



SECURITY PLAN

 High School

December 15, 2021

Table of Contents

Identification.....	2
Protecting Assets	15
Detecting Anomalies.....	20
Respond to Incidents	23
APPENDIX A – REFERENCES	26
APPENDIX B – IT ASSET INVENTORY DETAIL	31
APPENDIX C – CYBER-RELATED DISTRICT POLICIES	38
APPENDIX D – APPROVED SUPPLIERS	68

Tables List

<i>Table 1. Software and applications in use October 2021.</i>	<i>3</i>
<i>Table 2. Vulnerability assessment criteria.</i>	<i>8</i>
<i>Table 3. Sample vulnerability log.....</i>	<i>9</i>
<i>Table 4. Sample threat event log.....</i>	<i>10</i>
<i>Table 5. Probability rating table. NOTE: Adapted from Guide for Conducting Risk Assessments, U.S. Dept. of Commerce, 2012.....</i>	<i>11</i>
<i>Table 6. Probability rating table. NOTE: Adapted from Guide for Conducting Risk Assessments, U.S. Dept. of Commerce, 2012.....</i>	<i>12</i>
<i>Table 7. Risk analysis example.....</i>	<i>12</i>
<i>Table 8. Risk register example.</i>	<i>13</i>
<i>Table 9. Sensitivity and criticality classification descriptions.....</i>	<i>15</i>
<i>Table 10. Allocation of critical assets according to sensitivity classification.</i>	<i>16</i>
<i>Table 11. Metric reporting schedule.....</i>	<i>22</i>

Figures List

<i>Figure 1. BadgerNet data flow diagram.</i>	<i>3</i>
--	----------

Identification

The first step to any cybersecurity plan involves understanding what assets are affected from an IT security perspective. Besides physical assets, the business environment needs to be taken into consideration. It also includes knowing where the organization stands in terms of governance, threats and vulnerabilities, risk management, and supply chain strategy.

1.1. Asset Identification

Assets include the physical devices, systems, software platforms and applications, communications, data flows, external information systems, high priority security resources, and the security roles and responsibilities that enable ██████████ High School to achieve its business purposes.

1.1.1. Devices and Systems

- Smart boards
- Desktop computers (110)
- Laptops (9)
- Chromebooks (500)
- Servers
- Wireless access points (43)
- Surveillance cameras
- Printers/Scanners
- Security camera system
- Attendance system
- Grading system
- Internet service
- Email system
- HR & Payroll Services

1.1.2. Software Platforms, Applications, and External Systems

There are many different software and applications used within the environment. Below is a table of those that are used widespread throughout the high school. Online applications are considered external systems. Review [Appendix B](#) for detailed information regarding each asset.

Software or Application	<u>Installed</u>	<u>Users</u>
	Local (L) or Web-based (W)	Faculty (F); Admin (A); Students (S); Parents (P)
<i>Security camera software</i>	L	A
<i>Office Suite</i>	W	F A S
<i>Skyward HR</i>	W	F A
<i>Adobe Creative Suite</i>	W	F S
<i>Google Classroom</i>	W	F
<i>Xello for Teachers</i>	W	F
<i>Online textbooks & tools (various companies)</i>	W	F S
<i>Class Registration & Attendance</i>	W	F A S P

Software or Application	Installed	Users
	Local (L) or Web-based (W)	Faculty (F); Admin (A); Students (S); Parents (P)
<i>PowerTeacher (Grading & Testing)</i>	W	F A S P
<i>Pride Block Scheduling</i>	W	F A

Table 1. Software and applications in use October 2021.

Each subject area taught at the high school uses a different online textbook company and a number of web-based teaching tools. For example, one of the math teachers uses the following:

- Kami (web based PDF mark-up tool)
- Desmos (web based online graphing tool)
- Geogebra (web based online geometry graphing tool)
- TI 84 graphing calculator (online application)

A more comprehensive inventory regarding local and web-based applications that are used in the classroom environment needs to be performed (similar to the math teacher example). This would be best accomplished via interview with each teacher or by survey.

1.1.3. Communications and Data Flows

The [REDACTED] School District leverages network infrastructure via the State of Wisconsin's BadgerNet contract which provides for internet access. The contract uses a commoditized provider infrastructure, consisting of multiple third-party telco providers and using AT&T as the overall Managed Service Provider (MSP). In-depth information regarding the network infrastructure can be found in the [TEACH Customer Information Package](#) (BadgerNet & TEACH, n.d., p. 3).

Figure 1. BadgerNet data flow diagram.



Note: Extracted from BadgerNet & TEACH.

1.1.4. High Priority Security Resources (on premise)

1.1.4.1 Security Facilities

The server room is the single onsite facility that has a high priority as it relates to information security.

1.1.4.2 Security Hardware and Devices

The firewall and all on-premise servers are high priority security assets.

1.1.4.3 Security Personnel

The IT Director is considered high priority security personnel, as this person is the most familiar and knowledgeable of the status of IT security systems that are in place on site.

1.1.5 Security Roles and Responsibilities

Cybersecurity roles are managed by the State of Wisconsin. The IT director and school district administrator serve as a cybersecurity liaisons between the school district and the State.

1.2 Business Environment

1.2.1 Mission, objectives, activities, and stakeholders

Mission Statement: [REDACTED]

1.2.2 Current environment

The current environment consists of the following items of note:

- The current superintendent has a strong financial background and is focused on a priority budgeting approach whereby money is saved through strategically timed investing and maximizing operating funds.
- The goal is to keep the community engaged through communicating and creating programs that serve the entire village of [REDACTED].
- A focus is being placed on providing modern educational spaces, technology, and programs.
- [REDACTED] public schools wants to make all families feel proud to be a part of a strong, tight-knit community.
- The school district is committed to ensuring that all students are able to learn in a physically safe environment.
- The school district is currently involved in the strategic planning process. It will be designed to address immediate and long-term needs of the school while also reducing the financial impact on district residents and improving program offerings for students.

1.2.3 Stakeholders

Stakeholders include:

- Students
- Faculty
- Administration/Office employees
- School board
- Parents
- Village residents

1.2.4 Approach to Cybersecurity

1.2.4.1 Cybersecurity infrastructure priorities

At this time, infrastructure priorities include:

- Cybersecurity awareness training;
- Determining when it is worthwhile to use third party services; and
- Budgeting

1.2.4.2 Critical functions, services, and dependencies

██████████ High School is dependent on the decisions made at the state government level for identifying critical functions, services, and dependencies. It is recommended that the school district request this documentation from the State of Wisconsin. However, it is highly advised that the school district conduct its' own analysis since its size and location present unique challenges. The Analysis of Critical Infrastructure Dependencies and Interdependencies offers an excellent approach to completing this task (U.S. Department of Energy, 2015)..

1.2.3 General Resilience Requirements

Resiliency requirements are addressed throughout this document including topics on business continuity, disaster recovery, and risk assessment.

1.3 Governance Framework

██████████ High School defers to the policies and procedures provided by the State of Wisconsin's Board of Education policies and procedures which are aligned with state and federal laws.

To the knowledge of the IT Director at the high school, no formal vulnerability or risk assessments have been performed at the high school level. The school district administrator is designated to oversee governance. Threats and vulnerabilities are monitored via the State of Wisconsin.

1.3.2 Cybersecurity Risk Management

1.3.2.1 Establish a cybersecurity policy and define how it will be communicated.

Cybersecurity policies are mandated through the State of Wisconsin Board of Education. Policies exist for the following:

- Acceptable use
- Privacy
- Email
- Password protection
- Internet usage
- Social engineering awareness

Communication of these policies is available via internet by going to

[REDACTED]

These policies are reviewed on a once-per-year basis.

1.3.2.2 Cybersecurity Alignment

Aligning cybersecurity with the various functions within the high school can be best accomplished by making sure cybersecurity risk is a required consideration when it comes to all decisions that need to be made. As the school budget does not allow for the hiring of a cybersecurity professional to make sure this happens, the minimum expectation is to have all staff share in the responsibility. When making any decisions one question should always be, *does this create any cybersecurity risk?*

As the school district strives for the schools to be an integrated part of the community, consideration should be made for a volunteer from the community who has cybersecurity experience and can be that voice at every meeting.

1.3.2.3 Legal and Regulatory Requirements

The school district is bound by the following legal and regulatory requirements as they relate to cybersecurity:

- Sections 1232f through 1232i, 7165 and Title 34 C.F.R. Part 99 of the Family Educational Rights and Privacy Act (FERPA) are aimed at protecting the privacy of student records. This law applies to all schools, public or private, elementary or secondary. This law prohibits educational institutions from releasing any personally identifiable information (PII) without the written consent from parents and eligible students.
- Health Insurance Portability and Accountability Act (HIPPA) requires educational institutions to protect student health information such as insurance and health issues.

- Children's Internet Protection Act (CIPA) addresses concerns about children's access to inappropriate content. This requires educational institutions to adopt an internet safety policy indicating the measures that will be taken to ensure protection for children from content that is harmful. It also mandates educating students about appropriate online behavior.
- Wisconsin Data Breach Notification Law is an overarching mandate that organizations, including cities, towns, villages and counties must notify individuals in the event of a data breach. This includes student, as well as personnel information.
- Wisconsin Act 79 changed the E-Cycle Wisconsin program to require public and private elementary and secondary schools in e-cycling electronic devices and accessories.
- Wisconsin Statute § 103.13 requires employers to allow employees to access any records that the employer keeps about an employee, subject to certain exceptions.
- Wisconsin Statute § 19.36(1) is concerned with confidentiality as it puts limitations upon access and withholding of data records.
- No Child Left Behind Act of 2001, Section 9528, 20 USC §7908 requires educational institutions to provide the names, addresses and phone numbers of male and female 11th and 12th grade students if requested by military recruiters or institutions of higher education.
- Student and Staff Network and Internet Acceptable Use and Safety
 - H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000
 - 47 U.S.C. 254(h), (1), Communications Act of 1934, as amended
 - 20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
 - 18 U.S.C. 2256
 - 18 U.S.C. 1460
 - 18 U.S.C. 2246
 - 76 F.R. 56295, 56303 (for staff only)

1.4 Threats and vulnerabilities

1.4.1 Vulnerabilities

A risk occurs when a threat exploits a vulnerability and causes a negative impact to the organization. Therefore, the first step to a risk assessment involves identifying the vulnerabilities that can be exploited by a threat. When a threat coincides with a vulnerability it is categorized as a risk.

1.4.1.1 Process to Identify Vulnerabilities

The initial vulnerability assessment will focus on network-based and host-based vulnerabilities. Review of the initial vulnerability assessment will take place once per year to identify any changes in the environment.

Inputs to identify vulnerabilities will come from the following sources:

- Documentation from past security incidents
- Any outage reports
- Past assessment reports, if any
- System logs
- Audit logs
- Vulnerability network scanning
- Personnel interviews
- Controls catalog [NIST 800-53 Rev. 5](#)

The following criteria will be used to assess and rate the severity of vulnerabilities:

Qualitative Rating	Numerical Equivalent	Description
Very High	5	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. No security measure can be identified to remediate the vulnerability.
High	4	The vulnerability is of <i>high</i> concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation.
Moderate	3	The vulnerability is of <i>moderate</i> concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from exploitation.
Low	2	The vulnerability is of <i>minor</i> concern, but effectiveness of remediation could be improved.
Very Low	1	The vulnerability is not a concern.

Table 2. Vulnerability assessment criteria.

Vulnerabilities will be entered into a list formatted as in the example below and the threat assessment team will collaborate to determine a threat source definition and relevance rating.

ID	Vulnerability	Vulnerability Severity
V-0001	Example: No offsite location to conduct business in the event that existing building or network infrastructure is unusable.	Very High

ID	Vulnerability	Vulnerability Severity
V-0002		
V-0003		

Table 3. Sample vulnerability log.

1.4.1.2 Roles and Responsibilities

IT director is most familiar with information security and will oversee the assessment for the high school. This person will be responsible for identifying members of the internal staff that can assume the responsibilities of a vulnerability assessment role. Personnel from the school district office are additional approved options.

The vulnerability assessment team consists of two roles:

Vulnerability Analyst (1 or more)

- Identify vulnerabilities using designated resources.

Risk Assessment Director

- Identify vulnerabilities using designated resources.
- Manage assessment from beginning to completion.
- Conduct yearly threat assessment.

1.4.2 Threats

The initial threat assessment will focus on network-based and host-based-vulnerabilities. Review of the initial threat assessment will take place once per year to identify any changes in the environment.

1.4.2.1 Roles and Responsibilities

The IT director is most familiar with information security and will oversee the assessment. This person will be responsible for identifying members of the internal staff that can assume the responsibilities of a threat assessment role. Personnel from the school district office are additional approved options.

The threat assessment team consists of two roles:

Threat Analyst (1 or more)

- Identify threats using designated resources.

Risk Assessment Director

- Identify threats using designated resources.
- Manage assessment from beginning to completion.
- Conduct yearly threat assessment.

1.4.2.2 Threat Identification Process

The initial threat assessment will focus on threats related to network-based and host-based assets. Review of the threat assessment will take place once per year to identify any changes in the environment.

Inputs to identify threats will come from the following sources:

- Table of adversarial threat events in [NIST 800-30 Rev. 1](#) (U.S. Department of Commerce, 2012, pp. E-2-6);
- [MITRE ATT&CK® Matrix for Enterprise](#);
- Reviewing incidents that have occurred in other high schools;
- Personnel interviews; and
- Natural and weather events that typically occur in the area.

The following criteria will be used to assess and rate the severity of threats:

Threat Source Definitions

- *Adversarial*: Individuals, organizations, or states that want to exploit an organization's dependency on its cyber resources.
- *Accidental*: Unintentional actions of an employee or privileged user.
- *Structural*: Failures of physical equipment or software due to aging, defect, environmental controls.
- *Environmental*: Natural or man-made disasters.

Relevance Rating Definitions

- *Confirmed*: Threat event has been seen by organization.
- *Expected*: Threat event has been seen by organization's peer or partners.
- *Anticipated*: Threat event has been reported by a trusted source.
- *Predicted*: Threat event has been predicted by trusted source.
- *Possible*: Threat event has been described by somewhat credible source.

Each threat will be entered into a list formatted as in the example below and the threat assessment team will collaborate to determine a threat source definition and relevance rating.

ID	Threat Event	Threat Source	Relevance
T-0001	EXAMPLE: Attacker performs network reconnaissance or scanning to discover network and computer assets.	Adversarial	Predicted
T-0002			
T-0003			

Table 4. Sample threat event log.

1.4.3 Probability and Impact

The threat assessment team will also assess each threat in terms of probability and impact.

1.4.3.1 Probability

Probability relates to the likelihood of a risk occurring. For this assessment, each threat event was given a probability rating:

Qualitative Rating	Numerical Equivalent	Description
Very High	5	Threat event is <i>almost certain</i> to occur.
High	4	Threat event is <i>highly likely</i> to occur.
Moderate	3	Threat event is <i>somewhat likely</i> to occur.
Low	2	Threat event is <i>unlikely</i> to occur.
Very Low	1	Threat is <i>highly unlikely</i> to occur.

Table 5. Probability rating table. NOTE: Adapted from *Guide for Conducting Risk Assessments*, U.S. Dept. of Commerce, 2012.

1.4.3.2 Impact

Impact relates to the severity of the threat event when it occurs. Degrees of impact are described as:

Qualitative Rating	Semi-Quantitative Values	Description
Very High	96-100	Threat event could be expected to have <i>multiple severe or catastrophic</i> adverse effects on operations, assets, individuals, or other organizations.
High	80-95	Threat event could be expected to have <i>severe or catastrophic</i> adverse effects on operations, assets, individuals, or other organizations. This includes degradation to the point that primary business functions cannot be performed; damage to assets; major financial loss; and loss of life or serious life-threatening injuries.
Moderate	21-79	Threat event could be expected to have <i>serious</i> adverse effects on operations, assets, individuals, or other organizations. This includes situations where the organization is able to perform its primary functions but the effectiveness of the functions is significantly reduced; damage to assets; financial loss; harm to individuals but with no loss of life or serious injury.
Low	5-20	Threat event could be expected to have <i>limited</i> adverse effects on operations, assets, individuals, or other organizations. This includes situations where the organization is able to perform its primary functions but the effectiveness of the functions is noticeably reduced; minor damage to assets; minor financial loss; minor harm to individuals.

Qualitative Rating	Semi-Quantitative Values	Description
Very Low	0-4	Threat event could be expected to have a <i>negligible</i> adverse effect on operations, assets, individuals, or other organizations.

Table 6. Probability rating table. NOTE: Adapted from *Guide for Conducting Risk Assessments*, U.S. Dept. of Commerce, 2012.

The threat assessment team will assess each of the threats by providing a numerical rating describing its probability of occurring and level of impact if it were to occur. These ratings will be entered into a risk register as shown in Table 7 in example below.

Priority Level is determined by multiplying the *Impact* rating by the *Probability* rating:

$$\text{Priority Level} = \text{Impact} \times \text{Probability}$$

All information in the risk register are required fields that must be completed before submitting for recommendations review. After the initial assessment, high level administrators will have access to this register to add risk entries as necessary. These entries will be reviewed by the Risk Assessment Director.

Risks (threats) categorized as very high and high will require priority attention for mitigation. Any risks categorized as very low, low, or moderate will be noted and no further action will be required.

Risk Description	Impact Description	Impact Level	Probability Level	Priority Level
EXAMPLE 1: External threat actor can scan for network asset information to attempt exploits on.	Low	4	5	20
EXAMPLE 2: Threat actor places removable media (e.g. flash drives) containing malware in locations where employees will be tempted to pick up and use on computers that are connected to various servers.	Moderate	79	2	158

Table 7. Risk analysis example.

1.4.5 Risk Mitigation

Items on the risk register will be prioritized by the priority level designated for each risk. Each risk that is rated as high or very high will then be analyzed for mitigation strategies. They will be entered into a list as shown in Table 8:

ID	Status	Subject	Inherent Risk	Submitted
1001	New	EXAMPLE: Firewall rules are not regularly updated.	Very High	10/1/2021
1002	New	EXAMPLE: No defense in depth: IDS/IPS	Very High	10/10/2021
1003				

Table 8. Risk register example.

A risk mitigation form will be completed for each item on the list. This will provide information for suggested mitigation strategy and its justification.

EXAMPLE

1001 - Firewall rules are not regularly updated.

Risk Tolerance Level:

___ (AC) Acceptance ___ (T) Transference ___ (AV) Avoidance ___ (R) Reduction

Security Control Select controls from NIST SP 800-53 Rev. 5	Reduces (V) Vulnerability (T) Threat impact
SC-7(5) Boundary Protection – Deny by Default / Allow by Exception	V
SI-4(5) System Monitoring – System-Generated alerts	T

Risk 1001 Mitigation Plan	
Mitigation Submission Date:	Click or tap to enter a date.
Planned Mitigation date:	Click or tap to enter a date.
Planning Strategy (choose from drop down list):	Mitigate
Mitigation Effort: (choose from drop down list):	Exceptional
Mitigation Cost:	
Mitigation Owner:	

Mitigation Controls

Current Solution:	
Security Requirement:	
Security Recommendation:	

Justification:

1.5 Risk Management Strategy

Each risk will take on a different strategy. These strategies are:

- Acceptance: The risk is accepted and no action will be taken to mitigate it.
- Transference: Risk is transferred to a third party (i.e. insurance). The risk itself still exists.
- Avoidance: Risk is eliminated by not taking any action that would make it occur.
- Reduction: Risk is less severe because actions are taken to minimize it.

1.6 Risk Management for Supply Chains

1.6.1 Prioritized list of current suppliers for information systems, services, components

All vendors are required to apply to be a supplier via the WISEdata program which operates under the U.S. Department of Education. School districts are restricted to using these vendors.

1.6.2 Alternative providers for various systems, services, and components that support business critical functions

All vendors are required to apply to be a supplier via the WISEdata program which operates under the U.S. Department of Education. School districts are restricted to using these vendors.

1.6.3 Alternative provider selection criteria

Alternative providers shall be chosen based on the following criteria:

- Knowledge and experience with the hardware that is used by the high school.
- Knowledge and experience with the application software that is used by the high school.
- OEM certifications held by technicians for the hardware and software that used by the school.
- The number of people within the company who have the required knowledge to support the system. Having many people with the knowledge reduces the possibility of sufficient response time to incidents.
- Capability to provide support remotely.

1.6.4 Alternate providers and disaster recovery testing

Alternate providers will be informed of disaster recovery drills by Wisconsin Emergency Management. Dates for such drills will be coordinated with alternate providers to ensure their availability and review the goals and expectations of the simulation.

Protecting Assets

2.1 Access Management

2.1.1 Assets and Facilities

2.1.1.1 Physical Access to Facilities

The doors are controlled by locking system software.

2.1.1.2 Access to Assets Containing Critical or Sensitive Data

The IT director and network engineer are the only roles that have access to the server and telecommunications rooms on site. The server room itself is a locked area with a camera monitoring the entry door area.

Table 10 summarizes the sensitivity and criticality classifications for rooms that contain business critical assets or information. Each of these rooms are classified according to the following category descriptions:

Classification	Description	Special Treatment
<i>Proprietary</i>	Room contains proprietary information storage.	Doors and cabinets must remain locked at all times; administration staff access only with badge; security cameras inside and outside doors for monitoring; drives are encrypted; passwords on all equipment; equipment maintenance personnel escorted
<i>Confidential</i>	Room contains confidential information storage.	Server cabinets must remain locked at all times; visitors require badge and employee escort; security cameras outside doors only; drives are to be encrypted and passwords on all IT equipment
<i>Privileged</i>	Room contains IT equipment holding sensitive data.	Visitors require badge; equipment is to be encrypted and password protected
<i>Public</i>	General public is free to spend time in this room without escort or badge.	Computers auto-reimage at end of each business day.
<i>Critical</i>	Room contains critical computing resources which cannot be performed manually.	N/A
<i>Vital</i>	Room contains vital computing resources which can be performed manually for a short time.	N/A

Table 9. Sensitivity and criticality classification descriptions..

Room	Sensitivity Class	Criticality Class	Assets or Information	Controls
Offices	Privileged	Vital	Paper files	surge protection; smoke detectors; fire suppression system; annual fire department inspection; automatic door locks;
Server	Proprietary	Critical	Servers Switches Networking equipment ISP Connection RAID hardware	alternate power generator; Smoke detectors, fire extinguishers, fire suppression system, annual fire department inspection; water detection; air conditioning; RAID setup; redundant networking; surge protection, uninterruptible power supplies; badge system; automatic door locks; security cameras
Telecom	Confidential	Critical	Alternate ISP connection; Switches	Surge protection; uninterruptible power supplies; alternate power generator; water detection; air conditioning; fire extinguishers; smoke detectors; fire suppression system; annual fire department inspection; badge system; automatic door locks; security cameras

Table 10. Allocation of critical assets according to sensitivity classification.

2.1.2 Remote Access

There are no formal policies and procedures around remote access since the IT director and network engineer are the only roles that have remote access. Remote access is granted for troubleshooting purposes. Team Viewer is the application used to facilitate remote connections.

2.1.3 Access Permissions

Access permissions are managed by Active Directory. Information was unavailable regarding how access permissions are structured aside from confirming that principle of least privilege is enforced.

2.1.4 Network Access

The structure of the internal network was not available to be able to assess the degree of network segregation nor the manner in which it is segregated.

2.1.5 Authentication

Authentication goes through Active Directory and is directly tied to the school's Google Workspace account (school-specific) through Google Sync.

2.2 Cybersecurity Awareness

The State of Wisconsin Board of Education has developed a policy for enhancing cybersecurity awareness for both students and staff. This policy takes into account the requirements of the following federal and state laws and regulations:

- H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000
- 47 U.S.C. 254(h), (1), Communications Act of 1934, as amended
- 20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
- 18 U.S.C. 2256
- 18 U.S.C. 1460
- 18 U.S.C. 2246
- 76 F.R. 56295, 56303 (for staff only)

In addition, The Wisconsin Department of Instruction offers a website with resources for developing cybersecurity awareness. The site, <https://dpi.wi.gov/cyber-security>, has information about cybersecurity resources, data privacy resources (including a data breach tabletop exercise), webinars, and tips. In addition, Infosec.IQ is contracted with the State of Wisconsin (and therefore, the Wisconsin Department of Instruction) to provide cybersecurity awareness training.

2.3 Data Security Management

2.3.1 Protection and Preservation of Data at Rest

Daily backups are kept on site and off site. Exact location could not be revealed for security purposes. Backups to the cloud are also being conducted.

2.3.2 Protection and Preservation of Data in Transit

Data in transit is protected via a hardware-based firewall. Cipafilter and GoGuardian are used for web filtering.

2.3.3 Asset End-of-Life Disposal

According to school district policy, the following criteria is used to determine when IT devices need to be taken out of commission and physically disposed:

1. repair parts for the equipment no longer readily available
2. repair records indicate the equipment has no usable life remaining
3. obsolete and no longer contributing to the educational program
4. some potential for sale at a school auction
5. creates a safety or environmental hazard

Any school-owned IT assets deemed to be disposed of, will be e-cycled through the E-Cycle Wisconsin program.

2.3.4 Network Capacity

Network capacity is more than sufficient. All on-premise servers have been substantially upgraded since the summer 2019. Exact numbers were not available at the time of this plan was published but can be obtained from the School District of [REDACTED].

2.3.5 Maintenance and repair policies and guidelines for hardware

The school district administrator has the overarching responsibility of making sure that school equipment is inspected, repaired and has a preventative maintenance plan in place. The plan includes a:

- regular summer program of equipment repair and conditioning;
- maintenance of a critical spare parts inventory; and
- an equipment replacement program.

2.4 Information Management

2.4.1 Information Security Policies, Processes and Procedures

2.4.1.1 System Development Life Cycle (SDLC)

The System Development Life Cycle is implemented in a very loose manner. The high school does not have the capacity to develop its own systems. The SDLC is used to determine if a new system is required to create a solution for a recurring infrastructure problem. If the development of a new system is required, a third party vendor will be hired to design and test it.

2.4.1.2 Configuration Change Control Management

The IT director manages all on-premise IT infrastructure for the high school. In a formal change control process, this role serves as the change requester, implementer, reviewer, approver, and manager. Any configuration changes deemed necessary are documented into a change log spreadsheet that includes the date, system, nature of change to be made, and reason for change. This log is shared with the public school administration IT team.

2.4.1.3 Data Backup Policy

Documentation of a data backup policy is kept at the school district site but was unavailable to access at the time this plan was published. It is highly recommended that the IT director for the high school contacts the school district to obtain this information to ensure that the required backups are being performed.

The IT director confirms that daily backups are being performed and are secured both on site and in the cloud.

2.4.1.4 Data Destruction Policy

The State of Wisconsin's E-Cycle program requirement requires that any school-owned IT equipment that can no longer be used must be electronically recycled. The school district defaults to federal guidelines for data destruction policy due to all of the state and federal laws they must follow related to the treatment of data and personally identifiable information (PII). These state and federal laws are outlined in Section 1.3.2.3.

Before any school-owned IT equipment is turned in for e-cycling, however, the hard drives need to be removed and sent to a vendor (to be determined) that will perform physical data destruction on these drives in accordance with [NIST 800-88](#) (U.S. Department of Congress, 2014) specifications and provide certification of that destruction for audit purposes.

2.4.1.5 Business Continuity and Incident Response Plan.

The high school follows the school district's school safety plan which includes IT services.

2.4.1.6 Disaster Recovery

In the event of a disaster, ██████████ High School defers to the ██████████ School District which follows the plan outlined by Wisconsin Emergency Management (WEM). WEM "coordinates effective disaster response and recovery efforts in support of local governments. Through planning, training and exercising, WEM enhances the state's ability to prepare for, mitigate, respond to, and recover from both natural and technological emergencies" (State of Wisconsin Department of Administration, 2017).

The plan includes the following (at minimum):

- adequate equipment insurance;
- procedures used to backup all programs and data on a daily, monthly, quarterly, and year-end basis;
- backup storage off-site;
- maintenance agreements for hardware and software (including, but not limited to the operating system);
- a list of vendor contacts to be called for the immediate replacement of disabled equipment or corrupted software.

2.4.1.7 Incident and Response and Business Continuity Testing

All cybersecurity incidents are to be reported to the Wisconsin Cybersecurity Response Team (CRT) at crt@wisconsin.gov or 800-943-0003. Notifications of incidents affecting to the State of Wisconsin information technology infrastructure are communicated to the ██████████ School District's district administrator and ██████████ High School's IT director.

2.5 Asset Maintenance

The school district administrator has the overarching responsibility of making sure that school equipment is inspected, repaired and has a preventative maintenance plan in place. The plan includes a:

- regular summer program of equipment repair and conditioning;
- maintenance of a critical spare parts inventory; and
- an equipment replacement program.

2.6 Technology Management

2.6.1 Audit logs

Audit logs for Active Directory and firewall are configured. Locally, logs are reviewed on an as-needed basis, rather than proactively. The IT director, network engineer, school district administrator have permissions to access this information. The State of Wisconsin's BadgerNet infrastructure is monitored through AT&T Managed Services Division.

2.6.2 Removable media

Removable media restrictions have been put in place but are set as a precautionary measure since students, faculty, and staff utilize cloud computing. Students and faculty files are saved to a file directory in the cloud.

2.6.3 Essential capabilities of systems

All systems have been configured so that only the essential capabilities are enabled based on a user's role in Active Directory.

Detecting Anomalies

3.1 Detect anomalies through event analysis

Anomaly detection is important to identify network intrusions. It is necessary to "identify and take action on changing user needs, detect and mitigate malignant actors and behaviors, and take preventive actions to reduce costly repairs" (Kulandaivel & Irwin, 2020). To that end, alerts are set and monitored by BadgerNet personnel and AT&T Managed Services.

3.1.1 Baselines for network users and systems

Before anomalies can be detected, it is important to know what typical network traffic and user activity looks like. Baselines have been created for the ██████████ High School network. They have been established and are managed remotely via BadgerNet and AT&T Managed Services. The exact information describing the baselines is not readily available. A special request for this information is required which needs approval by the school board and superintendent. This was unavailable at the time of this writing.

3.1.2 Analyze events to understand targets and methods

The responsibility for the management of malicious cybersecurity events is delegated to the IT director. The IT director will collaborate with personnel from BadgerNet and A&T to ensure understanding of:

- Analyze malicious cybersecurity events
- Collect and correlate event data
- Determine impact of malicious events
- Establish incident alert thresholds

3.2 Detect anomalies by monitoring systems

3.2.1 Methods of monitoring assets and information systems

As the network infrastructure is run by the State of Wisconsin, the responsibility for monitoring activities is managed by the State. The IT director has permissions to pull reports specific to individual sites.

3.2.2 Continuous monitoring of assets and information systems

Metrics are reviewed on a schedule and are categorized as strategic, tactical, or operational.

The context of strategic metrics is from a management perspective; These metrics revolve around audits and policies and are discussed annually.

Tactical metrics are those that observe how the network is performing. The focus is on determining trends and is reviewed every six months.

Operational metrics are specific metrics and focus on key performance indicators.

Metric reports are pulled based on the following schedule:

Category	Metric	Calculation and Collection Method	Period of Reporting
Strategic	Cost of security	Review accounting reports at annual budget review	Yearly
	Cost of incidents	Incident response totals	6 months
Tactical	Percent of employees passing phishing test	Email phishing test via security awareness program vendor	6 months
Operational	Data recovery capability	Test backups quarterly for a random sample of systems, including operating system and data restoration	Quarterly
	Security skills assessment	Test security awareness understanding, attempt periodic social engineering tests using phishing emails and phone calls. If employee fails test, will need to attend a training.	6 months

Category	Metric	Calculation and Collection Method	Period of Reporting
	Limitation and control of network ports, protocols, and services	Automated port scanning; Temporarily place a secure test service randomly on the network which will respond to network requests. Reported via alert or email within 24 hrs. and reported every 24 hours by alert/email thereafter until the port is deactivated or approved.	Daily
	Secure configuration for network devices such as firewall, routers, and switches	Any change to network device is recognized within 24 hrs. with a log or email alert, and every 24 hours thereafter until it is investigated. Change to either software or configuration are reported.	Daily

Table 11. Metric reporting schedule.

3.2.3 Monitoring external suppliers

Since the high school is part of the Wisconsin Department of Public Instruction (DPI), it is required to select suppliers from an approved list. These suppliers are vetted and certified by via the U.S. Department of Education's WISEdata program. Please see Appendix D for a complete list. This list is updated regularly and can be viewed at <https://dpi.wi.gov/wisedata/schools/vendor-list>.

Suppliers apply to the WISEdata program and, if accepted, are given access to the WISEdata Ed-Fi Credentialing application which connects the various state DPI systems and "generates encryption keys and secrets that are used to establish a secure connection between the vendor system and DPI" (Wisconsin Department of Public Instruction, n.d.). This also allows the Department of Education and DPI to monitor a supplier's network connectivity via the secure connection.

3.2.4 Detecting unauthorized devices, software, and connections.

██████████ High School contracts with an approved third-party vendor to monitor for unauthorized devices, software, and connections, cybersecurity events and anomalies, and conducts regular vulnerability scans. The IT director is informed of issues and works with the vendor to mitigate issues that arise. The school district administrator oversees the overall program and is made aware of incidents.

3.2.5 Anomalous event detection and awareness processes.

██████████ High School contracts with a third-party vendor to maintain anomalous event detection and awareness processes. Monitoring and reporting is communicated by the vendor directly to the high school's IT director, the school district administrator, and the Wisconsin Department of Public Instruction Business and Information and Technology Department. Anomaly detection methods and activities are reviewed and approved on a quarterly basis by the vendor and the school district administrator.

Respond to Incidents

4.1 Respond to incidents by controlling steps

4.1.1 Establishment of incident response processes and procedures.

Incident response processes and procedures have been established by the State of Wisconsin to be implemented by the individual school districts.

4.1.1.1 Incident response plan

The State of Wisconsin is responsible for all elements of the information security incident response (IR) plan including classification of cybersecurity incidents, threats, and vulnerabilities. Analysis, differentiation, and categorization of cybersecurity incidents are defined by the IR plan. In the event of an incident, employees may contact the Cyber Response Team at Wisconsin Cybersecurity Response Team (CRT) at crt@wisconsin.gov or 800-943-0003.

4.1.2 Establishment of business continuity processes and procedures.

According to [REDACTED] School District policy # [REDACTED] regarding electronic data processing disaster recovery planning, the School District Administrator needs to have an electronic data processing disaster recovery plan. The plan includes documentation regarding:

- Insurance policies;
- Daily, monthly, quarterly, and year-end backup procedures;
- Off-site data storage;
- Maintenance agreements for all implemented hardware and software (including, but not limited to the operating systems used); and
- Vendor contacts list.

In the event of a disaster, [REDACTED] High School defers to the [REDACTED] School District which follows the plan outlined by Wisconsin Emergency Management (WEM). WEM “coordinates effective disaster response and recovery efforts in support of local governments. Through planning, training and exercising, WEM enhances the state’s ability to prepare for, mitigate, respond to, and recover from both natural and technological emergencies” (State of Wisconsin Department of Administration, 2017).

4.2 Respond to incidents by coordinating action

4.2.1 Stakeholder communication and roles

Coordinating messaging with internal stakeholders is necessary to ensure consistent and accurate information is being shared with necessary school, department, and agency personnel. The [REDACTED] School District administrator will be notified by a designated representative from the State of Wisconsin information security team of all incidents relevant to the school district.

The school district is small and therefore, the IT director manages information technology issues for the elementary and junior/senior high schools. The IT director is designated as a DPI statewide information security incident response team member.

4.2.2 Reporting criteria

All cybersecurity incidents are to be reported to the Wisconsin Cybersecurity Response Team (CRT) at crt@wisconsin.gov or 800-943-0003. Notifications of incidents occurring to the State of Wisconsin information technology infrastructure are communicated to the [REDACTED] School District's district administrator and [REDACTED] High School's IT director. Incident communication from the State of Wisconsin Department of Public Instruction information security representative will include (as applicable):

- What applicable groups, technologies, or processes are affected?
- What systems and/or configurations are vulnerable? Does a patch exist?
- Do automated mitigation methods exist?
- What level of effort is required to mitigate?
- How long will automated or manual mitigation methods take?
- What tools or technologies are required to implement mitigation method(s)?
- How does this effect unpatched systems?
- What level of access is granted by vulnerability?
- What group discovered it?
- What identifiers exist (CVE, etc.)?
- Describe prevalence of vulnerability among constituency, if able.
- Have threat actors been identified?
- What is the profile of technologies, processes, or people targeted by threat actors?
- What, if any, blacklists are effective against threat actors?
- Is the incident ongoing?
- How long has the incident been in progress?
- When were indicators of the incident detected?
- What happened and what is the result of the incident?

Adapted from Carnegie Mellon University 2020

4.3 Respond to incidents by analyzing the situation

For incidents that affect [REDACTED] High School directly, the IT director is designated to contact the Wisconsin Cybersecurity Response Team (CRT) at crt@wisconsin.gov or 800-943-0003. As the [REDACTED] School District uses BadgerNet for its network infrastructure, benchmarks and baselines are pre-established and alerting structure is designated within the contract between [REDACTED] School District and BadgerNet.

Upon notification to the IT director, the director will investigate alerts and work with BadgerNet to rectify the situation. The IT director will notify the school district administrator if further resources are necessary (e.g. forensic investigation, additional IT support).

The State of Wisconsin is responsible for all elements of the information security incident response (IR) plan including classification of cybersecurity incidents, threats, and vulnerabilities.

Analysis, differentiation, and categorization of cybersecurity incidents are defined by the IR plan. All school districts are directed to the follow procedures of the IR plan as directed.

4.4 Respond to incidents by mitigating the damage

The primary responsibility of containing, mitigating, and resolving cybersecurity incidents falls on the State of Wisconsin Department of Instruction information security department that disseminates cybersecurity vulnerabilities and threat notices to the individual school districts. The [REDACTED] School District will utilize the IT director to coordinate the mitigation of the damage caused by cybersecurity incidents and has the capability to engage the services of the designated third-party vendor.

When deciding what route to take forensically during the remediation of an incident, it is important to preserve the state of the affected systems as if they will be something needed for legal purposes. At the time the incident is happening, the seriousness of the incident is not completely known. An incident may appear to be one thing but may be something altogether different; a forensics analysis of the systems involved will be required for incidents that are categorized at level one or two.

4.5 Respond to incidents by making improvements

The State of Wisconsin Department of Instruction information security incident response team conducts quarterly tabletop scenarios and a live scenario once per year. All school districts in Wisconsin have a representative on the information security team. [REDACTED] School District's IT director is a member of that team and will coordinate with the district administrator to implement the necessary systems to conduct the live testing scenarios.

Lessons learned from actual incidents, tabletop exercises, and live incident scenarios and business continuity exercises will be reflected in updated incident response and business continuity plans. All updates and trainings are managed by the State of Wisconsin Department of Instruction information security incident response team.

5. Recovery from incidents

Incident recovery processes and procedures come from the State of Wisconsin Department of Instruction information security department. Recovery and restoration procedures will be executed while incidents are happening and after incidents have occurred. As part of the incident response process a post mortem will be performed to evaluate recovery or restoration activities that were implemented and determine improvements that need to be included in an updated version of the incident response and recovery plans.

Coordination of activities during incident recovery will be implemented according to the disaster recovery plan managed by WEM. A representative from each stakeholder group, as designated in the plan, will serve as part of a working group that will coordinate to implement recovery and restoration activities. The director of administration for the [REDACTED] school district will lead this working group. Another representative from each stakeholder group will also serve on a public relations working group to ensure all aspects of external and internal communication are being covered; the public relations director for the school district will head this working group.

APPENDIX A – REFERENCES

- Alberts, R. (2018, August). *IT Change Management: A Practical Approach for Higher Education*. EDUCAUSE. <https://uit.stanford.edu/sites/default/files/2018/09/19/Educause%20-%20IT%20Change%20Management%20-%20A%20Practical%20Approach%20for%20Higher%20Education.pdf>
- BadgerNet, & TEACH. (n.d.). *TEACH Customer Information Package* [Unpublished working paper]. <https://det.wi.gov/Documents/TEACH%20Customer%20Info%20Package%20-%20BadgerNet%20Support.pdf>
- Belfield, G. (2019, August 27). How Reliable is your School's Data Destruction? *The Headteacher*. <https://www.theheadteacher.com/school-procurement/ict/how-reliable-is-your-schools-data-destruction>
- Bellasio, J., Flint, R., Ryan, N., Sondergaard, S., Gonzalez Monsalve, C., Meranto, A. S., & Knack, A. (2018). *Developing Cybersecurity Capacity*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf
- Binwal, P. (2015, June 29). Creating a Cybersecurity Governance Framework: The Necessity of Time. *Security Intelligence*. <https://securityintelligence.com/creating-a-cybersecurity-governance-framework-the-necessity-of-time/>
- Centers for Disease Control and Prevention. (2018, September 14). Family Educational Rights and Privacy Act (FERPA). *Public Health Professionals Gateway: Public Health Law*. <https://www.cdc.gov/phlp/publications/topic/ferpa.html>
- Cole, P. D. (2021, August 18). *Background memo on Board Order WA-11-19, relating to revisions to chapters NR 500, 502 and 520 and creation of chapter NR 530 for the purpose of implementing electronics recycling program requirements* [Memo to All Members of the Natural Resources Board].

E-Cycle Wisconsin Program Information. (2021, October 23). *Wisconsin Department of Natural Resources*. <https://dnr.wisconsin.gov/topic/Ecycle/Wisconsin.html>

Employment Regulations, Wis. Stat. § 103.13. <https://docs.legis.wisconsin.gov/statutes/statutes/103/13>

Enterprise Matrix. (2021, October 20). Retrieved October 20, 2021, from <https://attack.mitre.org/matrices/enterprise/>

Family Educational Rights and Privacy, 34 C.F.R. § 99 (). <https://law.justia.com/cfr/title34/34-1.1.1.1.33.html>

Federal Communications Commission Consumer and Governmental Affairs Bureau. (2019, December 30). *Children's Internet Protection Act (CIPA)*.

https://www.fcc.gov/sites/default/files/childrens_internet_protection_act_cipa.pdf

Guardian Data Destruction. (2021). What is a Certificate of Data Destruction?

<https://guardiandatadestruction.com/resource-center/what-is-a-certificate-of-data-destruction/>

IBM Security. (2021). *Cost of a Data Breach Report 2021*. IBM Corporation.

<https://www.ibm.com/downloads/cas/OJDVQGRY>

Infosec. (2021). *Infosec IQ*. Infosec IQ. Retrieved November 27, 2021, from

<https://securityiq.infosecinstitute.com/>

Infosec IQ content library. Explore massive library of industry- and role-based training resources: Preview training modules, reinforcement tools, learner assessments and more.

Security awareness resource center: Jumpstart your security awareness program. Download our cybersecurity tip sheets to share with your employees or explore our security awareness webinar library. Pre-built training plans: Download the free security awareness campaign kits and get your next training program started today!

Kulandaivel, S., & Irwin, C. (2020, November 19). Use real-time anomaly detection reference patterns to combat fraud. *Google Cloud*. <https://cloud.google.com/blog/products/data-analytics/using-automated-ml-streaming-architecture-to-find-anomalies>

- Lieberman, M. (2020, March 17). 4 Big Cybersecurity Priorities for Schools: Training, Purchasing, Monitoring, and Budgeting. <https://www.edweek.org/technology/4-big-cybersecurity-priorities-for-schools-training-purchasing-monitoring-and-budgeting/2020/03>
- Lincke, S. (2015). *Security Planning: An Applied Approach*. Springer International.
- Manley, B. (2020). *A Guide to Effective Incident Management Communications*. Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651819.pdf
- National Computer Warehouse Services. (n.d.). How to Dispose of a Hard Drive While Being HIPAA Compliant. <https://nationalcws.com/how-to-dispose-of-a-hard-drive-while-being-hipaa-compliant/>
- National Institute of Standards and Technology. (2021). *Cybersecurity Framework*. NIST. Retrieved October 23, 2021, from <https://www.nist.gov/cyberframework>
- [REDACTED]
- [REDACTED]
- SANS. (2021). *Security Policy Templates*. SANS. Retrieved October 20, 2021, from <https://www.sans.org/information-security-policy/?page=6>
- Sethi, M., & Sharma, A. (2013). Information System and System Development. In *Software Development Techniques for Constructive Information Systems Design* (pp. 118-127). IGI Global. <https://doi.org/10.4018/978-1-4666-3679-8.ch007>
- State of Wisconsin Department of Administration - Division of Enterprise Technology. (2017, July 26). *State of Wisconsin Cybersecurity Strategy*. <https://det.wi.gov/Documents/Cybersecurity%20Strategy%202017.pdf>
- 2021 Data Breach Investigations Report. (2021). Verizon. <https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf>
- U.S. Department of Commerce. (2012, September). *Guide for Conducting Risk Assessments* (National Institute of Standards and Technology (NIST), Author; SP 800-30 Rev.1). National Institute for Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-30r1>

- U.S. Department of Commerce National Institute of Standards and Technology. (2014, December). *Guidelines for Media Sanitization* (R. Kissel, A. Regenscheid, M. Scholl, & K. Stine, Authors; Special Publications SP 800-88 Rev. 1). National Institute of Standards and Technology.
<http://dx.doi.org/10.6028/NIST.SP.800-88r1>
- U.S. Department of Commerce National Institute of Standards and Technology. (2020, September). *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53 Revision 5). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-53r5>
- U.S. Department of Congress. (2014, December). *Guidelines for Media Sanitization* (R. Kissel, A. Regenscheid, M. Scholl, & K. Stine, Authors). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-88r1>
- U.S. Department of Congress. (2020, September). *Security and Privacy Controls for Information Systems and Organizations* (Joint Task Force Interagency Working Group, Author; Publication No. SP 800-53 Rev. 5). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-53r5>
- U.S. Department of Energy. (2015, June). *Analysis of Critical Infrastructure Dependencies and Interdependencies* (F. Petit, D. Verner, D. Brannegan, W. Buehring, D. Dickinson, K. Guziel, . . . J. Peerenboom, Authors). Argonne National Laboratory.
<https://publications.anl.gov/anlpubs/2015/06/111906.pdf>
Argonne National Laboratory
- Wisconsin Department of Agriculture Trade and Consumer Protection. (2019, December). *Wisconsin's Data Breach Notification Law* (Bureau of Consumer Protection, Author).
<https://datcp.wi.gov/Documents/IDTheftDataBreach607.pdf>
- Wisconsin Department of Public Instruction. (n.d.). *Cyber Security Alerts in WISEadmin Portal*.
Wisconsin Department of Public Instruction. Retrieved November 21, 2021, from
<https://dpi.wi.gov/wisedata/help/wiseadmin-portal/cyber-incidents>

Wisconsin Department of Public Instruction. (n.d.). [Info for Vendors]. Wisconsin Department of Public Instruction. Retrieved November 21, 2021, from <https://dpi.wi.gov/wisedata/vendors>

Wisconsin Department of Public Instruction. (n.d.). *Vendor List*. Wisconsin Department of Public Instruction. Retrieved November 21, 2021, from <https://dpi.wi.gov/wisedata/schools/vendor-list>

Wis. Stat. § 7162 (Jan. 8, 2002). <https://statecodesfiles.justia.com/us/2014/title-20/chapter-70/subchapter-iv/part-a/subpart-4/sec.-7165/sec.-7165.pdf>

Wis. Stat. Ann. § 19.36. <https://law.justia.com/codes/wisconsin/2012/chapter-19/section-19.36/>

APPENDIX B – IT ASSET INVENTORY DETAIL

Groups included in asset analysis

- Teachers
- Parents
- Students
- Administration (Office Staff)
- Finance
- HR
- IT

Explanation of Granted Permissions

- R – Read permissions: User can only read documents.
- W – Write permissions: User can read, create, and save documents.
- X – Execute permissions: User can read, create, and save documents; execute programs

Criticality Classifications

- **Critical** – Cannot be performed manually. Tolerance of interruption is very low.
- **Vital** – Can be performed manually for very short time.
- **Sensitive** – Can be performed manually for a period of time, but may cost more in staff.
- **Nonsensitive** – Can be performed manually for an extended period of time with little additional cost and minimal recovery effort.

Source: *Security Planning: An Applied Approach* by Susan L ncke (2015)

Sensitivity Classifications

- **Proprietary** – Data protects competitive edge. Data is of critical strategic importance to the school. Dissemination could result in serious financial impact.
- **Confidential** – Information protected by FERPA, HIPAA, and breach notification law. Shall be available on need-to-know basis only. Dissemination could result in financial liability or reputation loss.
- **Private** – Data should be accessible to management or for use with particular parties within the school. Could cause internal strife or divulge trade secrets if released.
- **Public** – Disclosure is not welcome, but would not adversely impact the school.

Source: *Security Planning: An Applied Approach* by Susan L ncke (2015)

Asset Name	PowerTeacher Grading Application & Database
Functional Value to Organization	Aggregates and analyzes educational progress of students
Location	3 rd party vendor
Criticality/Sensitivity Classifications	Nonsensitive / Confidential
IS System/Server Name	Online
Data Owner	IT Director
Designated Custodian	IT Director
Granted Permissions	Teachers (R-W-X); Parents (R); Students (R); Administration (R)

Asset Name	Pride Block Scheduling Application
Functional Value to Organization	Collects all student/family personal information, immunization records, student fees; manages course registration and determines class rosters; manages day-to-day attendance records
Location	School Administration Building
Criticality/Sensitivity Classifications	Sensitive / Confidential
IS System/Server Name	Online
Data Owner	IT Director
Designated Custodian	IT Director
Granted Permissions	Parents (R-W); Students (R); Teachers (R-W); Administration (R-W); IT (R-W-X)

Asset Name	Security Camera Software/Files
Functional Value to Organization	Allows monitoring of areas inside and outside of the building for physical security.
Location	Administration Office
Criticality/Sensitivity Classifications	Sensitive / Confidential
IS System/Server Name	Dedicated desktop computer
Data Owner	Principal
Designated Custodian	IT Director
Granted Permissions	Administration (R-W-X); IT (R-W-X)

Asset Name	All Online Educational Resources
Functional Value to Organization	Provides online textbooks, assessment materials, and online student and teacher tools
Location	3rd party vendor
Criticality and Sensitivity Classifications	Nonsensitive / Public
IS System/Server Name	Online
Data Owner	Librarian
Designated Custodian	IT Director
Granted Permissions	Students (R-W); Parents (R); Teachers (R-W-X); IT (R-W-X)

Asset Name	Skyline HR Application/Files
Functional Value to Organization	Contains all HR records related to hired staff; timekeeping and payroll functions flow this system
Location	3 rd Party Vendor
Criticality and Sensitivity Classifications	Critical / Confidential
IS System/Server Name	Online
Data Owner	HR Director
Designated Custodian	IT Director
Granted Permissions	HR Department (R-W-X); Teachers (R-W); Administration (R-W); Finance (R-W); IT (R-W-X)

Asset Name	Office 365 Application/Files
Functional Value to Organization	Word processing, spreadsheet, presentation, and email applications used by all students, teachers, and office staff.
Location	3 rd party vendor
Criticality and Sensitivity Classifications	Critical / Proprietary
IS System/Server Name	Online
Data Owner	IT Director
Designated Custodian	IT Director
Granted Permissions	HR (R-W); Teachers (R-W); IT (R-W-X); Administration (R-W); Students (R-W); Finance (R-W)

Asset Name	Internet
Functional Value to Organization	Provides means to connecting to databases; cloud servers; online teaching resources
Location	High School Server Room
Criticality/Sensitivity Classifications	Critical / Public
IS System/Server Name	DNS_Server
Data Owner	IT Director
Designated Custodian	IT Director
Granted Permissions	IT (R-W-X); Teachers (R); Students (R); Administration (R); HR (R); Finance (R)

Asset Name	Email Server/Files
Functional Value to Organization	Provides communication between all departments, vendors, parents, students
Location	High School Server Room
Criticality/Sensitivity Classifications	Vital / Confidential
IS System/Server Name	Email_Server
Data Owner	IT Director
Designated Custodian	IT Director
Granted Permissions	IT (R-W-X); Teachers (R-W-X); Students (R-W); Administrative (R-W-X); Finance (R-W-X)

Asset Name	Adobe Creative Suite Application/Files
Functional Value to Organization	Design of curriculum documents and informational/promotional notices for printing or to post online. Editing of photos for social media marketing purposes.
Location	3 rd party vendor
Criticality and Sensitivity Classifications	Nonsensitive / Public
IS System/Server Name	Online
Data Owner	Office Administrator
Designated Custodian	IT Director
Granted Permissions	Administration (R-W-X); IT (R-W-X); Students (R-W); Teachers (R-W-X)

Asset Name	Google Classroom Application/Files
Functional Value to Organization	Provides student resources (instructional videos), assignment management, and additional learning materials.
Location	3 rd party vendor
Criticality/Sensitivity Classifications	Nonsensitive / Public
IS System/Server Name	Online
Data Owner	Principal
Designated Custodian	IT Director
Granted Permissions	IT (R-W-X); Teachers (R-W); Students (R)

Asset Name	Xello for Teachers Application/Files
Functional Value to Organization	College and career readiness resource
Location	3 rd party vendor
Criticality and Sensitivity Classifications	Non-sensitive / Public
IS System/Server Name	Online
Data Owner	Principal
Designated Custodian	IT Director
Granted Permissions	Students (R); Teachers (R-W); IT (R-W-X)

APPENDIX C - CYBER-RELATED DISTRICT POLICIES

APPENDIX D – APPROVED SUPPLIERS

<u>Vendor Name</u>	<u>Product Type</u>	<u>Ed-Fi Version 3.x - (19/20)</u>	<u>Ed-Fi Version 3.x - (20/21)</u>	<u>Ed-Fi Version 5.x - (21/22)</u>	<u>Website</u>	Supported Feature
Blackbaud	Student Information System (Choice Only)	Certified	Certified	Certified	https://www.blackbaud.com	♣ Digital Equity on SIS. ♣ Student Identity Integration.
FACTS	Student Information System (Choice Only)	Certified	Certified	Certified	https://factsmgt.com	♣ Immunization Registry Integration ♣ Digital Equity on SIS ♣ Digital Equity on Parent Portal/Online Registration Forms. ♣ Racial and Ethnic Subgroups on Portal/OLR.
FastDirect Communications LLC	Student Information System (Choice Only)	Certified	Certified	Participating - Developing	https://www.fastdirectsis.com/	♣ Digital Equity on Parent Portal/Online Registration Forms. ♣ Digital Equity on SIS. ♣ Racial and Ethnic Subgroups on Portal/OLR.

Gradelink	Student Information System (Choice Only)	Certified	Certified	Certified	https://www.gradelink.com/	❖ Student Identity Integration.
Illuminate Education	Behavior& Discipline Systems	Certified	Certified	Certified	https://www.illuminateed.com/products/educlimber/	
Infinite Campus	Student Information System	Certified	Certified	Certified	https://www.infinitecampus.com/	❖ Digital Equity on SIS. ❖ Digital Equity on Parent Portal/Online Registration Forms. ❖ Course Transcript for Xello Integration. ❖ Racial and Ethnic Subgroups on Portal/OLR. ❖ Student Identity Integration. ❖ Immunization Registry Integration.
JMC Inc	Student Information System	Certified	Certified	Certified	http://www.jmcinc.com/	❖ Course Transcript for Xello Integration. ❖ Digital Equity on SIS. ❖ Digital Equity on Parent Portal/Online Registration Forms. ❖ Immunization

						Registry Integration. ❖ Racial and Ethnic Subgroups on Portal/OLR. ❖ Student Identity Integration.
JupiterEd	Student Information System (Choice Only)	Certified	Certified	Certified	https://www.jupitered.com/	❖ Student Identity Integration ❖ Digital Equity on SIS. ❖ Digital Equity on Parent Portal/Online Registration Forms. ❖ Racial and Ethnic Subgroups on Portal/OLR.
MS/EdD	Migrant Data System	NA	Read-Only	Read-Only	https://www.msedd.com/MIS2000	
National Heritage Academies	Student Information System	Certified	Certified	Certified	http://www.nhaschools.com	❖ Digital Equity on SIS. ❖ Digital Equity on Parent Portal/Online Registration Forms. ❖ Student Identity Integration.
Oasys LLC	Special Education	Certified	Certified	Certified	http://www.oasys-llc.com/	

	Information System					
OptionC Inc	Student Information System (Choice Only)	Certified	Certified	Certified	https://www.optionc.com/	❖ Digital Equity on SIS. ❖ Digital Equity on Parent Portal/Online Registration Forms. ❖ Racial and Ethnic Subgroups on Portal/OLR.
PowerSchool - BusinessPlus	School Finance Management System	NA	NA	Participating - Developing	https://www.powerschool.com/solutions/school-district-management-software/businessplus/	
PowerSchool - PowerSchool SIS	Student Information System	Certified	Certified	Participating - Developing	https://www.powerschool.com/solutions/student-information-system/powerschool-sis/	❖ Student Identity Integration. ❖ Course Transcript for Xello Integration. ❖ Digital Equity on SIS. ❖ Digital Equity on Parent Portal/Online Registration Forms. ❖ Racial and Ethnic Subgroups on Portal/OLR. ❖ Immunization Registry Integration.

Rediker Software Inc	Student Information System (Choice Only)	Certified	Certified	Participating - Developing	www.rediker.com	
SchoolSpeak Inc	Student Information System (Choice Only)	Certified	Certified	Certified	https://www.communitybrands.com/products/school-speak/	❖ Digital Equity on SIS. ❖ Digital Equity on Parent Portal/Online Registration Forms. ❖ Racial and Ethnic Subgroups on Portal/OLR.
SEEDS	Special Education Information System	Certified	Certified	Certified	http://www.cesa6.org/services/seeds/	
Skyward - Qmlativ Business	School Finance Management System	Certified	Certified	Certified	https://www.skyward.com/k-12/school-erp	
Skyward - Qmlativ Student	Student Information System	Certified	Certified	Certified	https://www.skyward.com/qmlativ	❖ Student Identity Integration ❖ Course Transcript for Xello Integration. ❖ Digital Equity on SIS. ❖ Digital Equity on Parent Portal/Online Registration Forms. ❖ Racial and

						Ethnic Subgroups on Portal/OLR. ✦ Immunization Registry Integration.
Skyward - Skyward's Business Suite	School Finance Management System	Certified	Certified	Certified	https://www.skyward.com/k-12/school-erp	
Skyward - Student Management Suite (SMS 2.0)	Student Information System	Certified	Certified	Certified	www.skyward.com	✦ Student Identity Integration ✦ Course Transcript for Xello Integration. ✦ Immunization Registry Integration. ✦ Digital Equity on SIS. ✦ Racial and Ethnic Subgroups on Portal/OLR. ✦ Digital Equity on Parent Portal/Online Registration Forms.
Specialized Data Systems - Web Financial Office	School Finance Management System	Certified	Certified	Certified	https://schooloffice.com/systems/	
Specialized Data Systems -	Student Information System	Certified	Certified	NA	http://www.schooloffice.com	✦ Digital Equity on SIS. ✦ Digital Equity

Web School Office						on Parent Portal/Online Registration Forms.
SpEd Forms	Special Education Information System	NA	Certified	Certified	https://spedforms.com	
Sycamore Education	Student Information System (Choice Only)	Certified	Certified	Certified	https://sycamoreeducation.com/	❖ Digital Equity on SIS. ❖ Digital Equity on Parent Portal/Online Registration Forms. ❖ Racial and Ethnic Subgroups on Portal/OLR.
TADS	Student Information System (Choice Only)	Certified	Certified	Certified	https://www.communitybrands.com/products/tads/	❖ Digital Equity on SIS. ❖ Digital Equity on Parent Portal/Online Registration Forms. ❖ Racial and Ethnic Subgroups on Portal/OLR. ❖ Student Identity Integration.
Tomah - Infinity	Student Information System	Certified	Certified	Certified	https://www.tomah.education/	

Tomah - Sundance	School Finance Management System	NA	Participating	Certified	https://www.tomah.education/	
Tyler Technologies - Munis®	School Finance Management System	NA	NA	Certified	https://www.tylertech.com/products/munis	
Tyler Technologies - Tyler SIS™	Student Information System	Certified	Certified	Certified	https://www.tylertech.com/solutions/k-12-education/student-information	♣ Digital Equity on SIS
Wiedenhammer	School Finance Management System	Certified	Certified	Certified	https://www.hammer.net/solutions/k-12-management-software/	
Xello	College & Career Readiness Software	Read-Only	Read-Only	Read-Only	https://xello.world/en/	

*Legend - WISEdata Ed-Fi Certification Status

<u>Participating</u>	• One or more of the following criteria have been met by the vendor: • - Regular attendance on monthly vendor calls held by DPI • - Vendor development team is interacting with DPI on a regular basis via email, phone calls, etc. • - Vendor responds to DPI questions and requests for status updates
<u>Participating-Developing</u>	• DPI is seeing vendor activity in the last 3 months in the vendor UAT sandbox environment
<u>Participating-Certification Testing</u>	• Integration testing scheduled with DPI, or Integration testing with DPI is in process
<u>Certified</u>	• Vendor has passed Wisconsin DPI integration tests for all or at least data domains required to be submitted to Wisconsin DPI via Ed-Fi integration. • Note: Choice-only vendors and specialized vendors are not required to complete integration on all possible WI DPI Ed-Fi data domains either because they cannot support some domains or all domains are not needed because of LEAs supported.
<u>Read-Only</u>	• Vendor is only reading data from WISEdata (LEA has to authorize) to pull into their software; no create, update or delete of data in WISEdata. See 'Vendor Notes' column for more detail.
<u>Not Participating Yet</u>	• A new major Ed-Fi release is available to begin development. Vendor hasn't participated in use case reviews, other release meetings and / or acknowledged they have begun analysis on the implementation. This could change, but at this time this is the status of the vendor's participation.