Lower Merion School District
ADMINISTRATIVE REGULATIONS

Administrative Regulation No.:	832
Section:	OPERATIONS
Title:	CYBERSECURITY AND DATA BREACH RESPONSE
Date Adopted:	3/31/23
Date Revised:	

R832 CYBERSECURITY AND DATA BREACH RESPONSE

Purpose and Benefits

This Administrative Regulation defines the mandatory minimum information security requirements for the Lower Merion School District.

Failure to secure and protect the confidentiality, integrity, and availability of information assets in today's highly networked environment can damage or shut down systems that operate mission critical services in the accomplishment of the Lower Merion School District's goals.

This administrative regulation benefits Lower Merion School District stakeholders by identifying an information security framework that will assure appropriate measures are in place to protect the confidentiality, integrity and availability of data and critical services; and assure staff and all other stakeholders have adequate knowledge of security policy, administrative regulations, procedures, and practices and know how to protect information.

This administrative regulation encompasses all systems for which the Lower Merion School District has administrative responsibility, including systems managed or hosted by third parties on behalf of the Lower Merion School District.

Scope

This policy acts as an umbrella document to all other information security policies and administrative regulations. This policy defines the responsibility to:

1. Protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;

    a. The Information Systems Department will identify and adopt a security framework, such as the Center for Internet Security (CIS) Critical Security Controls.
    b. Implementation and maintenance of the information security framework will be reported annually to the Board of School Directors.
    c. Any system or process that supports business functions must be appropriately managed for information risk and the information security framework will be applied as appropriate.
    d. Information security risk assessments are required for new products that contain or process confidential or sensitive employee or student data, implementations of new

technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.

e. Risk assessment results, and the decisions made based on these results, must be documented.

2. Manage the risk of security exposure or compromise;

   a. All systems are subject to periodic penetration testing or vulnerability scanning.
   b. The results of penetration tests and vulnerability scanning will be reviewed in a timely manner with the system owner.
   c. Appropriate actions, such as patching, replacing the system, or applying compensating controls will be taken to address discovered vulnerabilities.
   d. Any penetration testing and vulnerability scanning must be conducted by individuals who are authorized by the District, such as authorized penetration testers and the Information Systems Department Information Security Analyst.
   e. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

3. Assure a secure and stable information technology (IT) environment;

   a. The intersection of information security, disaster recovery, and business continuity will be examined and developed.
   b. Ongoing patching, upgrades, and systems replacements will be performed on client, server, and network devices at times that minimize disruption.
   c. All penetration testing and vulnerability scanning will be conducted at times to minimize possibility of disruption.
   d. Out of band backups will be maintained for purpose of disaster recovery, and tested annually to ensure successful recovery operations.
   e. Out of band backups will be maintained for purpose of disaster recovery, and tested annually to ensure successful recovery operations.

4. Identify and respond to events involving information asset misuse, loss or unauthorized disclosure;

   a. The Lower Merion School District must have an incident response plan to effectively respond to information security incidents.
   b. All observed or suspected information security events or weaknesses are to be reported to a supervisor or an Information Systems Department member as quickly as possible.
   c. The Information Systems Department Information Security Analyst must be notified of any information systems events that may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.
   d. The Information Systems Department will conduct annually an incident response exercise.

5. Monitor systems for anomalies that might indicate compromise; and

    a. The Information Systems Department will identify and implement a security information and event management (SIEM) product(s) that will aggregate system, network, and cloud logs, provide visibility into system, network, and cloud activity in order to identify anomalous events and indicators of compromise.
    b. The Information Systems Department will identify and implement end point antivirus, endpoint detection and response (EDR), and network monitoring services that will provide alerts of potential compromises or provide logs to the SIEM that will correlate and generate alerts.

6. Promote and increase the awareness of information security.

    a. Employees and outsource workforce must receive general security awareness training within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to specific Lower Merion School District sensitive and confidential information not covered in the general security training. All security training must be reinforced at least annually and must be tracked by the Lower Merion School District.
    b. Require employees to abide by the Staff Access to and Use of Information Technology Resources Policy 350, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.
    c. Employee supervisors are responsible for ensuring all issued property is returned prior to an employee's separation;
    d. Employee accounts will be disabled and access removed immediately upon official separation from Lower Merion School District.

<u>Functional Responsibilities</u>

1. District administration is responsible for:

    a. evaluating and accepting risk on behalf of the Lower Merion School District;
    b. identifying information security responsibilities and goals and integrating them into relevant processes;
    c. supporting the consistent implementation of information security policies and standards;
    d. supporting security through clear direction and demonstrated commitment of appropriate resources;
    e. promoting awareness of information security best practices through the regular dissemination of information security training and materials;
    f. participating in the response to security incidents;
    g. communicating requirements of this policy and administrative regulation, including the consequences of non-compliance, to employees, students, and third parties.

2. The Information Systems Department is responsible for:

    a. maintaining familiarity with business functions and requirements;
    b. establishing and maintaining enterprise information security policy and administrative regulation;
    c. assessing compliance with information security policies and legal and regulatory information security requirements;
    d. evaluating and understanding information security risks and how to appropriately manage those risks;
    e. advising on security issues related to procurement of products and services;
    f. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;
    g. providing timely notification of current threats and vulnerabilities to appropriate parties;
    h. promoting information security awareness;
    i. recommending a cybersecurity framework for district to adopt to guide district cybersecurity goals;
    j. developing the security program and strategy, including measures of effectiveness;
    k. providing incident response coordination and expertise;
    l. monitoring services, systems, and networks for anomalies;
    m. maintaining ongoing contact with security groups/associations and relevant authorities, such as the FBI;
    n. providing awareness materials and training resources.
    o. providing training to appropriate technical staff on secure operations;
    p. maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security;
    q. implementing business continuity and disaster recovery plans.

3. The workforce is responsible for:

    a. understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of data and information;
    b. protecting information and resources from unauthorized use or disclosure;
    c. protecting confidential and sensitive information from unauthorized use or disclosure;
    d. abiding by *Policy 350 - Acceptable Use of Information Technology Resources*;
    e. reporting suspected information security events or weaknesses to an appropriate manager or a member of the Information Systems Department.