ADMINISTRATIVE ORDER	Approved By: City Manager	No. # 36 **Effective Date**: 01/01/2023 **Revised:** N/A

Subject: **Enterprise System Security Policy**

INTRODUCTION

Information Technology Management and Staff, End User Management and Staff

PURPOSE

Effective security is a team effort involving the participation and support of every City of Highland Park (City) network user and affiliate who deals with information and/or information systems. This policy defines what the City Information Technology (IT) Division deems minimum criteria to operate the IT function in a controlled and secured environment. This policy also specifies the system security requirements for the software, hardware, networks, data, platforms, databases, and end-user developed systems.

SCOPE

This policy is applicable to the following:

1. All core business software, hardware, networks, and system configurations.
2. All data related to the City including data created, received, transmitted and maintained by the City.
3. All end users at the City, which includes anyone with a computer attached to the network or anyone using the City computer resources.
4. All remote access connections used to do work on behalf of the City, including reading or sending email and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to VPN, and RDP.
5. Any person who supplies his or her own computer and that computer is connected in any way to the City's computer network.
6. Exemptions to this policy are third party systems such as Water Plant or Lift Stations SCADA systems as those are managed by City authorized SCADA Integrators or consultants.

POLICY

Configuration Management

1. Network Device
    a. There must be standard configurations documented for and applied to all network devices.
    b. Access to the network device configurations must be restricted to authorized IT personnel only.

2. Platform
    a. There must be standard configurations documented for and applied to all platforms.
    b. Access to the platform configurations must be restricted to authorized IT personnel only.
3. Database
    a. Access to the database configurations must be restricted to authorized IT personnel only.

Data Ownership

1. All data on City computers and equipment is the property of the City subject to public disclosure only in accordance with the Illinois Freedom of Information Act (FOIA). In the event of a FOIA request for IT systems information, exemptions included in FOIA shall be used, as legally applicable, to exempt the disclosure of any IT information which may jeopardize the safety, security, and integrity of the City's IT systems.
2. Ownership responsibilities for databases, master files, and other shared collections of information reside with department managers and not the IT department.
3. Due to the sensitive nature of some communications within the City, including, but not limited to email and voicemail, that are processed or stored on the City network, these will be considered confidential but subject to disclosure in accordance with FOIA with appropriate exemptions used as legally applicable, and as such will be protected.
4. City business should only be conducted on City approved devices and software systems. Any City business conducted on other platforms is also subject to the Freedom of Information Act.

Data Transmission

1. Reasonable steps should be taken to ensure that all data transmissions are accurate, complete, up-to-date and stored in a secure environment accessed only by authorized persons for legitimate business purposes.

End User Computing

1. End-user developed spreadsheets, programs, and applications should be controlled and secured based on the sensitivity of information they contain.
2. End-user developed files should be included in the backup regime.

End User Training

1. End users should be properly informed of the IT policies and procedures related to security awareness, password controls, etc.
2. End user training should include IT security awareness training and should be conducted and/or offered at least annually.

Incident Management

(Note: An incident is defined as a non-routine event. For example, routine events are typically captured in an operating systems event, application, or security log; while a non-routine event would be a network security breach or a network user email being read by an unauthorized person).

1. An incident management system must be in place to ensure all system events are recorded, analyzed, and addressed. See the Incident Management Policy.
2. The system must provide for adequate auditing and review of recorded incidents. See the Log and Monitoring Policy.

Wireless Services

1. Security
    a. It is the responsibility of each network user to use reasonable care in handling and protecting wireless devices provided by or paid for by the City.
    b. Network users are required to utilize wireless devices and services in an approved, ethical, and lawful manner to avoid loss or damage to the City's image, or financial interests, and to comply with other acceptable City use policies and procedures.
2. Privacy
    a. Network users do not have, and should not expect, privacy rights while using any City issued wireless devices or services.
3. Wireless Access Points
    a. The installation and use of wireless access points is prohibited unless prior authorization is received from the IT department.

Remote Access

1. It is the responsibility of the City network users, contractors, vendors and agents with remote access privileges to the City network to ensure compliance with security procedures related to remote access.
2. Remote access to the City network should be adequately restricted to a secure medium such as VPN.
3. Organizations or individuals who wish to implement non-standard remote access solutions to the City's production network must obtain prior approval from the IT department.

Logging and Monitoring (See Log and Monitoring Policy)

1. The IT department must configure all critical systems to automatically log system activity (i.e., events, application events, etc.) as related to networks, network devices, operating systems, database technologies, applications, and other technologies.

2. System security logs (i.e. operating & database systems and network devices) must be retained for 90 days and application-layer security logs must be retained for 90 days to support incidents management, compliance testing and research as deemed necessary. All logs will be retained for 180 days.
3. IT personnel will review each system log or the aggregation of system logs on a periodic basis not less than annually.

Network Security

1. Virus Protection
    a. All workstations connected to the network and network servers, whether strictly used for data storage, email, or other purposes, will have a virus protection program with the most current virus definition file.
    b. Virus definition data files will be kept current by either automatic file updating on a daily basis or by manual installation.
    c. Under no circumstances will this virus software be deactivated or removed for the purpose of intentionally bypassing the protection activity for which it is intended.
2. IDS/IPS
    a. If an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) is implemented it must be properly configured and configured to alert a Systems Administrator if a breach is detected.
3. Firewall Security
    a. All Internet connections, regardless of method of connectivity, must be protected by a firewall.
    b. All firewall platform changes must be approved by the IT manager and follow the formal change management process.
    c. Firewall administrators must have named accounts on the firewall, and must use passwords that conform to the City Password Policy.
    d. All firewalls logs must be enabled and must be retained for a minimum of 30 days.
    e. Logs of critical events, such as spoofing attacks, should be reviewed regularly to ensure no attack, directed at the City, goes unnoticed.

DISCIPLINARY ACTIONS

Failure to comply with the above stated policy may lead to corrective action, up to and including termination of employment.

DEFINITIONS

Term	Definition
City	City of Highland Park
Network User	All City employees (including full and part-time and seasonal workers), vendors, and independent contractors working on behalf of the City of Highland Park.

Severity	The relative assessment indicating the degree of impact for a reported issue. It is the key indicator for determining how IT responds and works on reported problems.

REFERENCES / DOCUMENTS/FORMS
None

EXCEPTIONS
None

RECORDS
None

MATERIALS/EQUIPMENT
None

APPENDIX
None