Gainesville ISD Cybersecurity Policy

All cybersecurity beaches are to be immediately reported to the GISD Technology Director (designated GISD Cybersecurity Coordinator), Jennifer Coleman.

I. Authentication and Access Control

a. Authentication is managed by use of Microsoft Active Directory and authorization by Active Directory group membership.

b. A robust firewall, content filter, and virus protection appliances are monitored, maintained, and updated daily to manage traffic, content, and prevent intrusion, breaches, or compromised data.

c. To reduce risks associated with account compromise, accounts are assigned the minimal security rights needed for the user.

d. Account resets and Help Desk requests are logged and monitored for potential abuse or attacks.

e. A tiered password policy allows different groups of users, including staff and students, to have different requirements for password complexity based on position and level of data access.

f. District acceptable use policies define what is suitable for each group to use and access, including digital citizenship, as well as accountability for actions online.

II. Physical Security

a. Physical access to data centers and controls rooms are locked and monitored.

b. Centralization of a primary data center has been moved to a secure, off-campus location.

c. Monitor and control temperature and moisture in MDF and IDF locations.

III. Incident Response

a. Phase 1: Determine the scope of the incident and which systems and users are affected.

b. Phase 2: Mitigate the incident while preserving evidence for further analysis.

c. Phase 3: Recover, as needed, including restoring from backup, eradicating a virus, or containing a vulnerability.

d. Phase 4: Report and review using Help Desk documentation.