BRIDGEVALLEY COMMUNITY & TECHNICAL COLLEGE

ACCOUNT MANAGEMENT

Date approved by cabinet: March 8, 2023
Effective date: April 20. 2023
Expiration date (5 years from effective date if not renewed): April 20, 2028

Section 1. Purpose

1.1. The purpose of this policy is to establish the guidelines for issuing and maintaining BridgeValley Community and Technical College (College) domain accounts.

Section 2. Scope

2.1. This policy applies to all College accounts issued to employees, students, and sponsored accounts (Domain Users).

2.2. This policy applies to Service Accounts created and maintained by the College Information Technology (IT) Department.

Section 3. Usage, Standards, and Responsibilities

3.1. The College will provide a domain account to Domain Users to communicate and conduct College business. Authentication to the provided domain account constitutes an official identification of the individual to the College. The domain accounts may be created only by the College IT Department.

3.2. The contents associated with all College domain accounts are property of the College, not the account holder; therefore, the College reserves the right to:

3.2.1. Monitor College accounts to ensure compliance with applicable laws and College policies;

3.2.2. Access and review all electronic information transmitted or stored in College accounts;

3.2.3. Release information from College accounts to third parties, when required.

3.3. The official repository for College domain accounts is stored in a Directory Service known as Active Directory. This system stores information about the domain account such as names, passwords, phone numbers, job titles, addresses, etc.

3.4. Use of Active Directory for authentication is preferred for all College systems when technically possible.

3.5. Multi-Factor Authentication (MFA) shall be required for all employees (faculty, staff, administration, and adjuncts) of the College to access their domain account where technically possible.

3.6. College usernames must be unique to each account.

3.6.1. Employee accounts shall be in the format of firstname.lastname and a unique consecutive assigned number, if necessary, contained in the bridgevalley.edu domain. Example: John Doe would be john.doe@bridgevalley.edu and a second John Doe hired would be given john.doe2@bridgevalley.edu.

3.6.1.a. Given name may substitute legal first name upon request by the employee account holder.

3.6.1.b. Last name must be legal last name.

3.6.1.c. Changes to the employee account name will only take place after a legal name change submitted to Human Resources (HR) and requested by the account holder to the IT Helpdesk.

3.6.2. Student accounts shall be in the format of first initial, last name, and a unique consecutively assigned number, if necessary, contained in the my.bridgevalley.edu domain. Example: Alex Smith would be asmith@my.bridgevalley.edu and Anna Smith would be asmith1@my.bridgevalley.edu.

3.6.2.a. Student account usernames will be automatically generated from the Student Information System (SIS).

3.6.2.b. Changes to the student account name will only take place after a legal name change submitted to the Office of the Registrar and then requested by the account holder to the IT Helpdesk.

3.7. Responsibilities carried out by the IT Department in support of this policy include:

3.7.1. Creating and managing the Domain User’s account and the associated domains the account resides in;

3.7.2. Administering all authentication and password management systems;

3.7.3. Handling administrative rights on the account such as assigning necessary permissions and group membership, and configuring global policies and settings;

3.7.4. Coordinating federated identity processes, single sign on, and other means of securely accessing College systems; and,

3.7.5. Establishing processes to ensure the individual attempting to authenticate to a College system is the individual to which the College domain account was assigned.

3.8. College Domain Users will be held accountable for the actions that occur within College systems that have been authenticated using their College domain account. Responsibilities of College Domain Users in support of this policy include:

3.8.1. Creating and using passwords that conform to the Password Policy;

3.8.2. Changing password immediately and notifying IT Department when there is reason to believe a password has been compromised;

3.8.3. Adhering to the Computer Use and Abuse Policy;

3.8.4. Safeguarding College login credentials by:

3.8.4.a. Never sharing your password;

3.8.4.b. Never using someone else's login credentials to authenticate to a College system;

3.8.4.c. Securing your computer/workstation by locking or logging out of the device when not in use;

3.8.4.d. Refraining from accessing College domain account on public kiosk devices.

Section 4. Employee Accounts

4.1. Employee Account Creation:

4.1.1. Creation of the employee domain account commences when HR informs the IT Department via written communication.

4.1.2. Upon receipt from HR, the IT Department will create the account within 5 business days prior to the employee’s scheduled start date.

4.1.3. The domain account’s initial password will be set by a member of the IT Department in compliance with the Password Policy. An initial password change will be required upon first successful authentication by the account holder.

4.1.4. The IT Department will assign permissions to the account based upon the role of the employee. A review of account permissions will be discussed between the employee’s supervisor and a member of the IT Department.

4.1.5. After account creation, the IT Department will forward account login information to the supervisor. The supervisor is then responsible for disseminating the login information to the employee.

4.2. Employee Role Change:

4.2.1. Upon an employee's role change at the College, HR shall notify the IT Department via written communication.

4.2.2. The IT Department will update directory service information within 5 business days upon receipt of necessary changes.

4.2.3. Permissions will be reviewed and updated as needed.

4.3. Employee Account Deactivation:

4.3.1. Upon the conclusion of an employee's employment, HR shall notify the IT Department via written communication to deactivate the employee's domain account.

4.3.2. The IT Department will disable the domain account at the time and date specified by HR.

4.3.3. The disabled domain account shall remain disabled for no less than 90 days. Afterwards, the domain account shall be permanently deleted from Active Directory.

4.3.3.a. Exceptions for permanent deletion must be requested by a Cabinet member via written communication to the IT Department.

4.3.4. The disabled domain account shall have all permissions removed and placed in the appropriate Organizational Unit during the disabled period.

4.3.5. The IT Department shall collect and store any files pertinent to the role of the employee and files created by the employee that are property of the College, making them available to the direct supervisor.

4.3.6. Following the guidelines outlined in the Email Policy, the IT Department will set email forwards and retention policies, as necessary.

4.4. Emeritus Faculty:

4.4.1. In accordance with the Emeritus Status Policy, Emeritus Faculty shall retain access to their employee email account.

4.4.2. Permissions of the Emeritus Faculty's domain account shall be reset to that of a

standard user.

4.5. Adjunct Faculty:

4.5.1. Adjunct Faculty shall retain access to their account on a semester-by-semester basis.

4.5.2. A bi-annual review of adjunct accounts shall be conducted by the IT Department in conjunction with HR and Payroll.

4.5.2.a. These reviews will take place 30 days after the start of the fall and spring semesters.

4.5.2.b. Adjuncts without an active contract after this 30-day period shall have their account disabled.

4.5.2.c. The disabled adjunct account shall remain disabled no less than 180 days. Afterwards, the domain account shall be permanently deleted from Active Directory.

Section 5. Student Accounts

5.1. Student Account Creation:

5.1.1. Creation of the student domain account commences when the Student Information System generates the report of new student accounts to create.

5.1.2. This automated process runs hourly every weekday during normal business hours.

5.1.3. The initial account login information will be provided via the student's Acceptance Letter.

5.1.4. The domain account's initial password is in the following format: BVctc+6 digit birthdate (e.g., BVctc020105 for a February 1st, 2005 birthdate)

5.1.5. An initial password change will be required upon first successful authentication by the account holder. The new password must comply with the Password Policy.

5.2. Student Account Deactivation:

5.2.1. An admitted student who does not enroll at the College shall have their account deleted 30 days following the conclusion of their last term of admission.

5.2.2. The IT Department reserves the right to deactivate a student account for cause following student disciplinary action.

5.3. Students that are employed by the College, excluding Work Study, shall be provided with a separate employee account as discussed in Section 4 of this policy.

5.4. Alumni Accounts:

5.4.1. Alumni of the College shall retain access to their account for life.

5.4.2. Access to certain services may be restricted based on licensing requirements for the service(s).

Section 6. Service Accounts

6.1. College IT Department may create a Service Account that must only be created and used for a specific purpose, such as running scripts or sending emails. The password for the account shall be created in compliance with the Password Policy.

6.2. A Service Account is a non-person account associated with a service or system that has a business function for the College.

6.3. All Service Accounts shall be created and stored in an Organizational Unit within the College Directory Service.

6.4. Using the Service Account to send messages or perform functions unrelated to the purpose of the account is strictly prohibited.

6.5. The Service Account name will be created to closely resemble the name of the application or service (e.g., helpdesk@bridgevalley.edu)

6.6. Each Service Account name must be unique.

6.7. Service Accounts must be granted least privilege permissions with explicit permission assigned.

6.8. Service Accounts must be approved by the IT Director. A short description of the business case that necessitates the creation of the account is required to approve creation.

6.9. The requestor of the Service Account shall be designated as the account owner and granted access to the password for the Service Account. College Domain Admins and Service Account owners are the only persons who have access to manage the account.

6.10. College IT Department will conduct an annual audit of all Service Accounts. Those Service Accounts no longer needed will be disabled.

Section 7. Sponsored Accounts

7.1. Sponsored accounts may be created for individuals authorized to access College systems that are not students or employees previously granted access.

7.2. Sponsored accounts require a College sponsor to request the account be created for an individual for a specific, approved purpose.

7.2.1. The request must be written and approved by the College IT Director prior to account creation.

7.3. Sponsored accounts must be granted least privilege permissions.

7.4. Multi-Factor Authentication (MFA) shall be required on sponsored accounts accessing sensitive data.

7.5. Sponsored accounts are only valid for one year and must be renewed annually by the sponsor.

7.6. Upon expiration of the account, the individual will lose access to College systems.

7.6.1. Accounts that remain expired for an additional one year shall be permanently deleted.

Section 8. Definitions

8.1. **Active Directory** - Active Directory is a directory service developed by Microsoft for Windows domain networks. It allows network administrators to create and manage user, computers, and other objects within a network. Active Directory provides a centralized location to authenticate and authorize users with the ability to access services associated with the domain.

8.2. **Alumni** – A graduate or former student of the College.

8.3. **Authentication** - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

8.4. **Directory Service** - A database for storing and maintaining information about users and resources.

8.5. **Domain Account** – A domain account will be the Domain User's username they use to authenticate against Active Directory to access the College domain.

8.6. **Domain Admin** – A user authorized to make changes to global policies and settings that impact all computers and users within a domain.

8.7. **Domain User** - A domain user is a person whose username and password are associated to a College domain and stored in Active Directory rather than the computer the user is

logging into. These users include College employees, students, and other authorized individuals performing College business.

8.8. **Multi-Factor Authentication** – An electronic authentication method that requires the user to successfully provide two or more verification factors (knowledge, possession, and inherence) to gain access to a resource such as an application, online account, or a VPN.

8.9. **Organizational Unit** - A container within a Microsoft Active Directory domain which can hold users, groups, and computers.

8.10. **Permissions** - The authorization given to users that enables them to access specific resources on the network, such as data files, applications, printers and scanners.

8.11. **Service Account** – A non-person account that must only be created and used for a specific purpose, such as sending email or running script.

8.12. **Sponsored Account –** a domain account created for a specific purpose to be used by an individual that is not employed or admitted to the College granting access to specific College systems.