Recommend

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

ACCESS CONTROL POLICY

POLICY: F25

WARNED: 1.27.21

ADOPTED: 2.17.21

EFFECTIVE: 2.17.21

Overview

This policy applies to Washington Central Unified Union faculty, staff, students, outside organizations, contractors and vendors that connect to servers, applications or network devices that contain or transmit WCUUSD Protected Data, per the Data Classification Policy. All servers, applications or network devices that contain, transmit or process WCUUSD Protected Data are considered "High Security Systems". Additionally, All WCUUSD access is controlled by the use of keys at offices or proximity badge within parts of the building. The proximity badge is managed by IT. Access levels are defined by job requirements and management.

Purpose

This policy is designed to protect WCUUSD from unauthorized access to facility and assets. Access controls are designed to minimize potential exposure to the District resulting from unauthorized use of resources and to preserve and protect the confidentiality, integrity and availability of the District's networks, systems and applications.

Policy

It is the policy of the Washington Central Unified Union School District (WCUUSD) to provide a safe environment for students and employees while facilitating access to school buildings, premises and equipment by authorized users. The safety and security of the district's physical space and assets is a shared responsibility of all members of the Washington Central Unified Union School District. This policy addresses the design and management of access-control systems and measures to ensure consistency in implementation.

The District shall establish access control procedures to address the design, administration and management of access control systems and measures. Access-control privileges shall be determined and assigned by the Superintendent or designee based on the specific needs and requirements of the District and the electronic identification/access badge.

Physical Security

For the purpose of this policy, physical security has been divided into two elements: site physical security and information asset physical security.

- **Individual Access**- Physical access to information assets is granted on a need-to- know basis to provide the minimum access to sensitive data necessary.
- **Responsibilities**- IT will be responsible for:
  - Developing, implementing, maintaining and enforcing information asset physical security policies.
  - Ensuring physical security policies and procedures are tested and reviewed annually.

        - Results of testing and review shall be used to make changes to policies and procedures as needed.
    - Documenting exceptions to policies and procedures and identifying compensating controls where exceptions are made.
    - Tracking all facility modifications

User Access

All users of District systems will abide by the following set of rules:

- Users with access to District Systems will utilize a separate unique account, different from their normal District account. This account will conform to the following standards:
    - The password will conform, at a minimum, to the published District Password Policy and Standards.
    - Inactive accounts will be disabled after 90 days of inactivity.
    - Access will be enabled only during the time period needed and disabled when not in use.
    - Access will be monitored when account is in use.
    - Repeated access attempts will be limited by locking out the user ID after not more than six attempts.
    - Lockout duration must be set to a minimum of 30 minutes or until an administrator enables the user ID.
    - If a session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.
- Users will not login using generic, shared or service accounts.
- Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.

Administrative Access

- Administrators will abide by the Access Control Policy.
- Users will abide by the above user access guidelines.
- Administrators will immediately revoke all of a user's access to High Security Systems when a change in employment status, job function, or responsibilities dictate the user no longer requires such access.
- All service accounts must be used by no more than one service, application, or system.
- Administrators must not extend a user group's permissions in such a way that it provides inappropriate access to any user in that group.

Identification Badges

Each employee of the facility will be issued a Photo ID and access card (or key) during their new hire orientation and office employees will be given a key to the office. All employees are expected to wear the Photo ID card at all times when on site at any facility where WCUUSD assets are stored digitally. These cards are the responsibility of each employee to maintain and keep secure. If either card is lost or stolen, the employee must notify their manager and the IT Manager of their facility immediately. The lost card will be deactivated and a new card issued after it is signed for by the employee.