**Jackson County Library District**
**Cyber Liability Policy**

**Background:**
The Jackson County Library District ("District") understands that the primary goal in mitigating risk in a digital environment is to safeguard the sensitive data. The data may be operational information, which is necessary for the organization to function; or, it may be library patron or staff data that the organization has a legal responsibility to secure. As set forth below, there are numerous things that must be done to safeguard the data, and the following guide identifies the priorities that will help get it done. Since the District has no employees, the intended audience for this policy are contractors of the Jackson County Library District that create, modify, analyze and distribute sensitive data on behalf of the District and its patrons.

1. **Safeguard the data:**
   a. Identify and empower a key individual(s) to own the responsibility of safeguarding sensitive data.
   b. Identify the data that is being received, transmitted and stored. What type of data - PI, PHI, and/or PCI?
   c. Identify how and where the data is being received or generated (email, cloud services, user devices, etc.). Data should only be received or generated if there is a legitimate business reason to do so.
   d. Identify how and where the data is being stored (network servers, user devices, removable media, cloud services, physical filing systems, etc.). Data should only be stored if there is a legitimate business reason to do so.
   e. Identify how the data is being protected. If it is sensitive data, consider encryption in both transit and at rest.
   f. Identify how and when the data is being disposed. Data should only be kept as long as there is a legitimate business reason to retain it, and it should thereafter be securely shredded or degaussed.

2. **Safeguard the information Systems**
   a. **Identify and empower a key individual(s) to own the responsibility** of safeguarding the information system – it may be the same person(s) responsible for safeguarding the data, but there must be someone empowered and resourced to protect the system.
   b. **Inventory authorized hardware** to help detect unauthorized devices. You have to know your network – know what should be on it - in order to protect it.
   c. **Inventory authorized software** to help detect unauthorized and malicious software. Similar to hardware, you have to know what should be on your network in order to detect and prevent unauthorized software.
   d. **Develop and implement secure configurations for all devices** to reduce the number of vulnerabilities an attacker could exploit.

e. **Continuously monitor for and assess vulnerabilities** and immediately remediate. The digital environment is in a constant state of flux, and the threats continue to change in scope and severity. It is therefore critical that you continuously seek to identify vulnerabilities, and immediately remediate them.

f. **Control use of administrative privileges** to ensure that only those individuals with legitimate occupational need are allowed administrative access to network resources and devices. **Control access based on the need to know** to prevent unauthorized access to the system and data.

g. **Actively monitor and control all active accounts** to minimize authorized access.
   - Review all accounts and disable inactive accounts;
   - Ensure all individual accounts are terminated immediately upon an individual's departure;
   - Ensure all contractor accounts are terminated upon completion of the project;
   - Ensure all service accounts are secured if used or terminated if inactive.

**h. Actively protect all accounts and user devices.**
   - Implement password complexity rules requiring passwords to meet length and strength requirements, including a mix of uppercase and lowercase letters, numbers, and symbols;
   - Require passwords to be changed routinely and kept private;
   - Encrypt devices to protect sensitive data;
   - Require screen locks after short intervals of inactivity.

i. **Implement email and web browser protections** to mitigate the risk that unauthorized users could compromise your system.
   - Use only fully-supported web browsers and email clients in your organization;
   - Use spam filters and firewalls to prevent unwanted, harmful email, and other forms of potentially vulnerable communications.

j. **Use anti-malware software** to prevent malicious programs like ransomware from being entering or being installed in your environment.

k. **Deploy boundary defenses**, including firewalls, to control the flow of traffic and search for evidence of unauthorized access or malicious programs.
   - Create **blacklists** of known malicious IP addresses and deny them access;
   - Create **whitelists** of known, trusted sites that individuals should or need to have access to from organization devices;
   - Use a VPN or other secured means for users to remotely access your organization's network;
   - Require **multi-factor authentication** for all remote access to your organization's network.

l. **Monitor both inbound and outbound traffic**. It is important to not just monitor what is entering your network, but it is increasingly important to monitor what is leaving your network. Unauthorized users often enter through encrypted tunnels, and are not detected until they attempt to leave with sensitive data.

m. **Strengthen the security of your wireless networks** and limit wireless access to your network to authorized devices with a bona fide business need.
   - Scan wireless network for, and disable all, unauthorized wireless access points;
   - Ensure that all wireless traffic is encrypted;
   - Create separate virtual local area networks (VLANs) for "bring your own devices" (BYODs) and other untrusted devices.

n. **Continuously update operating systems and software** to reduce vulnerabilities.

o. **Implement and test data recovery capabilities** to recover critical information in the event of a system failure or attack. It is increasingly important that data backups regularly be tested for integrity to ensure their availability in the event of a system compromise, such as an encryption attack.

p. **Develop and test an incident response plan**. It is essential that all key stakeholders are involved in the planning for the inevitable data security incident. It is also important to "test" the plan through simulated data security events. "Experiencing" a data security event before it actually occurs accelerates an organization's ability to effectively contain and remediate an incident.

q. **Develop and implement a records retention and disposal plan**. Information should only be retained as long as there is a legitimate business need for doing so. It must thereafter be securely disposed.

r. **Educate users on network security awareness and safe data practices**. Users are the "human firewall" and it is critically important to keep them apprised of how they can protect their data and the organization's system.
   - Inform them about the dangers of opening links in email, tweets, posts, online ads, messages or attachments, even if they are from a known source;
   - Inform them about the dangers of using removable media from unknown sources;
   - Inform them about social engineering techniques;
   - Require them to confirm any requests for W-2 information or wire transfers with appropriate organization personnel;
   - Encourage them to report requests for sensitive data, such as passwords or financial information, from new or unexpected sources.

*Adopted: November 9, 2017*