**Quitman County School District (QCSD)**

**Technology Department-**

**Remote Access Procedures**

**Remote Access Procedure**

**1.     Overview**

Remote access allows a user to connect from outside the QCSD organization network. This procedure applies to all QCSD employees, contractors, vendors and agents with a QCSD owned or personally owned computer or workstation used to connect to the QCSD network. This procedure applies to remote access connections used to do work on behalf of QCSD

**2.     Purpose**

The purpose of this procedure is to define standards for connecting to QCSD network from any host. These standards are designed to minimize the potential exposure to QCSD from damages, which may result from unauthorized use of QCSD resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical QCSD internal systems, etc.  Remote access implementations that are covered by this procedure include, but are not limited to DSL, VPN, and SSH.

**3.     Procedure**

It is the responsibility of QCSD employees, contractors, vendors and agents with remote access privileges to QCSD network to ensure that their remote access connection is given the same consideration as the user’s on-site connection to QCSD.

Please review the following procedures to ensure protection of information when accessing the QCSD network via remote access methods, and acceptable use of QCSD network:

* Encryption Procedures
* Wireless Infrastructure Communication Procedures
* Acceptable Use Policy/Procedure

### **Requirements**

* Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass phrases. For information on creating a strong pass phrase see the Password Procedures.
* At no time should any QCSD employee provide his or her login or email password to anyone, not even family members.
* QCSD employees with remote access privileges must ensure that their QCSD owned or personal computer or workstation, which is remotely connected to QCSD network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
* The QCSD Technology Coordinator must approve non-standard hardware configurations. Security configurations for access to hardware must also be approved.
* All hosts that are connected to QCSD internal networks via remote access technologies, must use the most up-to-date anti-virus software, this includes personal computers.
* Personal equipment that is used to connect to QCSD networks must meet the requirements of QCSD owned equipment for remote access.
* Organizations or individuals who wish to implement non-standard Remote Access solutions to the QCSD production network must obtain prior approval from QCSD Technology Coordinator.

**Password Procedure**

1. **Overview**

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the entire network. This guideline provides best practices for creating secure passwords.

1. **Purpose**

The purpose of this procedure is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.  This procedure applies to all personnel and entities working on behalf of QCSD, who have or are responsible for any account (or any form of access that supports or requires a password) on any system that resides at or is connected to QCSD.

1. **Procedure**

To minimize the possibility of unauthorized access, all passwords should meet or exceed the guidelines for creating strong passwords.

Password Characteristics

**Strong passwords**

* Contain at least 8 alphanumeric characters
* Contain both upper and lower case letters
* Contain at least one number (for example, 0-9)
* Contain at least one special character (for example,!$%^&\*()\_+|~-=\`{}[]:”;'<>?,/)

**Protection of passwords**

* Users must not use the same password for QCSD accounts as for other non-QCSD access (for example, personal email accounts, shopping sites, social media, and so on
* Where possible, users must not use the same password for various QCSD access needs or user accounts that have system-level privileges granted through group memberships or programs such as FileMaker must have a unique password from all other accounts held by that user to access system-level privileges; unless account has 2-factor authentication enabled
* All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis
* All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least annually.
* Password cracking or guessing may be performed on a periodic or random basis by MTC Staff . If a password is guessed or cracked during one of these scans, the user will be required to change it
* Default passwords must be changed during initial setup and configuration
* Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information
* Passwords must not be inserted along with the username into email messages or other forms of electronic communication
* Do not reveal a password on questionnaires or security forms
* Do not share your QCSD passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members
* Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption
* Never use the “Remember Password” feature of applications (for example, web browsers)
* Any user suspecting that his/her password may have been compromised must report the incident to their supervisor and change all passwords immediately

## ****Access Control****

**1.     Overview**

Access control is the process of authorizing users, groups, and computers to access objects on the network or computer. It is a good practice to assign permissions to groups because it improves system performance when verifying access to an object.

**2.     Purpose**

The purpose for setting access control in the QCSD organization provides system and application access based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.

**3.     Procedure**

This procedure is directed to the Technology Coordinator who is accountable to ensure proper access is given to individual employees.

* QCSD 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.
* QCSD shall ensure that user access should be granted and/or terminated upon timely receipt, and management’s approval, of a documented access request/termination.
* QCSD shall ensure that audit and log files are 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.
* QCSD shall limit IT administrator privileges (operating system, database, and applications) to the District Technology Coordinator and MTC Staff to perform these sensitive duties.