Non-Instructional/Business Operations

SUBJECT: DATA NETWORKS AND SECURITY ACCESS

The District values the protection of private information of individuals in accordance with applicable law, regulations, and best practice. Accordingly, district officials and information technology (IT) staff will plan, implement, and monitor IT security mechanisms, procedures, and technologies necessary to prevent improper or illegal disclosure, modification, or denial of sensitive information in the district computer system (DCS). Similarly, IT mechanisms and procedures will also be implemented in order to safeguard district technology resources, including computer hardware and software. District network administrators may review district computers to maintain system integrity and to ensure that individuals are using the system responsibly. Users should not expect that anything stored on school computers or networks will be private.

In order to achieve the objectives of this policy, the Board entrusts the Superintendent or designee to:

a) Maintain inventories of computer hardware, software, and data, to include:

   1. Computer hardware - physical description, person assigned to, physical location, and relevant purchase or lease information;

   2. Software - description of item, locations installed, and pertinent licensing information;

   3. Data - classification based on district data classification scheme, and location where data resides.

b) Regularly update inventories

c) Install and maintain antivirus software on all district devices. Antivirus software should be set to update definitions daily and to scan for threats throughout the day. Hardware should be set to force scans of all newly connected devices;

d) Ensure that software patches and updates are installed in a timely fashion to address potential weaknesses in out-of-date software;

e) Develop procedures for promptly disabling accounts of former employees and for ensuring that former employees cannot access district systems and accounts;

f) Develop password standards for all users that adhere to current industry standards for password security;

g) Periodically review user access rights to the network and to specific software applications to ensure that users are given access only to those resources necessary for their job duties;

(Continued)

SUBJECT: DATA NETWORKS AND SECURITY ACCESS (Cont'd.)

h) Establish policies for remote access, which should include eligibility and security requirements (MFA), District expectations, and provisions to monitor and control remote access;

i) Utilize a firewall configured to allow only communication types necessary for system operation and to explicitly deny all other communications. Such firewall logs should be monitored for potential security and resource issues, including for intrusion detection;

j) Develop procedures to control physical access to computer facilities, data rooms, systems, networks, and data, ensuring adequate physical security commensurate with the risks of physical damage or access;

k) Develop an IT contingency plan appropriate for the size and complexity of district IT operations to ensure continuous critical IT services in the event of any sudden, catastrophic event, including, but not limited to fire, computer virus, or deliberate or inadvertent employee action.

Adopted: 5/18/15
Reviewed with no changes: 9/9/24
Revised: 2/9/26