The Defining Difference

DATA SECURITY AND PROTECTION PROCEDURE (TCH-P029)

Clarksville-Montgomery County School System

1.0 SCOPE:

The online version of this procedure is official. Therefore, all printed versions of this document are unofficial copies.

1.1 This procedure outlines the steps used to secure and protect user data and to ensure user data integrity.

2.0 RESPONSIBILITY:

2.1 Systems Administrators

2.2 Network Security Engineer

2.3 Senior Network Engineer

2.4 Building Maintenance Manager

3.0 APPROVAL AUTHORITY:

3.1 Chief Technology Officer

4.0 DEFINITIONS:

4.1 Active Directory Account: A centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other systems.

4.2 Firewall: a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

4.3 Antivirus Software: Antivirus software is a kind of software used to prevent, scan, detect and delete viruses from a computer.

4.4 Access Control List (ACL): is a list of access control entries (ACE). Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied, or audited for that trustee.

5.0 PROCEDURE:

5.1 **User Security**

5.1.1 User password policies are enforced based on the current CMCSS password policy for user accountsTCH-P028.

5.1.2 Users are only given permissions to access the data they need to access based on job titles and or roles assigned to their Active Directory Accounts.

5.1.3 User accounts are disabled the day after their last day of employment, and all access to services are removed.

5.2 **Server and Data Security**

5.2.1 Servers must be secured with passwords that meet or exceed the CMCSS password policy TCH-P028.

5.2.2 Access control lists are set on all Windows NTFS permissions to access SMB file shares.

5.2.3 All servers have an active firewall in place.

5.2.4 All server operating systems are updated with security patch management as often and as practical as possible.

5.2.5 Antivirus software is deployed to most servers based on system compatibility and vendor support.

5.2.6 All data stored on servers is password protected and requires proper security permissions to access the files based on roles, and or security groups.

5.2.7 All mission critical servers are backed up daily and replicated to a disaster recovery site to ensure data protection and integrity.

5.3 Network Security

5.3.1 All network routers, switches, and controllers are secured with active directory authentication and command inputs are recorded.

5.3.2 Access is restricted on the principle of least privilege.

5.3.3 All network devices are backed up daily using an automated system, and are manually backed up after changes are made.

5.4 Physical Access Control

5.4.1 Most district buildings where servers reside are secured with an alarm system, key card access control, fire suppression system, and recorded video surveillance.

5.4.2 All servers located in the main datacenter room are protected by an alarm system, key card access control, fire suppression system, recorded video surveillance, and a key coded door lock.

6.0 RECORD RETENTION TABLE:

Identification	Storage	Retention	Disposition	Protection
None				

7.0 REVISION HISTORY:

Date:	**Rev.**	**Description of Revision:**
10/14/21		Initial Release
4/6/22	A	Changed "practically" to "practical" on 5.2.4 Changed "are" to "is" and changed "require" to "requires" on 5.2.6 Split the second sentence on 5.4.1 to a new point (5.4.2)
3/17/23	B	Grammatical error

End of Procedure