Indicators of Digital Readiness

Indicator	**Operational Best Practices**
Theme	**Technology Support and Services**
Priority Level	**P1**
Organizational Level	**District**

Description of the Indicator

District has formally adopted/implemented “best practices” and system-hardening standards for preventing unauthorized access to data and data systems wherever possible. District requires and has documented that any data or data systems hosted by third party organizations and vendors meet District’s security practices.

Why is this indicator important?

In order to safeguard student and staff data privacy it is critical to ensure best practice security standards are in place to limit/prevent unauthorized access to systems. Documenting these practices and formalizing them in the form of “Standard Operating Procedures” or “Security Policies” promotes awareness and ensures operational consistency/continuity.

Indicator Rubric

Insufficient Evidence of Implementation **(0 Points)**	● Internal policies and procedures exist but no gap assessment has been conducted and practices have not been evaluated or aligned to widely-accepted best practices/standards
Foundational Stage of Implementation **(3 Points)**	● Policies and procedures have been formalized in an operations manual or security policy ● Gap assessment has been conducted but no corrective action has been taken to align current practices with standards
Achieving Success in Implementation **(6 Points)**	● A comprehensive security policy and operations manual exists documenting best practices, procedures and policies ● Aligned to widely-accepted best practices or standards based on the results of a gap assessment
Exemplary Success in Implementation **(9 Points)**	● A comprehensive security policy and operations manual exists documenting best practices, procedures and policies ● Aligned to widely-accepted best practices or standards based on the results of a gap assessment, which is updated at least once per year ● Practices are shared with the school community in conjunction with training to raise awareness of cybersecurity risks and promote responsible use

Who in the school/district should lead and be involved with this indicator?

- Technology Director/Coordinator
- Security Director/Coordinator

How to execute the indicator

- Identify and prioritize in-scope systems.
- Conduct a security assessment to determine potential threats to, vulnerabilities of and any legal/regulatory requirements that must be met.
- Document current policies, practices and procedures regarding:
    - Management/configuration of firewalls, routers and other network components
    - Diagrams and documentation of network connections and data flows, including any BYOD/open wireless networks**.**
    - Network segmentation
    - Configuration/Maintenance of servers and computer systems
    - Deployment/configuration of antivirus/malware detection and removal software

    - Encryption of data while in motion and at rest
    - Storage, disposal and retention of data
    - System backups and disaster recovery
    - Access control/User account management*
    - Regular testing of security systems and processes including but not limited to vulnerability testing, penetration testing and rogue network/device detection
    - Physical security of data systems/servers and other network components such as wireless access points, switches and active network jacks
    - Network and system monitoring
- Using system-hardening standards (PCI, NIST, SANS, etc.), determine, analyze and prioritize gaps by comparing current practices with recommendations/requirements.
- Create an action plan to address gaps that includes a projected timeline/due date, resources needed and associated costs, if any.
- Conduct gap assessment annually, or as changes are made, to ensure alignment with current standards.

*Expanded example for access control/user account management:

- Ensure all users have unique accounts/credentials for accessing computer systems and network resources.
- Limit user access via group policy or other access control measures with a default "deny all".
- Limit creation, modification or deletion of user accounts to only assigned/authorized personnel.
- Immediately revoke access for terminated employees.
- Remove/disable inactive accounts within 90 days.
- Limit accounts/credentials for third parties to only during specific time periods necessary.
- Lock out user accounts after not more than 10 repeated access attempts.
- Set minimum lockout duration to 30 minutes.
- Require re-authentication for all user accounts after idling for 15 minutes.
- User account passwords use a minimum of 8 characters and contain both numeric and alphabetic characters.
- Passwords must be reset at least once every 90 days.
- Multi-factor authentication enabled and highly recommended whenever available, especially for Administrators, Confidential Secretaries and other staff in the Business Office/Purchasing/Payroll, Technology and Human Resources/Personnel Departments.
- Provide guidance on choosing strong passwords, protecting credentials and changing passwords.
- Limit/avoid use of shared or generic accounts/credentials.

Evidence to submit for successful execution of this action

- Network Operations Manual and/or Security Policy
- Standard Operating Procedures
- Gap Assessment
- Action Plan

Resources schools can use to complete this action successfully

- Center for Internet Security (CIS)
- SANS Institute
- PCI Security Standards Council

Certified Schools Exemplars

1. **Mountain Way School, Morris Plains School District, 2018 Silver Certified**

   MPSD has adopted and implemented operational best practices to protect and secure data and data systems. The district conducts security assessments regularly to identify areas of weakness and potential threats in alignment with legal and regulatory requirements. Precise documentation is kept with regard to policies, practices, and procedures for management and configuration of firewalls, routers, and all related network components. As a 1:1 district in grade 2-8, precise diagrams and documentation connections and data flows are kept for both district owned devices as well as that which connects to the guest network. The network is properly segmented to allow for more restricted access for identified users. Proper systems are in place to ensure access control management, deployment of antivirus/malware detection and removal software, encryption of locally hosted data, system backups and recovery plans, etc. MPSD uses NIST to effectively identify gaps and improve practices. Action plans, both short term and long range are developed by the Technology Leadership Team to prepare both operationally and fiscally for necessary updates and improvements. Annual assessments and reviews are conducted to continually improve upon operational practices.

2. **Demarest Middle School, Demarest, 2018 Bronze Certified**

   The Demarest school district has several documents in place outlining the physical security of the technology equipment used throughout the district. There are also Board of Education policies in place that detail the appropriate use of technology and Internet for both staff and students. Students and staff are given detailed instructions up on the receipt of their laptops to change their passwords, using Google's directions for strong passwords. Additionally, there is a procedure in place for deactivating student and staff accounts when they are no longer in district.

3. **East Hanover Middle School, East Hanover School District, 2018 Bronze Certified**

   The East Hanover School District has taken careful action to insure the safety and security of all members of our schools and community while utilizing district networks. The District has adopted a number of board policies that strongly support the integration of safe computing practices and the maintenance of a safe digital environment for staff and students. The district has adopted a one to one chromebook policy that very clearly details safe computing practices on the chromebook for parents and students. In addition, we have adopted a three year technology plan that further supports the continued implementation of safe computing practices. Finally, the district has a set plan based on conducted research to implemented before, during and after there is a breach in cyber security. We taken the careful use of our network and technologies very seriously and support safe computing consistently across the district.

4. **Hackensack High School, Hackensack School District, 2018 Bronze Certified**

   The District Digital Learning Committee has focused heavily on data privacy and security over the past year and a half, which culminated in the development of the District Data Privacy and Security Policy. This policy sets guidelines, expectations and standards for how District data is used, collected, stored, shared and viewed. Privacy and security information, alerts and tips are distributed to staff through the District Resource Portal, email and PD. Security awareness training is also a component of the New Teacher Orientation training

5. **Hazlet Middle School, Hazlet Township Public Schools, 2018 Bronze Certified**

   Our district maintains consistent network and tool operations through a series of best practices, evidenced by our district network design and policy guidelines. The system is protected using network and system monitoring procedures,

processes for backups and disaster recovery, regular maintenance and usage reports (i.e. gap assessment), and standard operations to remediate failures of the system.

6. **Lincoln Annex School, New Brunswick, 2018 Bronze Certified**

The district has a "Standard Operating Procedures and Internal Controls" document that Action Plan outlines plans and procedures for facility use, accounting protocols, security and emergency guidelines, and safety controls. The district also has a policy manual that outlines protocols for all departments and sub departments. The Technology Department has also commissioned a Vulnerability and Risk Assessment to identify areas that may need to be addressed in the area of cyber security.

7. **West New York Middle School, West New York, 2018 Bronze Certified**

The West New York Board of Education's Information Systems Department has always focused on operational best practices to ensure the safety of all of its users. The process for procuring hardware and software or any type of infrastructure always starts with ensuring best practices are followed based on security standards. The Information Systems Department conducts an internal yearly review all of user accounts and systems. Any security gaps found are corrected immediately. Additionally, we pay for our Student Information Systems (PowerSchool) Enterprise Management Service which provides an additional layer of security based on the services provided. The District is also a member of COSN and uses their tools regarding best practices. One example is, what type of questions to ask vendors regarding their handling of our District data. One of the biggest lessons we have learned over the years, is that the biggest gap in security is the Human Factor. Humans are always prone to Social Engineering and bad habits. For that reason, the District initiated a Cybersecurity Awareness program for the 2017 - 2018 school year. Through this program, we have seen an increase in awareness throughout the District. We plan to continue this program for many years to come. For more details regarding this program, please see the information provided in the Staff Awareness indicator.

8. **Indian Mills Memorial School, Shamong School District, 2018 Bronze Certified**

Comprehensive operational plans are essential in today's K-12 environment. State and educational institutions are constantly receiving cyber attacks and therefore incorporating policy and procedures helps to reduce valunabilites. Indian Mills Memorial School is a victim of a DDos cyber attack and knows first hand how important operational best practices are. In 2016 an independent security audit at Indian Mills Memorial School was conducted because of a cyber attack that directly targeted the school. Several reputable tools were utilized in the independent security scan, such as, NeXpose Vulnerability Scanner and Metasploit Pro. The results of this audit prompted immediate actions with a the creation of an Operations Manual. Procedures, policy changes/additions, and action plans to circumvent current issues are included in the Operations Manual. Additionally, a list of best practices with implemented and recommended actions in each category are presented. The full security report incorporates sensitive information but more detail can be made available if needed.