504 Cyber Security Policy

Cass County Public Library is committed to protecting its digital resources, systems, and the privacy of patrons and staff. This Cybersecurity Policy outlines security measures to safeguard information, prevent cyber threats, and ensure compliance with state and federal regulations, including those necessary for federal grant funding.

This policy applies to all employees, contractors, and any individuals who access Cass County Public Library technology resources, including computers, networks, databases, email, voicemail, internet access, and cloud-based services.

Responsibilities for Implementation and Maintenance:

- Library Administration is responsible for implementing and maintaining cybersecurity policies and procedures.
- Technology Coordinator will monitor threats, apply security updates, and provide necessary training.
- Employees must follow security protocols and report potential threats.

Acceptable Use Policy for Patrons:

- Users must follow password security best practices, including creating strong passwords and not sharing login credentials.
- Public access computers will be configured with appropriate security settings and automatically reset between user sessions.
- Unauthorized software or hardware installations on public access computers are prohibited.
- The use of email, voicemail, or the internet in any manner considered disruptive, offensive, illegal, or harmful to Cass County Public Library is prohibited.
- Users must follow the Acceptable Use of Electronic Resources Operations Policy.

Acceptable Use Policy for Employees and Contractors:

- Employees must follow password security best practices, including creating strong passwords and not sharing login credentials.
- Employees must lock or log off their computers when leaving their workstations.
- Employees should have no expectation of privacy regarding Cass County Public Library-owned computers, email, voicemail, internet activity, facility desks, lockers, or other storage devices.

- Cass County Public Library reserves the right to monitor and access employee email, voicemail, and internet usage at its sole discretion to ensure compliance with this policy.
- Unauthorized access to another employee's email or voicemail is prohibited.
- Employees are not allowed to install or delete programs on any Library computer without the permission of the Technology Coordinator.
- The use of email, voicemail, or the internet in any manner considered disruptive, offensive, illegal, or harmful to Cass County public Library is prohibited.

The following provisions apply to all employees.

Data Protection and Confidentiality

- Protection of confidential business information, including employee, patron, and circulation records, is an important aspect of all employee positions.
- Employees must exercise discretion when working with confidential data and must refrain from discussing such information.
- Disclosure of confidential information will be handled solely by Cass County Public Library Director, or their designee, in accordance with Missouri law.
- Any breach in confidentiality may result in disciplinary action, up to and including termination of employment and possible legal action, even if the employee does not personally benefit from the disclosure.

Confidential information includes, but is not limited to:

- Information about the termination of a staff member.
- Patron information, including borrowing records.
- Names, or other identifying details of patrons that identify a person or persons as having requested, used, or borrowed library material, and all other records identifying the names of library users.
- As a member of the Missouri Evergreen Consortium (MEC), whose libraries constitute an interconnected or combined system in order to enable collaboration, Cass County Public Library supports and abides by the Missouri Evergreen Policy on Personally Identifiable Information.

Employees unsure about what constitutes confidential information or an improper disclosure should consult their immediate supervisor, Human Resources, Assistant Director, or Library Director.

The Cass County Public Library network is protected by firewalls, antivirus software, and intrusion detection systems. Regular software updates and security patches will be applied to all library-owned devices. Remote access to Library systems will require authentication and secure connections. Cass County Public Library will maintain internal controls to ensure compliance with federal regulations, including 2CFR.200.303, which

outlines requirements for managing federal awards responsibly. These controls provide reasonable assurance that federal awards are handled in accordance with applicable laws, regulations, and grant conditions.

Incident Response

All security incidents, including data breaches and system intrusions, must be reported to Cass County Public Library Director, the Technology Coordinator, and Human Resources immediately. They will investigate and respond to any suspected intrusion or firewall failure.

- Cass County Public Library will maintain an incident response procedure to investigate and mitigate security incidents.
- Technology Coordinator will document incidents through the Cass County Public Library PITS reporting system and recommend preventive measures.

Cybersecurity Training

- All employees must complete annual cybersecurity training, through computer-based courses and in-person training held by the Technology Coordinator at each branch.
- Technology Coordinator will conduct yearly security awareness programs covering phishing, social engineering, and best practices.

Failure to comply with this policy may result in disciplinary action, including termination for employees and restricted access for patrons. This policy will be reviewed annually and updated as necessary to ensure continued compliance with applicable laws and grant requirements.

Policy References

Acceptable Use of Electronic Resources

Confidential Records

Compliance and Confidentiality

Adopted 3/19/25