CYBERSECURITY MANAGEMENT AND PLANNING

Policy 774

Sample Policy 2

{This sample policy assigns primary administrative responsibility for various cybersecurity-related duties to a designated staff member. Chief among those responsibilities is the duty to develop and maintain a district cybersecurity plan. This sample establishes an approach to cybersecurity management that draws from two key resources:

- ***The Cybersecurity Framework (CSF), version 2.0, which is published and maintained by National Institute of Standards and Technology within the U.S. Department of Commerce. The abstract to the framework indicates that the CSF offers a "taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks … to better understand, assess, prioritize, and communicate its cybersecurity efforts." The taxonomy is organized around six core functions: (1) govern, (2) identify, (3) protect, (4) detect, (5) respond, and (6) recover.***

- ***The Cybersecurity Performance Goals (CPGs) published and maintained by the Cybersecurity and Infrastructure Security Agency (CISA). According to CISA, "By implementing these CPGs, organizations can undertake prioritized and targeted investment to address the most significant cybersecurity risks. Each CPG was selected to (1) significantly and directly reduce the risk or impact caused by commonly observed, cross-sector threats and adversary tactics, techniques, and procedures; (2) be clear, actionable, and easily definable; and (3) be reasonably straightforward and not cost-prohibitive for even small and medium-sized entities to successfully implement. In addition, the CPGs are accompanied by a CPGs Checklist that allows organizations to prioritize their utilization of each goal based upon cost, complexity, and impact, making the CPGs uniquely useful for organizations with limited resources. To start, school districts should prioritize high-impact, low-cost CPGs." See "Protecting Our Future: Partnering To Safeguard K–12 Organizations From Cybersecurity Threats," CISA, U.S. Dept. of Homeland Security (Jan. 2023) at 15. See also the CISA resources for schools found at https://www.cisa.gov/K12Cybersecurity, https://www.cisa.gov/cyber-hygiene-services and https://www.cisa.gov/protecting-our-future-cybersecurity-k-12***

IMPORTANT: The commitment to create and maintain the district cybersecurity plan envisioned by this sample is a significant commitment. Compared to PRG 774 Sample Policy 1, this sample offers only a general outline for the local cybersecurity management plan that is envisioned by the board. For example, unlike 774 Sample Policy 1, this sample does not identify specific cybersecurity measures/practices or specific goals/initiatives that the board requires the plan to expressly address and monitor. However, both samples share the same fundamental approach to cybersecurity management and accountability.

The actual sample policy begins on the next page.}

The School Board directs the creation, implementation, monitoring, and periodic updating of a District plan ("Plan") concerning the identification, prevention, detection, and response to cybersecurity threats and any actual cybersecurity incidents affecting the District. The Plan shall be consistent with this policy, which is focused on (1) fostering continuous improvement in the area cybersecurity; (2) identifying and using benchmark-informed and risk-informed practices; and (3) establishing evaluation and accountability mechanisms in the area of cybersecurity management.

Key Administrative Responsibilities

The Director of Technology shall have primary administrative responsibility for the District's cybersecurity Plan, including all of the following:

1. Establishing an initial version of the Plan by no later than August 3, 2026.

2. Notifying the Board of substantive updates/modifications to the Plan and presenting the plan.

3. Providing recommendations to the regarding funding in the District's annual budgets and regarding other resources that are identified as necessary for the District to be able to maintain current cybersecurity measures, implement additional near-term priority items, and make progress on longer-term initiatives and goals. The Board acknowledges that resource limitations can affect the District's ability to make desired progress toward achieving specific cybersecurity priorities and goals.

4. Participating in the District's periodic evaluation of cybersecurity insurance options that may be available to the District and offering relevant recommendations.

Expectations for the District Cybersecurity Plan

The Board expects the District's cybersecurity Plan to:

1. In all iterations, address significant cybersecurity risks in a risk-informed manner that considers the goals, measures, and strategies set forth in the following:

    a. The Cybersecurity Framework (CSF) published and maintained by the National Institute of Standards and Technology (NIST), using version 2.0 or later. The Plan shall address each of the core functions of the framework.

    b. The Cross-Sector Cybersecurity Performance Goals (CPGs) published and maintained by the federal Cybersecurity and Infrastructure Security Agency (CISA).

2. Prioritize the timely near-term implementation and/or ongoing monitoring and enhancement of cybersecurity measures that are considered to be high-impact measures relative to the applicable resource requirements (i.e., not cost-prohibitive), as validated within the NIST Cybersecurity Framework, the CISA Cybersecurity Performance Goals, and/or other expert resources. Such measures should address the key cybersecurity functions of identifying threats and vulnerabilities, protecting against threats and vulnerabilities (i.e., incident prevention), incident detection, and incident mitigation (i.e., response and recovery).

3. Include, as soon as reasonably practicable, cyber incident response procedures, initially prioritizing response procedures that address at least (1) data breaches, (2) ransomware attacks, and (3) loss of access to operationally critical systems. ***{Editor's Note: The three types of incidents that are given express priority in this item may be modified at district discretion.}***

4. Identify additional cybersecurity measures that, even if not currently in place or planned for imminent implementation, the District should pursue during a *["1-year to 3-year"]* time horizon. The Plan shall track the District's current status and future progress with respect to such measures, including identifying any evaluation, planning, or implementation steps that are being taken, as well as any barriers that may be inhibiting or preventing progress.

5. Identify longer-term goals and initiatives that will enhance the District's position with respect to cybersecurity management and cybersecurity practices. The Plan shall track the District's current status and future progress with respect to such longer-term goals and initiatives.

6. Continuously evolve over time to increase the Plan's alignment with relevant portions of the NIST Cybersecurity Framework and the CISA Cybersecurity Performance Goals.

To summarize, the Board's expectation is that, under a locally-driven Plan, the administration will operationalize the management of the District's approach to cybersecurity in a manner that (1) identifies, prioritizes, and invests in the near-term implementation, monitoring, and enhancement of the most impactful cybersecurity measures, within applicable resource constraints; and (2) builds, over time, to demonstrate an increasingly more sophisticated, comprehensive, integrated, and effective strategic approach to cybersecurity management.

Legal References:

Wisconsin Statutes

Section 19.65	[mandate to establish rules of conduct and training for employees involved in the management of personally identifiable information]
Section 134.98	[a state "data breach" statute that requires certain covered entities to provide notice of unauthorized acquisition of certain personal information] ***{Editor's Note: There is some arguable ambiguity as to whether section 134.98 applies directly to school districts.}***

Federal Laws

34 C.F.R. Part 99	[regulations implementing the Family Educational Rights and Privacy Act (FERPA), including the expectation found in 34 C.F.R. §99.31(a)(1)(ii) that schools must use reasonable methods (e.g., physical controls, technological controls, and/or administrative policies) to ensure that school officials obtain access to only those education records in which they have legitimate educational interests]
34 C.F.R. §300.623	[confidentiality safeguards regarding IDEA-related records]

Other Federal Resources

- The Cybersecurity Framework (CSF), version 2.0 (released Feb. 2024), as published and maintained by National Institute of Standards and Technology

- Cybersecurity Performance Goals (CPGs), as published and maintained by the Cybersecurity and Infrastructure Security Agency (CISA)
- Other CISA resources, including those created pursuant to the K-12 Cybersecurity Act of 2021, Public Law 117–47, codified in part in a note added to 6 U.S.C. § 652

Cross References:

[Insert appropriate cross references to the policy as applicable to your district.]

Adoption Date:

