Cybersecurity Functional Annex Checklist

Purpose:

The primary purpose of a Cybersecurity Annex is to establish a standardized, flexible, and scalable foundation to prepare for, and respond to a cyber threat or attack. The identified tasks within this hazard sheet are meant to be a starting point for your planning.

Instructions:

Emergency planning teams should work with their community of responders to identify additional preparedness, response, and recovery tasks that may be applicable.

When completing the Preparedness section, assign a responsible party and document the date/time the action was completed. In the Response and Recovery sections, leave the responsible party and date/time blank until an incident has occurred. At that time, document who completed the task and on what date/time.

Utilize the comments/notes section to input basic information you may need to reference later in the planning, response, or recovery phases.

<table>
<tr><th colspan="5">CYBERSECURITY</th></tr>
<tr><td colspan="5">Cybersecurity is the protection of networks, devices, and data from unauthorized access or criminal use, and the practice of ensuring the confidentiality, integrity, and availability of information. Cyber threats can impact either the human (students, teachers, and staff) or the physical or virtual (e.g., information technology [IT] networks and systems) elements of schools and school districts. Types of threats can include data breach, denial of service, spoofing/phishing, malware/scareware/ransomware, unpatched or outdated software vulnerabilities, or removable media.</td></tr>
<tr><td>DATE</td><td>TIME</td><td>PREPAREDNESS TASKS</td><td>RESPONSIBLE PARTY</td><td>COMMENTS/NOTES</td></tr>
<tr><td></td><td></td><td><b>Leadership Buy-In:</b> Support from leadership is critical for effective security</td><td></td><td></td></tr>
</table>

		measures. Leadership should be involved in the creation and approval of all major components of the district's cybersecurity plan.		
		Understand Risk Profile: Identify what is valuable to the organization and how to protect those assets. In addition, identify and classify different cyberattack scenarios. Review the District's Disaster Recovery and/or Incident Response plans to review prioritized assets. Identify, prioritize, and set a budget for protecting environments.		
		Policy Documentation: Create Policies, Plans, and Agreements. Plan early, plan often. Develop policies and procedures for the protection of networks and systems. As applicable, incorporate or provide links to the district-approved plans for the following items: ● Risk Management Plan, ● Acceptance Use Policy, ● Device Use Policy, ● Disaster Recovery Plan, ● Incident Response Plan, ● Data Privacy Agreement, and		

		● General communication and reporting plans. Maintain all IT security-related plans organized in a network directory that is backed up nightly. Have someone outside of the IT Department review plans and take note of any confusion or questions. Keep things in simple terms that non-IT leaders and users can understand.		
		Training & Education: Awareness of security policies is paramount, especially training for those who deal with the most sensitive organization data. Develop a yearly training calendar for all staff on policies and procedures, as well as how to identify potential threats or attacks. Maintain a record of when the training was completed for each employee.		
		Employee Screening: Remember that people are often the weakest link in any security chain. Create a list of individuals who have authority to use the network and establish a regular schedule for review of the list. In addition, provide a "Responsible Use Policy" that all employees will sign for acceptance.		
		Offline Critical Data Backup: A copy of critical data in a secure off-site location is		

		one small step that should not be overlooked. Establish specific procedures to store data securely off-site and a schedule for backing up data.		
		Incident Reporting System: An incident reporting system tracks such things as data breaches, unauthorized access, and other types of information technology events that occur at an organization. Establish specific procedures for staff to follow to report a cybersecurity concern or incident.		
		Redundancy of Communication: Consider and implement procedures to communicate for when systems are down. Alternate communication methods for personnel should be stored off the network.		
		Patch Management: Ensure that patch Management/Security Updates for all devices have a defined process and a defined schedule. Use your device management systems to enforce written policies, centralize control, simplify administration, and support tracking and reporting. Include and extend practices to include: 1) inventory management, 2)		

		device-level protections, and 3) device sustainability.		
		Conduct Regular Self Reviews: Perform on-going internal vulnerability assessments and conduct on-going penetration testing (pen testing). Additionally, periodic testing should be performed by a trusted outside entity.		

DATE	TIME	RESPONSE TASKS	RESPONSIBLE PARTY	
		Internal Communication: If a cybersecurity threat or incident is suspect, notify IT designated contacts immediately. In addition, school administration should brief the director of schools.		
		Survey the Damage: Perform an internal investigation to determine the impact, identify the attacker, discover the vulnerability, and determine improvements. IT should identify the type of cybersecurity incident and notify the		

		school administration of mitigating actions that should be followed.		
		Limit Additional Damage: Strategies include re-routing network traffic, filtering/blocking traffic, and isolating all or parts of the compromised network.		
		Notify those Affected: When a breach puts an individual's data at risk, identify affected parties and follow the incident response communication plan for notifying those individuals.		
		Engage Law Enforcement: Notify law enforcement of the incident. Agencies to contact include the FBI, Secret Service, ICE, local district attorney, and state/local law enforcement.		
		Consider Notification Obligations: Depending on the significance of the incident you may need to notify the Department of IT.		
		Proactive Monitoring: Thoroughly check all monitoring systems for accuracy to ensure a comprehensive understanding of the threat.		

DATE	TIME	RECOVERY TASKS	RESPONSIBLE PARTY	

		Record Details: Log actions taken to respond to the breach, including affected systems, compromised accounts, disrupted services, affected data/networks, and amount/type of damage.		
		Network Monitoring: Conduct post-breach review of networks for any abnormal activity and verify intruders have been inhibited thoroughly.		
		Conduct Post-Incident Review: Perform a review to identify planning shortfalls and evaluate the execution of the incident response plan Develop processes to learn from a breach, such as document mistakes, assess how mistakes could have been avoided, and ensure training programs include lessons learned. Identify areas of improvement for protective and mitigating measures. In addition, update policies and procedures to reflect improvements. Train staff on any changes to policies and procedures. Provide school and district administration with a final report with the cause of the cybersecurity incident.		