

Backup and Recovery Policy

# Overview/Purpose

**<Utility Name>** is committed to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly, and protecting the Utility's data from alteration or destruction due to equipment failure and other causes. **<Utility Name>**'s intentions for publishing a Backup and Recovery Policy are not to impose restrictions that are contrary to **<Utility Name>**'s established culture of openness, trust and integrity.

The purpose of the Backup Policy is to establish rules and outline the use of media systems and network servers for the storage, backup and recovery of electronic information in **<Utility Name>**'s Information Technology environment. Electronic backups are a business requirement to enable recovery of data and applications in the case of events such as natural disasters, system drive failures, espionage, data entry errors, or systems operations errors.

# Scope

**<Person or group responsible for policy at Utility**> personnel, in coordination with respective departments, are responsible for providing adequate backups to ensure the recovery of data and systems in the event of failure. These backup provisions will allow **<Utility Name>** business processes to be resumed in a reasonable amount of time with minimal loss of data. Since hardware and software failures can take many forms, and may occur over time, multiple generations of data backups should be maintained.  
  
Federal and state regulations pertaining to the long-term retention of data (e.g., financial records) will be met using separate archive policies and procedures, determined by the Department responsible for the information. Backups are not primarily intended to archive data for future reference, but rather for system restoration. Data stored locally on desktop computers is not backed up, nor is data backed on systems that are not managed by **<person or group responsible for policy at Utility>**. Long-term archive requirements are beyond the scope of this policy.

# Policy

**<Utility Name>** requires that computer systems be backed up on a regular basis, with backup media being stored in a secure off-site location. The purpose of the these backups is to provide a means to restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster, to provide a measure of protection against human error or the inadvertent deletion of important files, and to secure data against possible deletion or alteration as part of a security incident. System backups are not intended to serve as an archival copy or to meet records retention requirements.

* + - Data stored on backup media shall be encrypted accordingly to the *Encryption Policy*.
    - The frequency and extent of backups must be appropriate to the importance of the information and the acceptable risk as determined by the **<Utility Name>** department for each data set.
    - **<Utility Name>** Information Technology backup and recovery processes for each system and service should be reviewed annually by the responsible business owner and the **<person or group responsible for policy >** personnel.
    - Backup recovery procedures should be periodically tested to ensure that data is recoverable, and that restored data is identical to what was originally saved.
    - Procedures for the offsite backup storage should be reviewed periodically.
    - Backup media must be readily identified by appropriate labeling, with notes in a centralized log as to physical storage location for each media element.
    - All critical or unique utility information stored locally on workstations must be placed on networked file server drives for backup.

Network storage structure

**<Utility Name>** has network servers in place in **<Identified Locations>.** Managementand staff have file storage folders allocated for their account on network servers. These storage areas are usually referred to as the user's "X: drive", where X denotes a mapped storage area on a network server as described below:

X: Drive - User's personal folder on the network server

When the user successfully logs onto their workstation, network connections are established to these folders which can then be accessed as the "X: Drive" in Windows Explorer, Microsoft Word, Excel, and other software programs. Files can be copied from the user's workstation to their "X Drive", or software programs may be configured to save files directly to these mapped drives. These mapped drives are backed up to removable media. The removable media shall be rotated to an off-site storage facility and securely stored to provide for security and disaster recovery.

*[Explanatory Note: This specific application of a network storage structure from utility to utility will vary. This information is provided only as a guide.]*

## Storage of user data files

In order to be able to recover lost data, management and staff should store essential data files requiring backup, to one of the network mapped drives. Data files on the user's local workstation may not be recoverable if the drive fails. Appropriate use of network storage will ensure ample capacity for archival storage of user data files. Users should store and maintain data files (or current copies) which are important to the company and which would be costly or impossible to recreate, on the network mapped drives. Users should not store non-business or non-essential data files on the network drives. Types of data files to be stored and their locations will be determined on a departmental level, and should be documented in a department level data backup guideline to be communicated with the **<person or group responsible for policy >**.

## Backup Schedule

Systems backups will consist of regular full and incremental backups in accordance with the **<Utility Name>** *Backup Procedure*.

## Documentation

**<Utility Name>** IT backup and recovery processes for each system and service must be documented by the **<person or group responsible for policy >** with assistance from the department for the related system or data set.

* Backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period.
* Documentation of the restoration process must include procedures for the recovery from single-system or application failures as well as a total data center disaster scenario.
* Backup and recovery documentation will be reviewed and updated at least annually to account for new technology, business changes, and migration of applications to alternative platforms. Recovery procedures will be tested on an annual basis, where feasible.

## Backup verification

Test restores from backup archives must be performed at least annually, where feasible. This ensures that both the archive media and backup/restore procedures work properly. It must be proven at least once that complete data restoration is possible. This testing ensures that:

* Data restoration is possible;
* The data backup procedure is practical;
* There is sufficient documentation of the data backup/restore process to allow a person unfamiliar with the procedure to carry out a data restoration, if necessary;
* The time required for the data restoration meets the availability requirements.

## Offsite Storage

In order to provide disaster recovery capabilities, backup media are rotated to an offsite storage location from the backup source. Backup media are maintained in offsite storage according to the schedule outlined in *Backup Schedule Form*.

## File Recovery

In order to have a file restored from a backup, the user should contact **<person or group responsible for policy>,** and provide complete details, including the date of the last known good version of the file – this will help identify the set of backup media to use in attempting to restore the file.

Files can usually be restored within a few hours or less, depending on the time required to obtain media from the offsite storage location. The **<person or group responsible for policy>** cannot restore data files which were not archived on the network servers. Given that backup media is reused, users should request restoration of data files as soon as possible to prevent data being overwritten on the backup media.

## Open Data Files

The creation of accurate backups is not always possible if the files being backed up are open at the time of the backup. As such, users should ensure that all files are closed at the end of their business day. For applications running beyond normal business hours, arrangements should be made with the **<person or group responsible for policy >** to use an alternate approach to obtain backups.

## Backup Failure

All backup failures will be logged and investigated as soon as practical upon detection.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the <**person or group responsible for policy**> in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* Adapted from “Cyber Security Policy Framework”

(<https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx>)   
Cyber Security Policy Framework was created by the Kentucky Association of Electric Cooperatives (KAEC) Information Technology (IT) Association - Cyber Security Subcommittee.

# Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO/GM** | **System Admin**  **Network Admin** | **IT Department** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |