Bergen Community College
Board of Trustees
Section (IT)

Policy #: IT 004-001.2025

Effective Date: June 11, 2025

Responsible Official:
Chief Information Officer

Access and Authorization Control Policy

Policy Statement:

Bergen Community College strives to provide appropriate security and privacy to Bergen IT Resources in accordance with state, federal, local, and institutional policies and regulations. Appropriate and required access and authorization processes, procedures, and policies ensure the security and integrity of Bergen IT Resources as well as safeguard the information of its constituents. All Bergen Users and access to Bergen IT Resources will adhere to a uniform access control standard and framework

Reason for Policy:

To provide the College community with guidelines regarding the authorized access to specific data or systems based on roles and needs, thereby preventing unauthorized access to sensitive information and minimizing the risk of data breaches or security compromises.

Who should read this Policy:

This policy applies to all College employees, contractors/vendors and students.

Definitions:

1. Administrative Access

   The Administrative Access level allows for unrestricted access to a computer system. This includes the ability to make system-level changes and install software. Changes made with this access level can introduce an increased risk to the system and data security.

2. Standard User Access

The Standard User Access level provides users with the ability to utilize their computer and the software installed on it without the ability of making system level changes.

3. Bergen IT Resources
   Laptops, desktops, servers, IoT, software, websites, data, and information owned by Bergen or that store or process Bergen IT Resources.

4. Bergen Data and Information

   Electronic data and information owned by Bergen. Examples of such data are, but not limited to, Bergen financial data, Bergen Employee Data, Bergen student data, Bergen Academic or instructional data, or Bergen research data.

Policy:

This Policy defines The Bergen Community College (the “College”) policy regarding the correct use and management of access and authorization to Bergen Information Technology (IT) resources, data, and information.

1. Principles of Access Control

   a. Bergen IT is the designated information owner responsible and accountable for managing and controlling access to all Bergen IT Resources.

   b. Access controls are the rules for establishing user identity, administering user accounts, and initiating and monitoring access to information resources.

   c. Access to Bergen IT Resources is commonly controlled by a logon ID associated with an authorized account. Proper administration of these access controls (e.g. logon IDs and passwords) is important to ensure the integrity of Bergen Data and Information and the normal business operation of Bergen IT Resources

   d. Access policies and management ensures enforcement of approved authorization for logical access to Bergen IT Resources. Access to Bergen IT Resources and Bergen Data and Information is commonly controlled by a logon ID associated with an authorized account. Proper administration of these access controls (e.g. logon IDs and passwords) is important to ensure the security of confidential information and normal business operation of Bergen as an institution, Bergen IT Resources, and Bergen Data and Information.

   e. Bergen employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with Bergen’s missions and business functions.

   f. Bergen employs session lock to ensure user sessions are locked after a period of user inactivity.

2. Administrative Access

   a. Administrative Access to Bergen IT Resources is not allowed by Users or those without an approved exception for administrative access.

   b. All Exception submissions must accompany a valid business reason.

   c. All exceptions must be approved by the User’s supervisor, Bergen CIO (Chief Information Officer), and Bergen CISO (Chief Information Security Officer)

   d. All Exceptions are valid for one (1) year and will need to be renewed on an annual basis.

   e. IT System administrators must only create new user accounts when they have received a valid and approved Request documented in the ticketing system prior to account creation.

   f. All Administrative accounts and activity via such accounts will be monitored 24X7.

   g. No IT-supported Server Operating system (e.g. AD Server, Web Server, File Server, etc..) should be accessed by a non-administrative IT account.

3. Remote and Third-Party Access

   a. Remote access to Bergen IT Resources should be authorized with established and documented usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

   b. Third-party service providers may be granted access to Bergen network and information systems and may be granted a Bergen account only if:

      i. There is a clear business need.

      ii. With the approval of a Bergen employee sponsoring of the vendor

      iii. With the approval of Bergen CIO or designee.

      iv. The request for such accounts must be documented in the ticketing system.

      v. Such accounts will expire and must be renewed on an annual basis.

4. Account Management

   a. Requests from users for password resets must only be performed once the user’s identity has been verified by the appropriate system administrator or IT helpdesk staff.

   b. Long-term group access via a single shared account is not permitted. All users must utilize individual accounts. A temporary shared guest account may be requested for a specific event, limited to a designated date.

   c. Existing users who require additional access privileges on or to a Bergen IT Resource must obtain approval from their supervisor, Bergen CIO, and Bergen CISO. Such changes in access must be documented in Bergen’s ticketing system.

d. The access accounts of Users who are about to change roles or transfer to another Bergen department, or location, must be reviewed to ensure access account privileges that are no longer required by the user in their new role are removed.

e. Where possible User accounts must be configured to:

   i. Force users to change their password at their first logon. Where this is not possible, users must be instructed to manually change their password the first time they logon to a Bergen IT Resource.
   ii. Automatically ‘lock’ a user account after 10 consecutive failed login attempts.
   iii. Automatically ‘lock’ or log out user accounts after 20 minutes of inactivity on all non classroom Bergen IT Resources. Where this is not possible, users must be instructed to manually log off or ‘lock’ their Bergen computer device (using Ctrl+Alt+Delete keys) when they have to leave it unattended for any period of time and at the end of the each working day.

f. When available audit logging and reporting must be enabled on all Bergen IT Resources.

Enforcement:

This policy is intended to comply with and augment the BCC Student/Employee Code of Conduct and all local, state, and federal laws. Individuals who violate any part of the policy will be subject to college disciplinary action (in accordance with all applicable collective bargaining agreements).

Related Documents/Policies:

- Data Classification and Handling Policy
- BCC Google Drive Docs Usage Guidelines and Support Agreement

Policy History (adopted/amended):

Adopted: June 10, 2025
Amended: