NEW GUIDELINE - TECHNOLOGY UPDATE

INFORMATION SECURITY INCIDENT MANAGEMENT

This administrative guideline governs the reporting and management of security incidents involving the District's Information of security incidents involving the District's Information Resources (as defined in Bylaw 0100).

Every Board of Education member, staff member/employee, student, parent, contractor/vendor, and visitor to school property who accesses District-owned or managed information through computing systems or devices ("users") must report information security incidents (as defined below) promptly per the procedures described herein.

When an information security incident involves District Confidential Data/Information (as defined below) or mission critical devices (as defined below), the Superintendent/Technology Director/District's Information Technology Office may, in coordination with the District's Security Office, direct the incident response and investigation. The Technology Director is authorized, in conjunction with the Superintendent, to take any action necessary to mitigate the risk posed by the information security incident.

An employee who puts District Confidential Data/Information at risk as a result of his/her failure to adhere to relevant policies/administrative guidelines/the law may be subject to disciplinary consequences, up to and including termination of employment and/or referral to law enforcement. Students who fail to adhere to applicable policies/administrative guidelines/the law will be referred to school and/or District administration for review and determination of the consequences of their actions, including referral to law enforcement. Contractors and vendors who fail to adhere to applicable policies/administrative guidelines/the law may face termination of their business relationships with and/or legal action by the District. Parents and visitors who fail to adhere to applicable policies/administrative guidelines/the law may be denied access to District Technology and Information Resources and/or referral to law enforcement. Violations can in some cases also carry the risk of civil or criminal penalties.

The Technology Director is responsible for establishing and maintaining an up-to-date information security management plan.

[NOTE: SELECT OPTION #1 or OPTION #2]

[x] [OPTION #1]

The school site administrator (e.g., the Principal) or the District-wide department administrator, along with the Tech Specialist [or equivalent], are responsible for reporting information security incidents at their site.

[END OF OPTION #1]

[ ] [OPTION #2]

The plan shall identify the primary and secondary information security contact for each school and Central Office/District-wide department (e.g., Human Resources, Treasurer/payroll, Business Services, Student/Pupil Services). Any unique requirements concerning a specific building or department must be delineated in a subsection of the plan that is particular to the given building or department.

[END OF OPTION #2]

Definitions

A. **Incident Management Plan**

The IT Department, in conjunction with Department/Division/Building Leaders, must develop and maintain a plan that contains procedures on how to handle information security incidents, including contact information for site/unit personnel with responsibility for responding to the incident, plans to contain an incident, and procedures on how to restore information.

B. **Information Security Incident**

Includes any incident that is known or has the potential to negatively impact the confidentiality, integrity, or availability of District information/data. This can range from the loss of a laptop, tablet or other mobile/portable storage device, the virus infection of an end-user workstation, or a breach of a District system by a hacker.

C. **Mission Critical Resource**

Includes any resource that is critical to the mission and operation of the District and any device that is running a mission critical service or stores District Confidential Data/Information. Mission critical services must be available. Mission critical resources for information security purposes include, for example, information/data assets, software, hardware, and facilities related to Human Resources, Finance, Student Information Services, Payroll, e-mail).

D. **District Confidential Data/Information**

Includes all data, in its original and duplicate form, that contains:

1. "personal identifying information", as defined by State and Federal laws;

   This includes employer tax ID numbers, drivers' license numbers, passport numbers, SSNs, State identification card numbers, credit/debit card numbers, banking account numbers, PIN codes, digital signatures, biometric data, fingerprints, passwords, and any other numbers or information that can be used to access a person's financial resources.

2. "protected health information" as defined by the HIPAA;

3. student "education records", as defined by the Family Educational Rights and Privacy Act (FERPA) and State law (R.C. 3319.321);

4. information that is deemed to be confidential in accordance with the Michigan Public Records Act.

(x) "card holder data", as defined by the Payment Card Industry (PCI) Data Security Standard (DSS).

Adherence to the procedures outlined below will streamline the handling of information security incidents and minimize the timeframe during which District Confidential Data/Information and mission critical resources are left in a vulnerable state.

Incident Reporting

Given the risks associated with information security incidents, as well as implications for the District related to compliance with Federal and State regulatory requirements, it is essential that school site administrators and District department administrators be aware of information security issues and their responsibilities for reporting and mitigating information security risks.

School site administrators and District department administrators who manage business units that maintain and manage their site's information resources must designate employees as primary and back-up information security contacts, provide the District's Information Technology Director with the names and contact information of these individuals, update this information whenever it changes, and verify that these contacts are trained by the District's Technology Office to perform their duties.

Each information security contact shall serve as an intermediary between his/her respective District site or office and the District's Information Technology Office and must assist the site or office s/he serves in implementing information security policies and information security initiatives including training of site staff and in responding to data breach incidents, all in close coordination with the District's Information Technology Office.

Every technology user, including Board members, staff members/employees, students, parents, contractors/vendors, and visitors to campus, who has access to Board-owned or managed information resources and who suspects that there may have been an information security incident (ranging from a lost or stolen laptop, tablet or other mobile/portable storage device, the virus infection of an end-user work station, or a major intrusion by a hacker) must promptly report the incident to his/her Principal or director/manager and/or the information security contact for that unit/site.

The information security contact's roles and responsibilities include, but are not limited to:

A. serving as a single point of contact for the District's Information Technology Office regarding security efforts and information security incidents that affect District sites;

B. aiding the District's Information Technology Office in improving information security in the District by coordinating with them on security matters;

C. working with the District's Information Technology Office on incident management and response as well as assist the District's Information Technology Office, as needed, in certain activities including coordinating the following with the District's Technology Office:

1. ensuring proper identification and classification of mission critical devices and Technology Resources storing District Confidential Data/Information within their school site or business unit/department;

2. advising and training their site's administration, faculty, and staff on the implementation of appropriate security controls for Technology Resources (as defined in Bylaw 0100) and Information Resources;

3. meeting periodically with the District's Information Technology Office to move forward District security initiatives for their respective sites;

4. maintaining an up-to-date list of staff/users with access to District Confidential Data/Information and Controlled Data/Information in their working group and promptly notify District's Information Technology Office of any personnel changes, including transfers within the District;

5. providing basic security advice for all assigned systems and users within their site;

6. ensuring timely compliance with security awareness requirements, including appropriate refresher training and training of new employees;

   In consultation with the Principal, the contact will oversee the site's compliance with applicable State and Federal laws as well as Board policies regarding District Confidential Data/Information.

7. ensuring that any detected vulnerabilities are remediated in a timely manner;

8. advising their site regarding the implementation of appropriate security controls consistent with the District's information security policy;

9. collecting incident response information;

   The contact must provide a timely notification of the District's Information Technology Office regarding any information security incidents for their respective site consistent with the incident management procedure. In addition, the contact must provide a timely and comprehensive response to information security incidents in coordination with the District's Information Technology Office.

10. coordinating with the District's information security strategic initiatives.

Each information security incident will be classified accordingly to the following "levels":

Incident Level	Examples	Investigation Type
Level 1	Violation of Board policies and administrative guidelines that relate to technology and information security.	Basic investigation of an incident.
	A virus or malware detection.	Remediation advice for an incident is provided.
		Device isolation, if necessary.
Level 2	Unauthorized computer/network access, misuse, or user permission issue. Computer/system theft, damage or loss. Malicious Denial of Service Attack or other attempt to interrupt normal operations.	Investigation of the incident.
		Notification will be provided if applicable pursuant to AG 8305C.

Level 3	Hacking or system breach to core/mission critical systems. Unauthorized release of District Confidential Data/Information.	Investigation of a likely or confirmed breach of a system processing/storing District Confidential Data/Information or a mission critical system. Investigation of information technology relevant issues performed in support of criminal or civil cases, as well as District internal investigations. Notification will be provided if applicable pursuant to AG 8305C.

In the event of a possible Level 2 or 3 information security incident, the user or administrator of the potentially compromised system or device should work with the site's information security contact to preserve all evidence, including leaving the possibly compromised machine powered up and online, and refraining from accessing the system or machine in any way. The information security contact will then report the incident to the District's Information Technology Office and/or Security Office. The District's Information Technology Office and the Security Office will advise how best to proceed for purposes of preserving evidence and constructing an audit trail for the investigation of the incident. As appropriate, the District's Security Office will coordinate with public safety and law enforcement officials.

The Superintendent will coordinate all external communications with the media or the public related to any information security incident.