CYBER SECURITY PROTOCOL

The following protocols are established in accordance with the Lincoln Public Schools Cyber Security Policy and are designed to take a variety of actions to prevent, protect the school community from, mitigate the effects of, respond to, and recover from cyber threats that occur in the form of ransomware attacks, data breaches, DDoS attacks, website and social media defacement, online class and school meeting invasions, and any other cyber threat directed at the education digital infrastructure.

1. SAFEGUARDS TO PREVENT CYBER SECURITY INCIDENTS

    a. The entire school community, consisting of all staff, students, and parents, must accept a Lincoln Technology Acceptable Use Acknowledgement in writing. This Acknowledgement must be accepted at the beginning of the school year and must be accepted every school year. The acknowledgments will be kept on record at the Central Office or at the school of record.

    b. Informational Technology (“IT”) staff must participate in a PD session before the school year begins reviewing any new local, state, and federal statutes and regulations regarding information security, privacy, and storage of sensitive information.

    c. IT staff will train all school staff members in using the Multi-Factor Authentication Process (“MFA”) the Lincoln Public Schools has chosen to utilize at the beginning of the school year and at least one other time later in the school year.

    d. All employees must use the MFA Process as directed by the IT Specialist or the Superintendent.

    e. IT staff will conduct either a Lincoln Public Schools-wide or school-specific PD session covering important elements of Cyber Safety for staff and students at least annually.

    f. IT staff will conduct an inventory of all assets (end-user devices, network devices, non-computing/ Internet of Things (IOT) devices, and servers) connected to the digital infrastructure physically, virtually, remotely, and those within cloud environments to accurately know the totality of assets that need to be monitored and protected.

    g. IT staff will identify any unauthorized or unmanaged assets to remove or remediate. A record of the totality of assets will be kept by an IT Specialist, and this record will be revised periodically.

    h. IT staff will actively manage (inventory, track, and correct) all software, including operating systems and applications, on the network so that only authorized software is installed and can execute and that any unauthorized and unmanaged software is found and prevented from installation or execution.

i. IT staff must conduct a cyber security risk assessment at the beginning of the school year to help the school understand the cybersecurity landscape to which the school is exposed.

j. IT staff must establish a system to securely store data to ensure that the whole school community's data is kept private and to comply with FERPA. When possible, to mitigate cyber risk, data will be moved to a cloud-based system. IT staff will prioritize high-impact targets, such as mail systems and identity services.[1]

k. IT staff will ensure that each school is regularly backing up their data in case of accidental or deliberate corruption or destruction of data.

l. Each school must create firewalls that act as a security barrier between a trusted internal network and an untrusted external network. These firewalls must monitor and filter incoming and outgoing network traffic to prevent unauthorized access by blocking malicious data while allowing legitimate traffic to pass through. The IT team will utilize the federally funded Protective Domain Name Service ("PDNS") and any other additional tools the IT Specialist deems appropriate to assist with preventing unauthorized access to the Lincoln Public Schools network and systems. All services and tools utilized by Lincoln Public Schools will satisfy all requirements pursuant to the Children's Internet Protection Act and R.I. Gen. Laws § 16-21.6-1 and adhere to Lincoln Public School's Internet Filtering Policy.

m. IT staff will establish processes and tools to create, assign, manage and revoke access credentials and privileges for user, administrator, and service accounts for Lincoln Public Schools assets and software.

n. IT staff must create an approved list of individuals who have access to the school Lincoln Public Schools or individual school's networks and systems. This list must be regularly reviewed to ensure that only those individuals who have permission to access the systems can do so. IT staff will limit administrative rights for each district asset to IT staff, IT Specialist, and any other school administrators the IT Specialist deems should have administrative rights.

o. The Lincoln Public Schools must monitor networks continuously to reduce the risk of cyber threats. To increase monitoring, detection, and protection capacity, the school will utilize dedicated cybersecurity incident response resources at the local, state, or regional level.

[1] Identity services are cloud-based services that manage user identities and access controls across different applications and systems.

p. IT staff will collect, review, and retain audit logs of events that could help detect, understand, or recover from an attack. These logs will be under the control of the IT Specialist.

q. Each year, the Lincoln Public Schools will assess whether the cyber insurance the Lincoln Public Schools pays for is adequate and whether coverage should be increased.

r. IT staff will periodically practice exercising response plans so that the staff can strengthen their capacity to respond effectively during a cybersecurity incident and identify vulnerabilities in the response plans. This may include simulating the objectives and actions of an attacker.

2. ACTION STEPS DURING A CYBER SECURITY INCIDENT

a. When there is a suspected malware/spyware attack, IT staff will attempt to isolate the attack from the Network by turning off the WIFI and/ or unplugging the network cable. IT staff should not turn off the device, as it is possible all backups and shares on the Network are affected.

b. IT staff will effectively report the cybersecurity incident. First, an IT staff member will alert the IT Specialist, who will coordinate the incident response. The IT Specialist will then contact the School Business Administrator, who will coordinate legal and insurance actions, and the IT Specialist will contact the Assistant Superintendent, who will coordinate any public relations actions related to the cyber security incident.

c. The IT Specialist will dictate the necessary steps to mitigate the incident and will communicate the incident to the building principal.

d. The IT Specialist, with the help of Building and Lincoln Public Schools Administrators, will limit any damage to the digital infrastructure and preserve sensitive information by responding quickly. The IT Specialist will determine if the incident can be mitigated by utilizing Lincoln Public Schools resources or whether outside assistance is required. This outside assistance may come in the form of local, state, or federal authorities or agencies or a private vendor.

e. The IT Specialist will notify the Multi-State Information Sharing and Analysis Center (MS-ISAC) and/ or Department of Health or any other necessary agency as needed, as well as any individuals whose personal information may have been compromised.

f. The IT Specialist will communicate when the incident has been contained to the Building Administrator and the Superintendent.

3. ACTION STEPS AFTER A CYBER SECURITY INCIDENT

    a. Once an incident has been contained, the Lincoln Public Schools will follow protocols for recovery.

    b. IT staff will work with building and Building Administrators to restore continuity of operations as quickly as possible, including but not limited to communication systems and computer systems to avoid school closure and learning disruptions.

    c. IT staff will rebuild any compromised digital infrastructure from the core out, starting with the fundamental computer systems and network systems.

    d. IT staff will identify any victims of the cybersecurity incident and connect them to relevant support services. This may include IT staff communicating to Building Administrators which staff or students were directly affected. This may require Building and/or Lincoln Public Schools Administration to communicate with staff and parents the nature of the cyber security threat.

    e. IT staff will identify and address any temporary or permanent damage to digital infrastructure and evaluate and remedy the system for any exploited vulnerabilities.

    f. Once the cybersecurity threat has been resolved and IT staff are confident the digital infrastructure is repaired and the exploited vulnerability is remedied, they will conduct, under the leadership of the IT Specialist, an after-action review and create an after-action report. This review should be conducted and the subsequent report written as soon as possible so that the experience is still fresh in the minds of the IT team. This process will allow IT staff to evaluate its response to the cybersecurity incident, document any gaps and strengths in the digital infrastructure, and plan to enhance any security to address any issues that arose.

Second Reading Approved:
Approved: