9.0 ACCESS CONTROL

9.1 Purpose

Controlling access to information assets is critical to the security of FCS. Access for all users, devices, and processes will be granted, verified, revoked and audited depending on operational need for continued access. Logical and Physical access will be granted and revoked based on the Principle of Least Privilege. The Principle of Least Privilege states that access is only allowed based on requirement to perform necessary functions and no more. Where possible, duties should be separated to prevent fraud and suspicion.

9.2 Policy

Access to all FCS information should be controlled by information owners and custodians.

9.2.1 Role Based Access Control

Where possible, logical and physical access should be based on a role or job function. Users that are granted access should be assigned to roles based on position and need. All roles should be audited annually for their permissions. All members of all roles should be audited at least annually for required access. Users, devices, and processes should have unique identifiers to prevent non-repudiation. The continuation to generic accounts will be decided by the Technology Services Department on an annual basis.

9.2.2 Physical Access

Physical access to all areas that contain FCS information and systems that create, store, process, or transmit FCS information that is classified at or above must be marked **FOR INTERNAL USE ONLY**. Physical access lists must be maintained by the manager of the area via electronic or hard-copy lists. All possible access methods should be documented in a risk assessment for the assets. Physical access can be limited via many methods including any method to restrict physical access to the area and information assets.

9.2.3 Remote Access

Remote access to internal information systems will follow the principle of least privilege. Only (Technology Department) approved methods of remote access will be used.

Only approved users and processes will be allowed access to the above methods of remote access. Approved user accounts will be managed via the Remote Users Group in Active Directory (AD). No other method of remote access to internal systems is allowed. All unnecessary ports and services should be closed at the perimeter.

9.2.4 External Asset Access

All assets that reside outside the network perimeter must managed access control carefully. External assets include (but are not limited to):

- Websites that maintain student and FCS data
- Cloud-based resources
- Third-party management tools hosted outside the FCS network
- Document and file sharing services

Access to external resources must be managed by an Asset Manager that is responsible for granting, verifying, revoking, and auditing access. Access to external resources should be federated wherever possible.

9.2.5 Privileged Access

Any elevated privileges to any system or information asset must be carefully controlled by the information owner or custodian. All elevated privileges must be reviewed at least quarterly for necessity. All elevated user passwords should be changed at least annually. Where possible Multi-Factor Authentication should be used for user accounts with elevated privileges. Elevated user accounts should be separated by a naming convention from standard user accounts. Users with elevated access should not perform standard activity (answering email, surfing web, etc.) while utilizing their elevated account. All users that have elevated access will have clear roles and responsibilities established and sign an agreement stating their understanding.

9.2.6 Authentication Architecture

Where possible, all authentication architecture should be designed with a single Source of Truth (SoT). Utilizing a single SoT will allow a unified place for permissions and roles to be assigned without having many places to alter or audit. The approved SoT for FCS is Active Directory (AD). The AD SoT will be managed through on-premise AD Domain Controllers (DC)s that are federated to an Azure AD instance for cloud-based authentication. If at all possible, applications, services, users, processes, devices, and systems should be authenticated through federation with AD. Any system classified as operationally critical shall have, at least, multi-factor authentication (MFA) assigned to all staff user accounts. Though not required, that MFA should be tied to the SoT. All connections and authentication assertions should be made through an acceptable level of encryption. Where possible, authentication data should be encrypted at rest and in transit.

9.2.7 Authentication Classification

Data that is capable of authenticating a user (a password, ticket, session, etc.) is classified as **CONFIDENTIAL**. Users should never share their passwords with anyone, including IT. Users are not permitted to write down their passwords and keep them in an unsecure place. If a user suspects their authentication information may have been lost, it is imperative that the user change their password and notify the Technology Department immediately.

9.2.8 Event Detection

All users, employees, contractors, students, visitors, volunteers, and anyone else who utilizes any FCS information system, network component, or classified data should expect that all actions are monitored and logged for security applicability. Users should not expect privacy of personal information while using the FCS network.

9.2.9 Type 1 Authentication Policy

Type 1 authentication is something that a user knows. Examples of Type 1 authentication are passwords, passphrases, pin numbers, secret codes, etc. Type 1 authentication is the least secure method of authentication because it can easily be stolen or guessed and used to authenticate a malicious actor in the user's place. Type 1 authentication is also the most common form of authentication. Users will be required to create strong passphrases consisting of 16 or more characters, upper- and lower-case letters, and numbers or symbols. Users will be required to change their passphrases at least annually. Users should never use their FCS credentials in any other online service such as social media or another website.