Adopted: October 8, 2024

EOHWC - IT Data and Disaster Recovery Policy

1. Purpose

The purpose of this policy is to establish procedures for the maintenance, backup, and recovery of IT systems and data. The policy also creates procedures to follow in the event of a disaster or significant disruption to EOHWC IT systems. This ensures business continuity, minimizes downtime, and protects the integrity and availability of data.

2. Scope

This policy applies to all IT systems, data, and personnel involved in the management, operation, and maintenance of the organization's IT infrastructure.

3. Objectives

To create guidelines on good data and IT equipment management to avoid disasters.
To define the roles and responsibilities for disaster recovery.
To establish a framework for the recovery of IT systems and data.
To minimize the impact of disruptions on business operations.
To ensure timely and effective response to disasters.

4. Roles and Responsibilities

To ensure that IT systems and data within EOHWC are maintained properly, there are several roles and responsibilities that must be provided through a hired IT professional or divided amongst staff. Personnel involved will be denoted as part of the “Disaster Recovery Team” (DRT) who are responsible for overseeing the implementation of the disaster recovery plan, coordinating recovery efforts, and ensuring communication with all relevant stakeholders.

<u>IT MANAGER:</u>

- Oversees the maintenance and updating of onsite and remote servers, computers and equipment.
- Develops and maintains backup systems and manages data recovery processes.
- Ensures IT resources are available as per the disaster recovery plan.

<u>DATA CUSTODIAN:</u>

- Ensure data is regularly backed up (as relevant per data type)
- Check integrity of backups monthly

EOHWC STAFF:

- Comply with established best practice procedures for long term data security
- Follow disaster recovery plan
- Report any issues to the Disaster Recovery Team

5. IT Best Practices

DATA SAFETY

- No data is to be kept in a computer's storage. All files should be kept and worked on the server. This is to ensure continuity in backups and failsafe for data loss.
- When working in the office, ALWAYS access files via the L Drive (Locally)
- When working remotely, ALWAYS access files through the Synology Drive App
- Important files received via email should be saved to the server
- For complex technical tasks, create documentation so it can be repeatable

CYBER SECURITY

- Do not respond to or open suspicious emails, calls, messages, etc.
    - If something seems strange or out of context, ask a colleague for a reality check
    - The most successful hacking method is SOCIAL ENGINEERING, where a hacker will try to appear relevant to you (spoof supervisor's email, create logical sounding links, etc).
        - Hackers can create IDENTICAL email addresses to someone you know
        - They will often have a couple of glaring issues, like weird links, irrelevant information and typos that will help you spot phishing
- IMMEDIATELY report any strange or suspicious activity to the IT manager
- Passwords should be unique for each service and should be changed regularly
    - Use a password manager, like a Firefox account
- DO NOT plug in any random devices to your computer (external HDD, flash drive, dongles, etc) if you do not know who or where they are from
- NEVER access secured files, documents or accounts while on public Wi-Fi
- Always enable multi-factor authentication when possible

6. Risk Assessment and Impact Analysis

Conduct regular risk assessments to identify potential threats to IT systems and data. Perform a Business Impact Analysis (BIA) to determine the potential impact of disruptions on business operations and identify critical systems and data.

7. Backup and Recovery Procedures

Data Backup: All critical data shall be backed up daily, following the 3-2-1 strategy. (3 Copies of Data, on 2 Different Media Types, with 1 off-site for disaster recovery)

- 3 Total copies of the data at all time
    - 1 Active File maintained and used on the server for daily work function
    - 1 Local Backup File kept on a different piece of media
    - 1 Offsite Cloud Backup File that is always accessible

- As of 8/2024, company files are maintained on a Synology NAS.
    - It utilizes a redundant storage method (RAID 1) to ensure that if one of the two disks die, there is no immediate loss of data
    - The local backup is through an external HDD connected to the NAS
    - Remote backup is through C2 Synology, which is a cloud service

Backup Testing: Backups will be tested monthly to ensure data integrity and successful recovery. This will be best done by spot checking random files from the on-site backup.

1) Pull 5 different files from different folders, from different time periods

ex) 1 file from each of these folders → Projects, FAD Accounting, Meeting Agenda, Meeting Minutes, Installation Agreement

2) Restore files to desktop → check for any issues, corruption, inconsistencies
3) Remove copied files from computer

Data Recovery: In the event of data loss, first the severity of the event will be determined whether it is a single file to recover, a folder, or the whole NAS. Recovery methods are outlined in the HOW TO MAINTAIN THE SERVER documentation guide.

Backups will be checked backwards in time to find the first correct file.

In the event of full system failures, the IT Manager will first assess the extent of data loss and determine the priority of data recovery.

8. Disaster Response Procedures

Initial Response: Assess the situation, determine the extent of damage, and activate the Disaster Recovery Team.

Communication: Notify all affected employees about the disruption and ongoing recovery efforts.

System Restoration: Follow predefined procedures to restore IT systems and data. Use backup data to rebuild or repair affected systems.

Testing and Validation: Once systems are restored, test and validate to ensure they are functioning correctly, and data integrity is maintained.

9. Plan Maintenance

Review and Update: The disaster recovery plan will be reviewed and updated annually or whenever there are significant changes to the IT environment or business processes.

Training and Drills: Conduct regular training sessions and disaster recovery drills to ensure all personnel are familiar with the procedures and can respond effectively.

10. Documentation

Records: Maintain detailed records of all disaster recovery activities, including incidents, response actions, and recovery outcomes.

Plan Documentation: Ensure that the disaster recovery plan is documented, accessible, and understood by all relevant personnel.

11. Compliance

Regulatory Requirements: Ensure compliance with relevant regulatory requirements and industry standards related to data protection and disaster recovery.

12. Policy Review

This policy will be reviewed annually and updated as necessary to reflect changes in the organization's IT environment, business operations, and industry best practices.

Signed:

EAST OF HUDSON WATERSHED CORPORATION

2 Route 164, Suite 2, Patterson, NY 12563
Phone: (845) 319-6349 Fax: (845) 319-6391
eohwc.org

MEMO

To: Board of Directors of the East of Hudson Watershed Corporation

From: Keith Giguere

Date: September 26, 2024

Re: IT Data and Disaster Recovery Policy

The IT Data and Disaster Recovery Policy requires employees to be designated to certain roles to ensure that IT systems and data within the East of Hudson Watershed Corporation are maintained properly. As personnel and responsibilities change, an updated memo will be provided to the Board.

At the current time, Kevin Fitzpatrick will be appointed the responsibilities of the IT Manager and Linda Matera will be appointed the responsibilities of the Data Custodian.