VERMONT
AGENCY OF EDUCATION

1 National Life Drive, Davis 5, Montpelier, VT 05620-2501
(p) 802-828-1130 | (f) 802-828-6430 | education.vermont.gov

Cybersecurity Breach Planning Rubric

The Cybersecurity Breach Planning Rubric can be used as a self-assessment to identify areas of strength as well as those that require additional work. Information gathered from completing this self-assessment may be used as building blocks for a data breach response plan. The quality criteria are taken from the US Department of Education's Privacy Technical Assistance Center's "Data Breach Response Checklist" and from the National Institute of Standards and Technology's Cybersecurity Framework (CSF). For more information, see the AOE companion document School Cybersecurity.

What do we already have in place? What is our evidence?	Quality Criteria	What will we focus on in the coming year? What evidence will we collect?
	1. Establish and implement a written data breach response policy. Activities in this quality address the IDENTIFY function in the NIST CSF. The key steps are: • incorporating applicable breach notification legal requirements; • addressing data breach response strategy, goals, and requirements; • specifying incident handling procedures, strategy for deciding on the course of action in a given situation, and procedures for communicating with organizational leadership and outside parties/law enforcement; • establishing employee expectations in conjunction with Human Resources (HR) policy and/or employee agreements; • identifying the incident response team; • conducting regular reviews of the policy to include any necessary improvements and ensure	

Contact Information:

If you have questions about this document or would like additional information, please contact:
Lisa Helme, Student Pathways Division at lisa.helme@vermont.gov or (802) 828-6956.

What do we already have in place? What is our evidence?	Quality Criteria	What will we focus on in the coming year? What evidence will we collect?
	that it reflects up-to-date federal, State, and local requirements; • identifying a team manager who will be in charge of the incident response with at least one other person designated to assume authority in the absence of the manager; and • assigning and establishing team roles and responsibilities, along with specifying access credentials.	

What do we already have in place? What is our evidence?	Quality Criteria	What will we focus on in the coming year? What evidence will we collect?
	2. Review your information system(s) and data and identify where Personally Identifiable Information (PII) and other sensitive information resides. NIST CSF functions are capitalized by each bullet. This can be done by: • documenting what PII and other sensitive information is maintained by your organization, where it is stored (including backup storage and archived data), and how it is kept secure; (IDENTIFY) • conducting regular risk assessments and evaluating privacy threats for your organization, as well as any contractors, vendors, and other business partners; (RESPOND)	

What do we already have in place? What is our evidence?	Quality Criteria	What will we focus on in the coming year? What evidence will we collect?
	• reviewing who is approved for access to PII and/or other sensitive information and checking user activity status to determine which accounts should be deactivated after a pre-determined period of inactivity; (PROTECT) • reviewing separation of duties to help ensure integrity of security checks and balances; (PROTECT) • implementing mitigation controls designed to prevent and detect unauthorized access, theft, or misuse of PII and/or other sensitive data; (DETECT) • implementing security controls, where feasible, such as encryption of sensitive data in motion and at rest; (PROTECT) and • regularly reviewing and keeping up-to-date your data destruction policies, to minimize the risk of data breaches through unauthorized access to archived media or computers that are no longer in use. (PROTECT)	

What do we already have in place? What is our evidence?	Quality Criteria	What will we focus on in the coming year? What evidence will we collect?
	3. Continuously monitor for PII and other sensitive data leakage and loss. NIST CSF functions are capitalized by each bullet. This includes: • employing automated tools like Intrusion Detection and Prevention Systems[1], next generation firewalls, and anti-virus and anti-malware tools, to monitor and alert about suspicious or anomalous activity; (DETECT) • using data loss prevention[2] solutions to track the movement and use of information within your system, to detect and prevent the unintentional disclosure of PII and/or other sensitive data, for both data at rest and data in motion; (DETECT) • conducting regular searches of the information system and physical storage areas to identify PII that may be outside of approved areas. For example, scan your network for policy violations or occasionally walk through areas for PII left unattended on desks; (PROTECT) • conducting internet searches to locate (and, whenever possible, remove) information that is already in the public domain or visible to the public; (DETECT) and • periodically testing and checking privacy and information security controls through the use of “real-life” exercises to validate their effectiveness as part of a risk management program. (RESPOND)	

What do we already have in place? What is our evidence?	Quality Criteria	What will we focus on in the coming year? What evidence will we collect?
	4. Conduct frequent privacy and security awareness trainings as part of an on-going training and awareness program. Activities in this quality address the PROTECT function in the NIST CSF. This includes: • providing mandatory privacy and information security training on a recurring basis to all employees, school officials, contractors, and any other staff involved in data-related activities; • posting and communicating privacy policies to customers and users (for instance, on the agency web page or on a bulletin board at the office, through statements inserted in documents or emails, etc.); and • clearly defining and making easily accessible processes for reporting privacy incidents and complaints. Depending on the nature of the event, this may include reporting to the authorities, public, and/or individuals affected.	

Resources

Below is a list of organizations and resources on cybersecurity.

Council for School Networking (CoSN): CoSN is a professional association for school system technology leaders. CoSN offers a cybersecurity toolkit to help schools assess their risk and a planning rubric to provide guidance in school planning efforts.

Cybersecurity & Infrastructure Security Agency (CISA): CISA leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. CISA has a page of free cybersecurity services and tools.

Multi State Information Sharing and Analysis Center (MS-ISAC): The mission of the MS- ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery. Membership is free to school districts. MS-ISAC offers network vulnerability assessments, cyberthreat alerts and other related services. As of March, 2022, 24 Vermont school districts were members. Free Tabletop Exercises.

National Cybersecurity Center of Excellence (NCCoE): The center is part of the Applied Cybersecurity Division of NIST's Information Technology Laboratory. NCCoE brings together private industry, government agencies, and academia to create practical, standards-based solution. The center website features a security guidance section with information based on specific technology, sector, and status use.

National Institute of Standards and Technology (NIST): NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, April 25, 2019. Other resources include NIST publications. "Zero Trust Architecture."

SchoolSafety.gov: U.S. government collaborative of federal school safety resources, including cybersecurity resources.

U.S. Department of Education (US DOE): The department administers and enforces student privacy laws such as the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA). In addition, the US DOE provides technical assistance to help schools and school districts safeguard information about students through the Privacy Technical Assistance Center.

[1] Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents. (NIST, Computer Security Resource Center glossary)

[2] A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of National Security System (NSS) information. (NIST, Computer Security Resource Center glossary)