Nebraska K12 Cybersecurity Rubric 2024 v1.0

Instructions	
Evaluate the current state of each domain within your organization based on the descriptions provided for each risk level.	
Assign the appropriate risk level (at risk, baseline, good, better) to each domain based on your assessment.	
Areas for improvement will be available in the Technical Report Tab.	
Use the assessment results to develop a roadmap for enhancing cybersecurity maturity, setting specific goals, timelines, and responsibilities for implementing improvements in each domain.	
Tabs	
Instructions	Instructions
1.0 Sanitize Network Traffic to/from the Internet	Domain 1.0, Sanitize Network Traffic to/from the Internet emphasizes the importance of implementing robust security measures to monitor, analyze, and filter network traffic to safeguard against cyber threats and maintain the integrity and confidentiality of data exchanged over the internet.
2.0 Safeguard Devices	Domain 2.0, Safeguard Devices, focuses on implementing measures to protect and secure individual devices within a network infrastructure. This includes computers, servers, mobile devices, IoT devices, and any other endpoints that connect to the network. The primary objective is to prevent unauthorized access, mitigate potential vulnerabilities, and ensure the integrity and confidentiality of data stored and processed on these devices. Measures may include implementing firewalls, antivirus software, encryption protocols, access controls, regular security updates, and employee awareness training to promote best practices in device security. Overall, this domain emphasizes the importance of securing individual devices as a fundamental component of a comprehensive cybersecurity strategy.
3.0 Protect Identities	Domain 3.0, Protect Identities, focuses on safeguarding user identities and credentials within a network environment. This includes implementing authentication mechanisms, such as multi-factor authentication (MFA), strong password policies, and identity management solutions to prevent unauthorized access and mitigate the risk of identity theft or misuse. The goal is to ensure that only authorized individuals can access resources and sensitive information, thereby enhancing overall cybersecurity posture.
4.0 Practice Continuous Improvement	Domain 4.0, Practice Continuous Improvement, emphasizes the importance of ongoing enhancement and refinement of cybersecurity practices and processes. It involves establishing mechanisms for monitoring, evaluating, and adapting security measures to address evolving threats and vulnerabilities effectively. This domain underscores the need for organizations to adopt a proactive approach to cybersecurity, regularly reviewing and updating policies, conducting security assessments, and investing in training and awareness programs to foster a culture of continuous improvement in cybersecurity practices.

5.0 Communicate and Collaborate	Domain 5.0, Communicate and Collaborate, highlights the significance of effective communication and collaboration within an organization's cybersecurity framework. It emphasizes the importance of facilitating clear and open communication channels among stakeholders, including IT teams, management, employees, and external partners. This domain stresses the need for collaboration to share threat intelligence, coordinate incident response efforts, and align cybersecurity initiatives with business objectives. Effective communication and collaboration enable organizations to respond swiftly and effectively to cybersecurity threats and challenges, enhancing overall resilience and security posture.
Results	
Technical Report	
Submission	