DISTRICT OFFICES
Tom Flanagan, Superintendent
150 Colchester Avenue
Burlington, VT 05401
802-865-5332
tflanagan@bsdvt.org

BURLINGTON SCHOOL DISTRICT PROCEDURE

PROCEDURE CODE EP14: CYBERSECURITY

Summary

BSD's Cybersecurity Procedure outlines best practices aligning with the NIST Cybersecurity Framework and the K12 Six Security Information Exchange. The components of these frameworks provide the necessary guidelines for BSD to offer continuity of IT services that are critical to its educational mission.

These practices include how to best identify and categorize critical assets and services, how to protect those assets and services, methods to detect inappropriate events, ways to respond to, mitigate and manage events or attacks, and how to better prepare for the future following an incident, should one occur.

In the event of a major event or breach, the District's Incident Response Plan must be followed to ensure an appropriate response and recovery.

Best Practices

Our cybersecurity best practices use four components:

1. The NIST Cybersecurity Framework: A comprehensive list of controls, from the National Institute of Science and Technology that is specifically designed for cybersecurity. It is the foundation of this procedure.
2. The K12-SIX Runbook: A subset of the NIST Framework that is specific to K-12 schools.
3. A self-evaluation of existing BSD cybersecurity practices: Shows alignment with the NIST Framework.
4. An independent cybersecurity evaluation from the Leahy Center for Digital Forensics and Cybersecurity: This evaluation shows where BSD aligns with the NIST Framework and where adjustments are needed to achieve alignment. Feedback on known vulnerabilities was also provided.

A summary of each major NIST category is shown below. Detailed information about how BSD is meeting best practices for each category can be found in BSD's Cybersecurity Procedure-Detailed Components document (for internal use only).

NIST Categories

1. **Identify**
    a. The purpose of this category is to determine which BSD assets to secure and protect from a cybersecurity perspective. Each asset has a place and hierarchy in the organization's mission. Knowing the assets and understanding how the systems work together provides a clear picture of what needs to be protected and in what order of precedence.

b. Risk assessment and risk management decisions need to be applied to existing BSD assets. It is also extremely important to take equal care and assessment when new assets are added to the system.
c. The District must also know, or seek legal guidance on any legal or regulatory requirements on any cybersecurity-related assets that fall under the District's responsibility.

2. **Protect**
   a. The protection component defines what we are doing to defend the District's cybersecurity assets once they are identified properly. This is a critical category. Every step taken at this stage improves the District's cybersecurity defenses. The goal is prevention. Adherence to best practices in this category will help the District avoid incidents. Best practices for protection include:
      i. Defining measurable responsibilities for managing accounts and devices, ensuring proper access to resources, and auditing related processes to prevent unauthorized activity.
      ii. Providing training and awareness for staff, especially for those working with sensitive data.
      iii. Managing and securing the District's sensitive data.
      iv. Documenting and regularly reviewing security policies and processes.
      v. Maintaining and updating systems routinely; removing unsupported systems from service.
      vi. Evaluating security options annually to ensure the systems are modern, effective, and meeting the District's needs.
3. **Detect**
   a. The purpose of this category is to ensure the District has systems and personnel that can effectively monitor for anomalies. Indicators must be defined for the various systems and processes, i.e. determining what constitutes normal versus abnormal activity.
   b. Once the indicators have been defined, notifications must occur and unusual activity investigated.
   c. An important component of the detection process is internally testing the existing protection measures to ensure their validity.
4. **Respond**
   a. There may come a time when the District suffers a cyber attack or data breach despite its best efforts. At that time, the District needs to be prepared to respond appropriately. This requires response planning and procedures, controlled communications internally and externally, thorough analysis, documented mitigation and improvements to prevent future occurrences.
   b. A cybersecurity incident is a complicated and fluid situation. As such, there is a specialized document that is used for such an event: The Incident Response Plan. (That document is included below.)
5. **Recover**
   a. Following an effective response to an incident, systems need to be restored safely once the event is mitigated.
   b. Lessons learned are incorporated into improved processes and protective measures.
   c. Communication with internal and external stakeholders is a necessity to bring closure to the situation and a return to a sense of normalcy. Sharing of knowledge and experience with other organizations helps everyone improve their cybersecurity posture.

Annual Review

This procedure and the Incident Response Plan should be reviewed by BSD Network Administrators and the Incident Response Manager annually (at a minimum). If there is a significant change in systems, processes, or personnel, a more immediate review would be warranted.

Staff Training

All BSD employees should have a basic understanding of cybersecurity best practices. A minimum level of training is supplied annually by Human Resources via BSD's online training system: Vector.

A more comprehensive training should be provided to employees who are more involved in working with sensitive data and systems, including those working in Information Technology, Technology Integration, Human Resources, Data, Special Education, and the Business Office.

Additional training should not be limited to specific departments. Any additional training by employees improves the District's cybersecurity posture.

Incident Response Plan

The purpose of the Incident Response Plan is to establish a clear and structured framework for BSD to respond effectively to cybersecurity incidents, including data breaches. This plan aims to minimize the impact of data breaches, protect sensitive data, and restore normal operations as quickly as possible. It is aligned with the five key functions of the NIST Framework: Identify, Protect, Detect, Respond, and Recover. These five widely understood terms, when considered together, provide a comprehensive view of the lifecycle for managing cybersecurity risk over time.

This Incident Response Plan outlines the processes BSD uses to detect and respond to unauthorized access or disclosure of private information from systems utilized, housed, maintained, or serviced by BSD. Specifically, it defines the roles and responsibilities of various BSD staff with respect to the identification, isolation, and repair of data security breaches, outlines the timing, direction, and general content of communications among affected stakeholders and defines the different documents that will be required during various steps of the response.

1. **Incident Response Team**
    a. Designate an incident response team consisting of individuals with the necessary expertise and authority to handle data breach incidents.
    b. Define the roles and responsibilities of team members, including incident coordinator, technical experts, legal counsel, communication liaison, and system administrators.

BSD Incident Response Team	
Role	**Responsibility**
Incident Manager, Tech Manager	• Lead incident response plan for team
Network Administrators IT Staff Member(s)	• May receive initial reports of possible incidents if generated during school day; responsible for contacting Incident Manager/Tech Manager immediately • Perform response tasks designated by the Incident Manager
Superintendent of Schools	• Lead decision-making efforts related to impacts of cyber incident and District needs (i.e school closure)
Executive Director of Finance and Operations	• Contact Cyber Insurance policyholder (Liberty Mutual) and report incident per policy guidelines • Contact financial institutions and related services, if and when necessary
District Communication Specialist	• Communicate with staff, community, external stakeholders, and press
District Safety Team Lead	• Impart Cybersecurity Procedures to Safety Team • Collaborate with Communication Specialist to provide relevant incident updates and processes
Vermont (NE Region1) Contact	• Provide coordination and support in times of cyber threat, disruption, or attack
Cyber Liability Insurance	• Provide necessary steps for BSD to file claim and receive policy benefits
BSD Attorneys	• Provide legal counsel
Local Law Enforcement	• Provide relevant cyber and investigative support

2. **Preparation Phase**
    a. Conduct a risk assessment to identify potential vulnerabilities and prioritize security measures, particularly focusing on data protection (aligned with NIST SP 800-30).
        i. Conducted by Leahy Center Assessment Team May-June 2023. Findings provided September 2023.
    b. Implement robust security controls, such as encryption, access controls, and data loss prevention mechanisms, to safeguard sensitive data (aligned with NIST SP 800-53).
        i. BSD currently uses the following to mitigate cyber security risk: pfSense application and network firewall, web filtering to reduce exposure to websites posing a security risk, redundancy of server application nodes, activity, and intrusion logs, daily backups for disaster recovery, anti-spam/anti-phishing through our email provider, deploying up-to-date patches for all systems and current anti-virus software on district computers.
        ii. Since June 2022, BSD has maintained a subscription with The Education Cooperative for the purpose of securing student data privacy agreements with educational technology vendors who have access to student data.
        iii. BSD implements practices designed to proactively reduce the risk of unauthorized access or disclosure, such as training staff with respect to legal compliance requirements (FERPA compliance), following appropriate physical security and environmental controls for technical infrastructure and deploying digital security measures such as firewalls, malware detection, and numerous other industry-standard systems.
    c. Develop and implement an ongoing training program to educate staff and students about data protection best practices, including handling personal information and detecting and reporting data breaches.
        i. BSD staff are assigned an annual cybersecurity training module to complete at the beginning of each school year.
        ii. Teachers and applicable staff continue to receive annual FERPA, Confidentiality and Acceptable Use Training.
        iii. Building Principals have access to appropriate steps to report a potential incident via the BSD Emergency Procedures Manual.
        iv. All BSD Staff will be made aware of the BSD Data Incident Response Plan and the individual responsibility to report a suspected data breach:
            1. Contact the BSD HelpDesk at (802-) 864-8437 and leave a message if it is not answered. The voicemail triggers contact to the whole IT Team.
3. **Detection and Analysis**
    a. Establish real-time monitoring and alerting systems to detect data breaches promptly.
    b. Train the incident response team to recognize signs of a data breach, including unauthorized access, data exfiltration, and abnormal data activity.
4. **Response**
    a. Isolate affected systems and networks to prevent further unauthorized access or data exfiltration.
    b. Implement incident-specific response procedures, including:
        i. Activating an incident response team to coordinate the response efforts and execute the data breach response plan.
        ii. Engaging forensic experts to investigate the root cause, identify vulnerabilities, and provide recommendations for remediation.
        iii. Collecting and preserving evidence related to the data breach for potential legal proceedings.
        iv. Notifying appropriate internal stakeholders, such as senior management and legal counsel, regarding the data breach.

v. Complying with applicable legal and regulatory requirements, such as data breach notification laws.
vi. Implementing containment measures, such as disabling compromised accounts, blocking unauthorized access, and patching vulnerabilities.
vii. Collaborating with law enforcement agencies, if necessary, to investigate the breach.
viii. Assessing the extent of the breach and determining the affected data, individuals, and systemizing the responsible parties.

5. Communication

a. Establish a clear communication plan to notify affected individuals, regulatory authorities, and other relevant stakeholders about the data breach.
b. Designate a communication liaison within the incident response team to coordinate messaging and ensure accurate and timely information is shared.
c. Provide regular updates on the response efforts, mitigation measures, and actions taken to prevent future breaches.
d. Initial communication to affected stakeholders should occur expeditiously upon the identification of the incident. In some cases, this may include an initial communication (letter, email, phone call) that simply states that BSD is aware of the issue and is addressing it, with the promise of a follow-up.
e. Scenarios for the release of Personally Identifiable Information (PII) are as follows:
    i. Should the unauthorized release of student data occur, the District shall notify the legal guardian (or eligible students) affected by the release in the most expedient way possible.
    ii. Should the unauthorized release of protected staff data occur, the District shall notify the staff members affected by the release in the most expedient way possible.
f. Updated communications will come from the Superintendent's Office and Communication Specialist. If staff receive requests for information, they should transfer those requests to the Communication Specialist.
g. District staff should be clearly informed of what information is public and what is internal/confidential. District leadership should be aware that any material or information communicated to staff can and likely will be shared with the public, including the news media.
h. If the breach represents a threat to affected individuals' identity security, consider providing credit monitoring or identity theft protection services to mitigate the risk of negative consequences for those affected.
i. Prepare resources, such as frequently asked questions (FAQs) documents and guidance, to assist affected individuals in understanding the breach and mitigating potential harm.

6. Recovery and Lessons Learned

a. Restore affected systems and networks to a secure state, ensuring vulnerabilities are addressed and proper security controls are in place (aligned with NIST SP 800-61).
b. Conduct a thorough post-incident analysis to identify the root cause and vulnerabilities.
c. After the conclusion of the incident, the team will meet to discuss the event in detail, review response procedures, and execute a formal after-action review to prevent a recurrence of that incident or similar incidents.
    i. The Incident Response Team will use *Sample Learning and Improvement Questions* from the K12 Six Cyber Incident Response Runbook to guide A*fter Action Review and Incident Report Compilation*.
    ii. The compiled Incident Report will serve as a guide for this meeting. In the meeting, a full debrief of the incident will be presented and the findings discussed. The Incident Response Manager will share the full scope of the breach as comprehensively as possible including causes of the breach, how it was discovered, potential vulnerabilities that still exist, communication gaps, technical and procedural recommendations and the overall effectiveness of the response plan.

iii. As a whole, the group will review the information presented and will determine any weakness in the process and determine the appropriate actions moving forward to modify the plan, address any vulnerabilities and update communication to stakeholders.

d. Update security policies and procedures based on lessons learned from the incident and the post-incident analysis (aligned with NIST SP 800-61).
e. Update training and awareness programs to reinforce cybersecurity practices among staff and students.
f. Document the incident response process, including actions taken and outcomes, for future reference and continuous improvement.

7. Plan Testing and Maintenance

a. Regularly test the incident response plan through tabletop exercises and simulated scenarios to evaluate its effectiveness and identify areas of improvement (aligned with NIST SP 800-84).
b. BSD IT and Incident Response Team will participate in an annual tabletop exercise to review the Data Breach Response Checklist and Procedures and make necessary adjustments.
c. Review and update the plan periodically to incorporate changes in technology, threats and organizational structure.
d. Ensure all relevant stakeholders are aware of the plan and their roles in responding to cybersecurity events or incidents.

Clerical Information

BSD Version:	*BSD E14 Procedure*
Date Adopted:	*11/19/24*
Legal Reference(s):	*N/A*
Policy Reference:	*E14: Building and Grounds Security*