# Disaster Preparedness, Prevention, and Recovery for Electronic Records

## Table of Contents


Core Principles ..... 1
Cyberattack ..... 1
Fire or Extreme Heat ..... 2
Flood or Water Damage ..... 2
Power Surges and Electrical Events ..... 3
Human Error and Internal Failures ..... 4
Technological Obsolescence ..... 5
Conclusion ..... 6
Questions? ..... 6
Resources ..... 6


## Core Principles

Electronic records are essential evidence of government actions. Disasters can threaten legal compliance and retention obligations, public access and transparency, and agency operations and service delivery.

All disaster planning for electronic records should be based on these principles:

- **Records are assets** that require proactive protection
- **Prevention is more effective and less costly than recovery**
- **Redundancy and documentation are critical**
- **Records management and IT must work together**
- **Disaster preparedness is an ongoing process**, not a one-time task

## Cyberattack

**How to Prepare (Before a Cyber Incident)**

- Require use of approved systems for creating and storing electronic records
- Implement role-based access controls and permissions
- Ensure multi-factor authentication is enabled where available
- Maintain offline backups protected from ransomware for vital records
- Provide regular cybersecurity and records management trainings

**How to Respond (During and Immediately After a Cyberattack)**

- Disconnect affected systems from the network, if directed by IT
- Do not delete files, logs, or compromised systems
- Report the incident immediately according to agency procedures
- Suspend routine records disposition and system clean-up activities

**How to Recover (After a Cyberattack)**

- Restore records only from verified, clean backups
- Validate that restored records are complete and accurate
- Coordinate with legal counsel and cybersecurity staff regarding notification requirements
- Document records impacted, lost, or altered
    - If records are lost or altered, report this to the Kentucky Department for Libraries and Archives per KRS 171.720
- Update policies, controls, and trainings based on lessons learned

## Fire or Extreme Heat

**How to Prepare (Before Fire)**

- Maintain regular, automated backups stored off-site or in geographically separate locations
- Document system inventories, including where electronic records are stored
- Ensure records retention schedules are current
- Coordinate with facilities and IT on fire suppression systems and power shutoff procedures

**How to Respond (During and Immediately After a Fire)**

- Prioritize staff safety and follow emergency procedures
- Notify IT, records management staff, and leadership

- Preserve affected systems and devices; do not discard damaged hardware without consultation
- Suspend routine records disposition activities

**How to Recover (After a Fire)**

- Assess which electronic records and systems were impacted
- Restore records from verified backups
- Validate data integrity and completeness after restoration
- Document any permanent losses and actions taken
    - If records are lost or damaged, report this to the Kentucky Department for Libraries and Archives per KRS 171.720
- Review whether storage locations, backup strategies, or system protections need improvement

## Flood or Water Damage

**How to Prepare (Before a Flood)**

- Avoid locating servers, network equipment, or records storage in basements, below water pipes, or flood-prone areas
- Ensure secondary backups are stored off-site and not in the same geographic area
- Monitor humidity and environmental controls where equipment is housed
- Prohibit storing official records solely on portable media (USB drives, external hard drives)

**How to Respond (During and Immediately After a Flood)**

- Ensure staff safety and follow emergency guidance
- Do not power on wet or potentially damaged equipment
- Notify IT, records management, and facilities staff
- Preserve affected devices and storage media for assessment
- Document which systems and records may have been exposed to water or excess humidity

**How to Recover (After a Flood)**

- Coordinate with IT to determine what equipment or systems are salvageable
- Restore records from clean, verified backups

- Check for data corruption or incomplete files
- Document any unrecoverable records and hardware
    - If records are lost or damaged, report this to the Kentucky Department for Libraries and Archives per KRS 171.720
- Reassess physical locations of equipment and storage practices

## Power Surges and Electrical Events

**How to Prepare (Before a Power Surge)**

- Use surge protectors and uninterruptible power supplies (UPS) for servers, network equipment, and workstations that store or process records
- Coordinate with IT to ensure mission-critical systems are on protected power circuits
- Maintain regular, automated backups stored off-site or in the cloud
- Avoid storing records solely on local hard drives or individual workstations

**How to Respond (During and Immediately After a Power Surge)**

- Do not immediately power on systems that shut down unexpectedly
- Notify IT and records management staff as soon as possible
- Document which systems were operating at the time of the surge
- Preserve affected devices for assessment if data corruption is suspected
- Suspend routine records disposition until system integrity is confirmed

**How to Recover (After a Power Surge)**

- Allow IT to assess hardware and system integrity before resuming operations
- Check electronic records for corruption, incomplete files, or altered metadata
- Restore affected records from verified backups if necessary
- Document any data loss, system damage, or recovery actions taken
    - If records are lost or altered, report this to the Kentucky Department for Libraries and Archives per KRS 171.720
- Review power protection measures, replace affected power supplies, and update disaster preparedness plans as needed

# Human Error and Internal Failures

**Common examples include:**

**Accidental deletion or alteration:** Inadvertent deletion of files, overwriting records, or improper handling of data

**Misconfiguration:** Improperly configured systems or servers, such as unsecured cloud storage, incorrect permissions, or disabled logging

**Insider threats:** Carelessness or negligence—such as sending sensitive data to the wrong recipient—often more common than malicious intent

**How to Prepare (Before an Incident Occurs)**

- Require use of approved systems for creating and storing electronic records
- Implement role-based access controls and permissions
- Use system features such as version control, audit logs, and change tracking
- Provide regular training on records management, data handling, and security awareness
- Establish clear procedures for file naming, storage locations, and sharing
- Maintain regular, automated backups that allow recovery from accidental loss

**How to Respond (When Error or Failure Is Discovered)**

- Report the incident promptly according to agency procedures
- Preserve affected records, systems, and logs; do not attempt ad hoc fixes
- Suspend routine records disposition and clean-up activities
- Identify what records were deleted, altered, disclosed, or exposed
- Coordinate with IT, records management, legal counsel, and leadership

**How to Recover (After an Incident)**

- Restore affected records from verified backups or version histories
- Validate restored records for accuracy, completeness, and authenticity
    - If records are irretrievably lost, report this to the Kentucky Department for Libraries and Archives per KRS 171.720
- Assess whether sensitive or protected information was improperly disclosed
- Document the incident, impacts, and corrective actions taken

- Update procedures, permissions, and training to prevent recurrence

## Technological Obsolescence

Technical and technological obsolescence occurs when hardware, software, storage media, or file formats are no longer supported, compatible, or reliable. Unlike sudden disasters, obsolescence is a **gradual but predictable risk** that can silently render electronic records inaccessible, corrupted, or unusable if not actively managed.

**Common forms of obsolescence include:**

- **Hardware and storage failure:** Magnetic tapes, hard drives, and flash drives have a limited lifespan (often 5–10 years) and can fail suddenly without warning
- **File format obsolescence:** Software or operating systems may become obsolete, making older files difficult or impossible to open or read
- **Data degradation ("bit rot"):** Over time, digital media can lose data integrity, resulting in corrupted or incomplete files

**How to Prepare (Before Obsolescence Occurs)**

- Use widely supported, non-proprietary file formats whenever possible
- Store electronic records in managed, centralized systems rather than on removable media
- Maintain an inventory of hardware, storage media, systems, file formats, and dependencies
- Monitor vendor support lifecycles, end-of-life announcements, and media age
- Plan for regular refreshment and migration of records stored on aging media

**How to Respond (When Obsolescence Is Identified)**

- Identify records stored on at-risk hardware, media, systems, or file formats
- Prioritize records with permanent, long-term, or legal value
- Suspend disposition until records accessibility and integrity are confirmed
- Coordinate with IT to evaluate migration, export, normalization, or emulation options

**How to Recover (After Migration or System Change)**

- Migrate records to supported systems or formats that preserve content, metadata, and context
- Validate migrated records for completeness, accuracy, usability, and integrity
- Preserve documentation of what was migrated, when, how, and by whom
- Update inventories, procedures, and retention documentation
- Retire obsolete hardware, media, or systems only after records are verified and accessible
- If records are unable to be accessed and migrated, report this to the Kentucky Department for Libraries and Archives per KRS 171.720

## Conclusion

Effective disaster preparedness for electronic records depends on proactive records management, strong collaboration with IT, and ongoing commitment from leadership. By planning ahead, agencies can protect the integrity, accessibility, and trustworthiness of government records before, during, and after a disaster.

## Questions?

If you have any questions about electronic records management, please contact us at:

Electronic.Records@ky.gov

## Resources

Digital Preservation Coalition. *Digital Preservation Handbook*. 2nd ed., 2015, https://www.dpconline.org/handbook. Accessed 3 Aug. 2026.

National Archives and Records Administration. *Essential Records Guide*. Aug. 2018, https://www.archives.gov/files/records-mgmt/essential-records/essential-records-guide.pdf. Accessed 3 Aug. 2026.

National Archives and Records Administration. *Records Management Guidance*. National Archives and Records Administration, https://www.archives.gov/guidance/records-management-guidance. Accessed 3 Aug. 2026.

National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29, U.S. Department of Commerce, 26 Feb. 2024, https://doi.org/10.6028/NIST.CSWP.29

Swanson, Marianne M., et al. *Contingency Planning Guide for Federal Information Systems*. Rev. 1, National Institute of Standards and Technology, May 2010, https://doi.org/10.6028/NIST.SP.800-34r1