disciplined for infractions of security policies or standards in the past.

Any restrictions on access to information resources should be communicated to the security official so the necessary technical restrictions in access privileges can be implemented.

Workstation Use
Users must observe the guidelines on use of workstations:

All users must log off all workstations overnight rather than leaving them locked. This includes workstations in private offices.
Screens should be positioned within workstations so that they are visible only to the persons who use them.

Staff members should not access proprietary or confidential information when visitors to LHC may be able to view the information that is displayed on their screen.