
	ADMINISTRATIVE ORDER	Approved By:  City Manager	No. # 38
			Effective Date: 01/01/2023 Revised: N/A
Subject: Log and Monitor Policy			

PROCESS OWNER/RESPONSIBLE PARTIES

Information Technology Management and Staff.

PURPOSE

The City of Highland Park (City) relies on the availability of its systems and data to perform daily tasks. To ensure that all systems remain available it is important to review the systematic logs these systems generate as processing events occur. Often these logs can be helpful in troubleshooting irregular or unexpected system behavior. This policy outlines the process IT personnel will take to ensure system logs are captured, reviewed and retained. This policy also establishes the minimum requirements for the logging and monitoring of all critical systems, networks, network devices and technologies implemented at the City.

SCOPE

This policy is applicable to all core business software, hardware, networks, and system configurations. This includes, at a minimum, all applications, databases, platforms, networks, network devices, and appliances.

POLICY:

Logging of Events

1. IT personnel 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. Remote network connections will be logged.
3. Third party access into the network to support any type of troubleshooting will be logged.
4. All activity performed using a 'root', 'administrator', or 'super-user' type account must be logged.
5. System generated activity related to IT processes (i.e., backups, patches, security events) must be logged.
6. Systems should be configured to log authentication attempts, authenticated user (by user ID), access date and time (i.e., timestamp), source of access, duration of access and, actions executed.
7. Only IT personnel are authorized to adjust the information required to be logged and only after performing a risk assessment relative to the system begin adjusted.
8. All logs should be configured to automatically port to a syslog server. The syslog server should be hardened and access strictly controlled.
9. The City will/has implemented a security information and event management (SIEM) solution to aggregate system generated logs.

10. The SIEM solution will be configured to correlate events into incidents. Incidents will be investigated as deemed necessary.
11. Security Logs are only subject to public disclosure in accordance with the Illinois Freedom of Information Act (FOIA). Such disclosures shall use exemptions, as legally applicable, to exempt disclosure of any information which may jeopardize the safety, security, or integrity of the City's IT systems.
12. Any suspected breach of the City's network, software, email, or other City-related software, subscription, or service must be immediately reported to the IT Division. IT personnel will triage, notify, and advise the Finance Director and City Manager.

Log Retention

1. 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.
2. Security measures must be implemented to ensure that unauthorized parties cannot access, modify, or delete logs.

Monitoring by IT Management

1. IT personnel will review each system log or the aggregation of system logs on a periodic basis not less than annually.
2. All isolated events or incidents will be investigated as deemed necessary by the IT Management.
3. IT Management will ensure a Root Cause Analysis (RCA) is completed for all incidents deemed necessary.

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.

REFERENCES / DOCUMENTS/FORMS:

None

EXCEPTIONS

1. Service account activity is not required to adhere to this policy.
2. Application-level accounts (i.e., accounts not associated to a user) are not required to adhere to this policy.

RECORDS

None

MATERIALS/EQUIPMENT

None

APPENDIX:

None