Hillcrest School District

IT SECURITY POLICY

Security Management
Commissioner's Memo: RT-15-010

Arkansas. A State of Technology.

Arkansas Department of Education

1. SECURITY MANAGEMENT

1A. Policy Statement

District management and IT staff will plan, deploy and monitor IT security mechanisms, policies, procedures, and technologies necessary to prevent disclosure, modification or denial of sensitive information.

1B. Standards

1B1 Security Responsibility

- **Hillcrest School District** shall appoint, in writing, an IT Security Officer (ISO) responsible for overseeing District-wide IT security, to include development of District policies and adherence to the State-wide (ADE) standards defined in this document.

- **Hillcrest School District** shall ensure that the job description and annual performance evaluation for the appointed ISO identifies IT security responsibilities.

1B2 Data Sensitivity

- **Hillcrest School District** shall recognize that "sensitive data" identified within this Standard is considered any and all student and employee data which is considered personally identifiable information (PII) or any non PII information which assembled together would allow a reasonable person to identify an individual. Sensitive data includes, but is not limited to:
  - Student personally identifiable information, except as allowed by the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99).
  - Employee personally identifiable information, except as required by Ark. Code Ann. § 6-11-129.

1B3 Training

- **Hillcrest School District,** led by the ISO, shall ensure that all District employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information.
  - Training resources will be provided to all District employees.

- **Hillcrest School District**, led by the ISO, shall ensure that all Parents and Students are informed of Cyber Security Awareness. A web link to this information is located on the Parent's page of the school's website.

2. PHYSICAL SECURITY

2A. Policy Statement

Physical access to computer facilities, data rooms, systems, networks and data will be limited to those authorized personnel who require access to perform assigned duties.

2B. Standards

2B1 Workstation Security

- **Hillcrest School District** shall ensure that user workstations must not be left unattended when logged into sensitive systems or data including student or employee information. Automatic log off and password screen savers will be deployed to enforce this requirement.

- **Hillcrest School District** shall ensure that all equipment that contains sensitive information will be secured to deter theft. No sensitive data shall be retained on any mobile devices unless that device is encrypted in accordance with the Arkansas State Security Office's Best Practices.

2B2 Server/Network Room Security

- **Hillcrest School District** shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school or District office areas. Access control shall be enforced using either keys, electronic card readers, or similar method with only those IT or management staff members having access necessary to perform their job functions allowed unescorted access.

3. NETWORK SECURITY

3A. Policy Statement

Network perimeter controls will be implemented to regulate traffic moving between trusted internal (District) resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technological feasible.

3B. Standards

3B1 Perimeter Security

- **Hillcrest School District** shall maintain a network configuration management program which includes as a minimum: a network diagram identifying all connections, addresses, and purpose of each connection including management approval of all high risk internet facing ports, such as mail (SMTP/25), file transport protocol (FTP/20-21), etc.

- **Hillcrest School District** shall ensure that all non-State supplied internet connections with public facing servers or workstations will be segmented on a demilitarized zone (DMZ) separate from the internal District network. Segmentation will be achieved by using VLAN's and security policies that prevent unauthorized users from accessing services that their position doesn't require to do their job duties.

3B2 Wireless Networks

- **Hillcrest School District** shall ensure that all wireless access units have non-relative information Service Set Identifiers (SSID) and encrypted authentication requirements that meet the standards set in the Arkansas State Security Office's Best Practices.

- **Hillcrest School District** shall scan for and disable any rogue wireless devices on a regular basis.

3B3 Remote Access

- **Hillcrest School District** shall ensure that any remote access with connectivity to the District's internal network is achieved using following encryption protocols: SSH, RDP-HIGH, or VPN (L2TP).

3B4 Warning Banners

- **Hillcrest School District** shall ensure that appropriate warning banners have been implemented for all district owned equipment, before any user access the District's internal network.

4. ACCESS CONTROL

4A. Policy Statement

System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.

4B. Standards

4B1 System Access Controls - Authentication

- **Hillcrest School District** shall enforce strong password management for employees and contractors as specified in Arkansas State Security Office Password Management Standard.
- **Hillcrest School District** shall enforce strong password management for students as in the Arkansas State Security Office K-12 Student Password Management Best Practice.

4B2 System Access Controls - Authorization

- **Hillcrest School District** shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.
- **Hillcrest School District** shall ensure that user access should be granted and/or terminated upon timely receipt, and management's approval, of a documented access request/termination. Ongoing access shall be reviewed for all users as a minimum annually.

4B3 System Access Controls - Accounting

- **Hillcrest School District** shall ensure that audit and log files are generated and maintained for at least ninety days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/ configuration, and failed attempts to access objects by unauthorized users, etc.

4B4 Administrative Access Controls

- **Hillcrest School District** shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

5. APPLICATION DEVELOPMENT & MAINTENANCE

5A. Policy Statement

Application development and maintenance for in-house developed student or financial application will adhere to industry processes for segregating programs and deploying software only after appropriate testing and management approvals.

5B. Standards

5B1 Systems Development

- **Hillcrest School District** shall ensure that any custom-built student or financial applications or supporting applications which interface, integrate with, or provide queries and reporting to/from student or financial systems are developed using a system development life cycle approach which incorporates as a minimum:
  - Planning, requirements, and design
  - User acceptance testing (UAT)
  - Code reviews
  - Controlled migration to production

5B2 Systems Management and Change Control

- **Hillcrest School District** shall ensure that any changes to core or supporting applications which provide student or financial processing or reporting are implemented in a controlled manner which includes as a minimum:
  - Mechanisms which serve to document each change, both infrastructure and/or application.
  - Management approval of all changes.
  - Controlled migration to production, including testing as appropriate.

6. INCIDENT MANAGEMENT

6A. Policy Statement

Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

6B. Standards

6B1 Incident Response Plan

- **Hillcrest School District** shall develop and maintain an incident response plan to be used in the event of system compromise which should include:
  - Emergency contacts (i.e, Vendors, DIS, ADE/APSCN, law enforcement, employees, etc.)
  - Incident containment procedures
  - Incident response and escalation procedures.

7. BUSINESS CONTINUITY

7A. Policy Statement

To ensure continuous critical IT services, IT will develop a business continuity/disaster recovery plan appropriate for the size and complexity of District IT operations.

7B. Standards

7B1 Business Continuity Planning

- **Hillcrest School District** shall develop and deploy a district-wide business continuity plan which should include as a minimum:
  - Backup Data: Procedures for performing routine daily/weekly/monthly backups and storing backup media at a secured location other than the server room or adjacent facilities. As a minimum, backup media must be stored off-site a reasonably safe distance from the primary server room and retained in a fire resistant receptacle.
  - Secondary Locations: Identify a backup processing location, such as another School or District building.
  - Emergency Procedures: Document a calling tree with emergency actions to include: recovery of backup data, restoration of processing at the secondary location, and generation of student and employee listings for ensuing a full head count of all.

8. MALICIOUS SOFTWARE

8A. Policy Statement

Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.

8B. Standards

8B1 Malicious Software

- **Hillcrest School District** shall install, distribute, and maintain spyware and virus protection software on all district-owned equipment, i.e. servers, workstations, and laptops.
- **Hillcrest School District** shall ensure that malicious software protection will include frequent update downloads (minimum weekly), frequent scanning (minimum weekly), and that malicious software protection is in active state (realtime) on all operating servers/workstations. Districts should consider implementing enterprise servers for required updates to conserve network resources.
- **Hillcrest School District** shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.