
	ADMINISTRATIVE ORDER	Approved By: 	No. # 35
		City Manager	Effective Date: 01/01/2023 Revised: N/A
Subject: Data and System Backup 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 ensure continuity of operations. A critical component to ensuring the continuity of Information Technology (IT) operations is ensuring the systems and data are periodically backed-up. This enables recovery of systems and data in the event of an unplanned disruption to IT operations. This policy establishes requirements for periodic backups of systems and data and a current and documented recovery strategy.

SCOPE

This policy is applicable to all core business data, network files and documents, software, networks, and system configurations. This includes, at a minimum, all platforms, databases, applications, and network configurations.

POLICY

Backups

1. All critical systems and data files should be part of the backup schedule.
2. The backup process should be periodically reviewed to update the backup schedule with any new systems and/or data files.
3. Backups should be performed on a regular basis.
4. Backup activity should be monitored and errors investigated in a timely manner.
5. Media containing the backups, whether disk or tape, will be off-site from the primary source location.
6. Backup restoration should be tested at least annually.
7. Critical data on remote computers should be included in the backup schedule.
8. All files pertaining to network devices and components, including configuration files, must be backed up to ensure a working copy of the device can be restored at any time. These files should be backed up to make sure recent changes are archived.

Disaster Recovery Plan (DRP)

The content of the DRP, at a minimum, should include these sections:

1. Scope and Limitations
2. Assumptions
3. Reporting Structure Overview
4. Disaster Recovery Strategies
5. How-To Information for Exercising the Plan
6. Plan Maintenance
7. Business Department-Specific Information
8. Technology-specific Detailed Recovery Steps
9. Technology Vendor Contact Information
10. Recovery Test Plan Overview

DRP Review, Approval and Activation

1. The IT manager and department leaders that own the systems should approve the DRP.
2. The IT manager should determine the need to activate the DRP, conditional upon the approval of the City Manager or designee.
3. The DRP should be updated on a continuing basis and reviewed annually.
4. The DRP should be tested on a periodic basis for all critical systems.
5. Responsibilities of staff should be followed as noted in the Disaster Recovery Plan.

DISCIPLINARY ACTIONS

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

DEFINITIONS

None

REFERENCES / DOCUMENTS/FORMS

None

EXCEPTIONS

None

RECORDS

None

MATERIALS/EQUIPMENT

None

APPENDIX

None