Effective Date: **January 1, 2011** Revised: **April 28, 2024**

POLICY

EMPLOYMENT, INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Identity and Access Management Policy

RESPONSIBLE OFFICE

Information Security

Reviewed and Approved: April 28, 2024 (BY CSIS GOVERNANCE)

This policy supersedes the previous versions of 1.2.C entitled "Access Management and Authentication Requirements" and "Account Maintenance and Security"

Overview

This policy describes types of digital identities in use for systems and applications; criteria for creating, maintaining, and deprovisioning identities and accounts; how identities should be authenticated; how authorizations should be managed; and how accounts and access should be audited.

Scope

Part I is applicable to all individual account holders. It defines account holders' responsibilities

to protect their accounts and properly use their authorizations.

Part II is applicable to anyone who has access to or determines access for a Shared/Departmental Account

Part III is applicable to any individual responsible for configuring Identity and Access Management functions for any system or application.

Part IV sets the standards for the operation of Identity and Access Management services to ensure smooth operation of services and support interoperability.

Part V grants the authority to audit identity access management controls to Information Security and Internal Audit and Advisory Services.

Definitions

Accounts

Accounts are the basis for interacting with information systems. They link a digital identity to a login name, using one or more authentication methods, and enable the assignment of access rights to an information resource (authorizations).

Enterprise Accounts

Enterprise Accounts grant university-wide access to information resources. They are provisioned, maintained, and deprovisioned by established standard processes overseen by IS&T's Identity and Access Management team.

Local Accounts

Local accounts are created within applications and operating systems when they are required for functionality or when enterprise accounts cannot be used.

Affiliation

An affiliation describes the association of an individual to the university. These include Faculty, Staff, Student, Alum, Applicant, Aramark Employee, Visiting Researcher, Volunteer, and many others. The complete list of affiliations associated with each persona are maintained by the Identity and Access Management team in Information Services and Technology.

Authorizations

Authorizations are the implicit or explicit permission to use an information resource associated with an account.

Boston University ID numbers (BUID)

The primary identifier of a person is the Boston University ID (BUID) number, which is a letter followed by eight numbers. The process for the determination of uniqueness is defined in the Identity section of this policy.

Information Resource

Any system, application, or information repository that contains data for which access needs to be managed. This could be an enterprise application like the Student Information System or BU Works, smaller departmental applications including web applications, endpoint devices like an individual's laptop and desktop, a filesharing service like OneDrive, Google, or other forms of shared storage, or a collaboration service like Teams or SharePoint.

Person Identity

The authoritative repository for the Boston University ID Number, a unique identifier of each person affiliated with Boston University.

Person Registry

A repository that contains additional attributes for all personas from the University Systems of

Record. Additionally, Person Registry is the System of Record for gender affirming attributes.

Persona

Personas are used to group Affiliations together. We have three personas: Student, HR, and Affiliate.

Student Persona

An individual who is actively registered and maintains an academic record with Boston University's University Registrar. Examples: Student, Applicant, Alum

HR Persona

An active, compensated employee of Boston University; this includes faculty, staff, emeritus, retired. Examples: Faculty, Staff, Emeritus

Affiliate Persona

A guest who does not receive compensation from Boston University but requires access to our systems or otherwise have a business need for a BU login name. Examples: Aramark Employee, Visiting Researcher, Volunteer, Vendor

Privileged Accounts

Certain accounts may have extra privileges related to the management of a device or application. This is often thought of as an account type, but it is more accurately described as an account with privileged authorizations.

Privileged Access Management (PAM) System

Privileged Account Management refers to the mechanisms that manage and audit accounts that have access beyond that of a default account. Privileged Account Management refers to technology that stores credentials and provides access to them after an individual has authenticated themselves and after validating that the individual should have access to such

privilege. The best systems do not allow the individual direct access to the authentication credential but performs the authentication on their behalf.

System of Record

A System of Record is an enterprise application with the authority to request the creation or retention of an account as part of a university-wide business process. These systems may also maintain certain elements within a Person Identity or Person Registry record. There are four systems of record:

- Student Information Systems (Campus Solutions or Mainframe)
- BU Works (SAP)
- Affiliate System (Affiliates Database)
- Research Computing
    - Research Computing can preserve an existing account for a researcher but cannot request the creation of an account or update Person Identity or Person Registry information. This pathway exists to enable the smooth transition of research for individuals who have left the university.

Due to the special privileges given to Systems of Record, these systems must work closely with IAM to develop processes than ensure the accuracy and integrity of data the provide to the Identity System. Inaccurate or incomplete information may affect an individual's access and or lead to a breach of data.

Part I: Responsibilities of the Individual

Every person with access to Boston University systems is responsible for selecting strong passwords, keeping the passwords secure, protecting their multifactor authentication tokens and applications, and reporting any unauthorized use of accounts. Individuals must:

1. Create passwords that conform to best practices for selecting passwords which address length and complexity.
2. Not share passwords related to any University account with any other person except for authorized Shared/Departmental Accounts.
3. Not use passwords related to any University account for non-University accounts.
4. Immediately change passwords and notify the appropriate system administrator and/or

Information Security if there is reason to believe that a password has been improperly disclosed, accessed, or used by an unauthorized person.

5. Protect multifactor authentication tokens and applications by not sharing codes, approving authentication requests not associated with their own authentication attempts, adding devices belonging to other individuals to their account, or attempting to bypass multifactor authentication.
6. Use privileges associated with an account only for the purpose for which they were authorized and no more.
7. Use privileged accounts and authorizations only when such privilege is needed to complete a function.
8. Avoid saving passwords in scripts and configuration files that can be read by others. This is not intended to prohibit proper use of password management tools.
9. Log off or use screen locking technologies that require authentication when leaving a device unattended.

Part II: Responsibilities Related to Shared/Departmental Accounts

Credentials for accounts that are shared or used by systems or applications must be handled carefully. This section applies to anyone who has access to such an account, or oversees authorizations related to such an account.

1. Ensure that only people with a need to know a password have access to it. Do not share the password with anyone unless explicitly authorized to do so.
2. Change the password associated with the account any time a person with knowledge of it ends their affiliation with the university.
3. Use multifactor authentication for these accounts or obtain a waiver from Information Security. This is particularly critical for accounts with access to Restricted Use data or privileged access to a system or application.
4. Revoke multifactor authentication rights for Shared/Departmental accounts to anyone who has ended their affiliation with the University.
5. Where reasonable and possible, require the individual to authenticate as an individual first and then switch to the privileged account, using tools such as Privileged Account Management or the capability provided by the sudo utility.
6. Where possible, apply secondary controls on how these accounts may be used such as by controlling where the accounts be used from (on campus only, e.g.) or when (working

hours only).

Part III: Responsibilities of Application and Systems Administrators

Individuals who are responsible for configuration of authentication and authorization controls on applications and systems intended for general use, including cloud (Software as a Service) applications, must:

1. Use enterprise authentication over local authentication whenever possible and reasonable.
2. Limit the use of Departmental/Shared accounts to access data.
3. Ensure privileged access is granted only to appropriate accounts with need for such access. Ideally, passwords for accounts with privileged should be stored in a privileged access management system (see below).
4. Ensure that locally defined access is revoked at appropriate times.
   a. When access is managed locally, the system or application must account for termination of access when an individual's affiliation change. Some individuals will retain access to their account based on affiliation even though a role may have ended (e.g. alumni, retiree).
5. Ensure that any account or authorization created, deleted, removed, or changed is audited and available for review. This log would contain proof of approvals for the creation, deletion, removal, or change and the system and any system or application-level log that the account or authorization was modified, if such can be logged.
6. Ensure that non-privileged accounts do not have access to privileged functions and audit any use of privilege.
7. Ensure that any system or application that authenticates or authorizes an account logs both successful and failed activities to a standard location and format.
8. Conduct routine audits of account and authorization activity to ensure that only authorized use is occurring and maintain audit documentation accordingly. As part of this audit:
   a. Provide a list of accounts with privileged access to the appropriate management approvers for review.
   b. Support and encourage periodic review by Data Trustees for information covered under a Trustee's responsibilities.

Variances from these requirements must be approved by Information Security.

Part IV: Identity and Access Management Standards

This part of the policy applies to all university community members who configure and/or maintain devices and applications for the university. This part also applies to how vended solutions (e.g. cloud applications, Software as a Service) must be configured.

A. Digital Identity

All persons associated with the university shall have a unique digital identifier that is never revoked. This unique identifier is the Boston University ID number (BUID). The authoritative source for pairing an identity to their BUID is the Person Identity system run by IS&T.

When a new identity is requested by a System of Record, the following *Elements of Identification* are evaluated to ensure that an individual receives only one identifier. A matching routine referred to as the *Four Point Match* is used to determine uniqueness. A *Duplicate Identity (dup-id)* process exists to resolve situations where an individual is assigned more than one BUID.

Elements of Identification

The following data elements are collected to identify each person uniquely:

- Legal First Name
- Legal Last Name
- Date of Birth
- Personal non-BU e-mail address
- Social Security Number (optional)
- Passport (optional)

Non-human Identities

There is a need to support the creation of accounts that are not directly associated with a person, such as shared or group accounts. When these accounts require a unique identifier,

they are issued a BUID number that starts with the letter “G”, also known as a “GID”. Accounts with a GID are recorded in our legacy directory system.

Person Registry

The Identity Service maintains a *Person Registry* which contains additional optional information about an individual including display name, pronouns, gender identity, and sexual orientation.

Additional information about the governance (collection and use) of this information can be found at https://www.bu.edu/asir/data-use/data-standards/bu-governed-identity-data-diversity-inclusion/.

The Identity Service shall provide a mechanism for the individual to provide and maintain this information. The Person Registry is the university’s System of Record for these attributes. Other systems should not collect or maintain this information but rather reference the data kept in the Person Registry.

B. Accounts

Accounts are the basis for interacting with information systems. They link a digital identity to a login name, using one or more authentication methods, and enable the assignment of access rights (authorizations) to information resources.

Enterprise Accounts

Enterprise Accounts grant university-wide access to information resources. They are provisioned, maintained, and deprovisioned by established standard processes overseen by IS&T’s Identity and Access Management team.

Requirements for an Enterprise Account

1. Individuals must have an approved affiliation with the university to have an enterprise account.
2. The affiliation of an individual with the university must be validated at least annually. If

the affiliation expires, the account should be deprovisioned in a timely fashion.

3. Enterprise Accounts that do not have an active affiliation are promptly disabled.

Types of Enterprise Accounts

Enterprise Accounts are provisioned and deprovisioned based on the *affiliation* as defined by a *System of Record* or based on a manual request policy for some account types. Enterprise accounts should be used to authorize access whenever possible. These accounts are divided into groups as shown in the table and further defined below.

Account Type	Sub Type
Human Accounts	BU Login Accounts
	Web Accounts
	Role Accounts
Non-Human Accounts	Shared/Departmental Accounts
	Student Group Accounts
	Service Accounts

Human Accounts

There are three types of accounts associated with individuals, BU Login Accounts, Web Accounts, and Role Accounts. They have the following properties:

BU Login Accounts

BU Login Accounts are the most common account used for all individuals with an ongoing relationship to the university, including student, faculty, staff, and affiliates. The login name associated with an account is assigned or chosen at account creation and is used as the university e-mail address, such as loginname@bu.edu.

Web Accounts

Web Accounts are used with individuals that have temporary relationships with the university, such as applicants and parents. These accounts generally do not require extensive access rights. The login name associated with the account is assigned at account creation based on the non-BU personal email, such as loginname@gmail.com.

Role Accounts

Role accounts are similar to BU Login Accounts and are used to give named individuals privileged access to systems without assigning those privileges to the accounts they use every day. These accounts include Active Directory administrative accounts, such as loginname-adm@bu.edu. Role account names derived from a person's account name may be longer than 8 characters, but otherwise follow the BU Login Account Naming rules.

Non-Human Accounts

There are three types of non-human accounts. These accounts may be shared amongst multiple individuals, such as shared/departmental accounts or student group accounts, or used in system-to-system communication, such as service accounts.

Shared/Departmental Accounts

Shared/departmental accounts are created to support multiple individuals sharing the same identity. The direct use of shared accounts should be discouraged as it lacks accountability. In many cases these accounts are necessary to receive e-mail for a university department or function. Access to these accounts should be achieved by delegation of access rather than password sharing. These accounts follow the BU Login Account Naming rules.

Student Group Accounts

These accounts are used by official university student groups as approved by the Student Activities Office. It is expected that these accounts will be shared by multiple officers of the group. These accounts follow the BU Login Account Naming rules.

Service Accounts

A service account is used when it is necessary for systems or applications to authenticate to other systems or applications without any association to a person. These accounts should be created sparingly, and documentation of their purpose should be kept. Service accounts may not be used by people to authenticate aside from initial testing. Service accounts with elevated privileges must be closely monitored for abuse. These accounts follow the BU Login Account Naming rules.

Account Naming Rules for Enterprise Accounts

Enterprise Accounts Except Web Accounts, including Human and Non-Human Accounts

- Must be 2 to 8 characters in length.
- Can contain both letters and numbers but cannot contain a number as the first character.
- Cannot include any punctuation characters.
- Account Names must not be reused.

Enterprise Web Accounts

- The account name is based on the personal email address.

Local Accounts

Local accounts are created within applications and operating systems when they are required for functionality or when enterprise accounts cannot be used.

When local accounts are created, the system or application administrator must define the procedure by which they will be approved, created, maintained, and deprovisioned. The procedure must be consistent with the guidelines expressed for enterprise accounts. Deprovisioning must be performed in a timely fashion.

Local accounts with privilege must be carefully protected and ideally stored in a privileged access management system.

Privileged Accounts

Certain accounts may have extra privileges related to the management of a device or application. This is often thought of as an account type, but it is more accurately described as an account with privileged authorizations. Administrative privilege can only be added to BU Login Accounts, Role Accounts, and Service Accounts, or Local Accounts. The use of privilege should be limited to what is needed. These accounts must be carefully protected and ideally stored in a Privileged Account Management system.

C. Directory Services

The University provides a mechanism to query account information about members of the community to enable collaboration. The following attributes are available by default:

- Display Name
- E-mail Address
- Primary Department (for faculty and staff)
- Office Information (for faculty and staff)
- School or College (for students)
- Pronouns (if configured by individual, see *Person Registry*)

There are options for restricting the display of individuals in the directory. The options available depend on the individual's affiliation. Individuals should contact Enrollment Services or Human Resources to discuss their options.

D. Authentication

Authentication is the process by which a system or application confirms that a person or device really is who or what it is claiming to be. Strong authentication protocols help both to protect personal and University information and prevent misuse of information resources.

All Enterprise Accounts are authenticated against services provided by Information Services and Technology.

Types of Authentication

Authentication may take many forms. Authentication is generally broken down into three types:

- **Something you know:** The most common forms are a password, pin, or pattern.
- **Something you have:** The most common forms are a hardware token, certificate, or a software authenticator like Duo or Google Authenticator.
- **Something you are:** This category is often called biometric authentication. The most common forms are fingerprint readers and facial recognition.

Multifactor Authentication

Multifactor Authentication (MFA) involves combining more than one authentication type and generally provides a stronger assurance of the person's identity. Combining only two of the types is sometimes called two-factor authentication (2FA).

Authentication Policies

These policies should be applied to all systems and applications. Enterprise accounts comply with all of these policies.

Authentication Policy

1. All accounts must require authentication before use. Unauthenticated access may be used only with data classified as Public (See Data Classification).
2. Authentication credentials should be set by the account holder at the time of account creation or temporary passwords may be used so long as the temporary password is immediately changed upon login. Temporary passwords must conform to all other password requirements.
3. Any application or system, whether on premise or in the cloud, should use enterprise authentication services instead of local accounts and passwords whenever possible and reasonable.
4. Passwords must be encrypted in transit over any network.
5. Passwords must be encrypted when stored.

Password Policy

1. The minimum password length is 16 characters.
2. Passwords must be changed at least every 5 years.
3. Passwords must be complex. The password must contain at least three of the following four types of characters: Lowercase letters, Uppercase letters, Numbers, Special characters.

Multifactor Authentication Policy

1. Use multifactor authentication for all applications and systems where possible and reasonable. Use of multifactor authentication for local authentication may consider the physical security of the device.
2. Use multifactor authentication for all BU Login accounts, Role Accounts, Shared/Departmental Accounts, and Student Group Accounts.
3. To prevent replay attacks, multifactor authentication for network-based access should use tokens that expire in a short period of time or incorporate the current time into the authentication process.
4. If an application or system that contains Restricted Use information cannot support multifactor authentication a compensating control must be used, and the plan must be approved by Information Security.

Additional Recommendations and Compliance Specific Requirements

1. Consider a policy that prevents individuals from reusing the same password. This is required for systems containing credit card data per the PCI-DSS regulation.
2. Authentication failures should not provide feedback to the client on why the authentication failed, only that it did.
3. Consider locking access to accounts after multiple failed authentication attempts within a period such as 30 failed attempts in 5 minutes.
   a. Locked accounts should remain unusable for at least 30 minutes or until unlocked by a system or application administrator.
   b. Locking accounts after 6 attempts is required for systems containing credit card data per the PCI-DSS regulation.

E. Authorization

Authorizations are the implicit or explicit permission to use a resource associated with an account. Once the use of an account is authenticated, a system or resource may determine if the person or software requesting access is authorized to use it. The management and maintenance of authorizations is shared responsibility of Information Services & Technology and local system and application administrators.

All units engaged in granting authorizations are encouraged to develop procedures that meet the requirements articulated below in the authorization policy.

Types of Authorizations

There are several types of authorizations to consider.

Birthright Privileges

When an account is created in the university's central identity management system, certain authorizations are immediately created with it, such as the ability to authenticate against our enterprise authentication systems, access to our network and enterprise remote access services, and several online resources. Accounts are granted these authorizations automatically either implicitly or explicitly in the account creation process managed by IS&T and are related to the individual's affiliation with the university. For some types of affiliates, it is possible to customize what these birthright privileges are.

Application and System Administrators must not circumvent the authorizations contained within birthright privileges by, for example, encouraging sharing accounts, creating proxy authentication services to enable individuals to make requests with the privileges of other accounts, or creating secondary authentication and authorization systems aimed at bypassing these controls.

System and Application Level Authorizations

In some cases, accounts may need to be defined explicitly in an application or system. When an account is defined in a local system or application, some authorizations may be implicitly granted, such as the ability to use some or all functions of the application or system.

Privileged Authorizations

Certain authorizations grant access to administer a system or application and/or access to see data that is created or maintained by others. Privileged access should be granted based on the specific person's job duties, not the duties of the person's organizational unit. Use of privilege should be recorded by the system or application.

Principles of Authorization

Least Privilege

An authorization should only provide the privileges required for the function to be performed and no more. Following this principle helps ensure proper workflows are followed and access to data is constrained.

Separation of Duties

When non-birthright authorization is granted to an account it must be approved by multiple individuals. Multiple approvers ensures that the Principle of Least Privilege is followed from both a technical and process perspective, decreases opportunity for conflict of interest or fraud, and reduces the risk of error. As applied to authorization, separation of duties requires that the administrative and technical approver are not the same person, or if they must be, then the Data Custodian is not filling either role.

Roles in Authorization

Authorizing an account to use a system or application is a distributed responsibility shared by Information Services & Technology, our IT partners, and sometimes external partners who might create authorizations at our direction.

Data Custodians

In general, these authorizations are implemented by “Data Custodians”, who are entrusted with the maintenance of data. These are typically Systems Administrators, Database Administrators, or Application Administrators. See the Data Access Management Policy for details on this role. These individuals are responsible for executing the approved authorization changes, after validating that appropriate approvals have been granted.

Data Trustees and Data Stewards

Data Trustees are leaders entrusted with the responsibility to ensure that university data is used appropriately by the institution. Their roles are defined in the Data Access Management Policy. Within authorization, they have a role in approving access to data types. Data Trustees may designate additional individuals, called Data Stewards, to make approvals on their behalf.

Administrative and Technical Approvers

All requests for non-birthright authorization must be approved from an administrative and technical approver. These approvers must be two different people to ensure separation of duties. These approvers are responsible for ensuring the Principle of Least Privilege is applied from their respective viewpoints.

Administrative Approval: The administrative approval confirms that the authorization requested is needed to perform a required function. The approver should sufficiently understand the full scope of the authorization being granted before deciding and ensure Least Privilege is applied.

Technical Approval: The technical approval confirms that the privilege requested is required to achieve the approved administrative need. The approver should sufficiently understand the full scope of the authorization being granted before deciding and ensure Least Privilege is applied.

Application and System Authorizations

Authorizing access may be automated based on a person’s membership in a specific group or

a manual process. When authorizing a person to use an application or a system, a Data Custodian must adhere to the following authorization policy.

Authorization Policy

Before granting access to a system or application, the Data Custodian must ensure the following policy is adhered to:

1. Use role-based authorization schemes over individual authorizations whenever practical.
2. Be as granular as possible in your authorizations.
3. Ensure that the authorization has the appropriate approvals:
   a. Administrative and Technical Approvals are always required. These approvers must:

      i. Ensure the principles of Least Privilege and Separation of Duties are applied.
      ii. When approving privileges to a shared account consider everyone who has access to that account and whether such privilege is appropriate for everyone.

   b. All requests for access to data for which there is a Data Trustee must be approved by the Data Trustee or their Data Steward. See the Data Access Management Policy for more details.

4. Privileged access may be granted permanently only if that specific person's job duties routinely require that level of access, otherwise, the access must be temporary.
5. All authorization requests must be documented, including the nature of the request, the period for which it has been granted, all related approvals that were obtained, and the names of the approvers.

Pre-authorized requests

As appropriate, the Data Trustee or Data Steward may pre-approve authorizations for roles that always need such authorizations. See the Data Access Management Policy for more details.

Pre-authorization for privileged account authorizations may be considered but are generally discouraged.

NOTE:

It is insufficient to rely on the central deprovisioning of accounts as a method of terminating locally deployed authorizations, as the timeliness of the account deprovisioning is dependent on several factors that are beyond the control of the local systems and application administrators.

Part V: Auditing

Information Security and/or Internal Audit and Advisory Services may make routine or ad-hoc requests to audit the accounts and authorizations of any university information system along with the associated audit trail. These audits will ensure that accounts and authorizations are consistent with this document, including that:

1. There is a request for every account with elevated privilege, shared account, or service/process account;
2. The request was approved by all applicable parties;
3. The request is compliant with applicable regulation, policy, and best practice;
4. The granted privileges were required for the approved administrative use;
5. Requests for temporary privileges are revoked on the agreed expiration date;
6. Every active account is held by a person with an active affiliation at the institution; and
7. The account holder's job function still requires the granted privilege.

Exceptions

Information Security is authorized to grant exceptions to the requirements set forth in this document. Any exception granted will require a thorough review of the situation and the implementation of appropriate compensating controls.

In addition, Information Security may publish directives aimed at clarifying the intent of a standard to aid in the interpretation of this policy.

Important

Failure to comply with the Data Protection Standards may result in harm to individuals, organizations, or Boston University. The unauthorized or unacceptable use of University Data, including the failure to comply with these standards, constitutes a violation of university policy

and may subject the individual to revocation of the privilege to use University Data or Information Technology or disciplinary action, up to and including termination of employment.

Appendix A: NIST Cyber Security Framework and SP 800.171 Mapping

The following table maps the National Institute of Science and Technology (NIST, nist.gov) Cyber Security Framework (CSF) and Special Publication (SP) 800.171 controls to policy expressed in this document. Fully implementing this policy with associated procedures and evidence of adherence to those procedures would likely indicate that all the controls listed here are met. However, compliance must always be evaluated for the scope of the information system in question, and having policy by itself does not guarantee compliance.

CSF Control	800.171 Control	Control
PR.AC-1		Identities and credentials are issued, managed, verified, rev and audited for authorized devices, users and processes
PR.AC-1	3.5.1	Identify system users, processes acting on behalf of users, a devices.
PR.AC-1	3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organization systems.

PR.AC-1	3.5.5	Prevent reuse of identifiers for a defined period.
PR.AC-1	3.5.6	Disable identifiers after a defined period of inactivity.
PR.AC-1	3.5.7	Enforce a minimum password complexity and change of cha when new passwords are created.
PR.AC-1	3.5.8	Prohibit password reuse for a specified number of generatio
PR.AC-1	3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.
PR.AC-1	3.5.10	Store and transmit only cryptographically-protected passwor
PR.AC-1	3.5.11	Obscure feedback of authentication information
PR.AC-3		Remote access is managed
PR.AC-3	3.1.1	Limit system access to authorized users, processes acting o behalf of authorized users, and devices (including other syst
PR.AC-3	3.1.2	Limit system access to the types of transactions and functio authorized users are permitted to execute.
PR.AC-4		Access permissions and authorizations are managed, incorp the principles of least privilege and separation of duties
PR.AC-4	3.1.4	Separate the duties of individuals to reduce the risk of malev activity without collusion.

PR.AC-4	3.1.5	Employ the principle of least privilege, including for specific functions and privileged accounts.
PR.AC-4	3.1.6	Use non-privileged accounts or roles when accessing nonse functions
PR.AC-4	3.1.7	Prevent non-privileged users from executing privileged funct and capture the execution of such functions in audit logs.
PR.AC-4	3.1.8	Limit unsuccessful logon attempts.
PR.AC-4	3.1.10	Use session lock with pattern-hiding displays to prevent acc and viewing of data after a period of inactivity
PR.AC-4	3.1.11	Terminate (automatically) a user session after a defined con
PR.AC-4	3.5.3	Use multifactor authentication for local and network access privileged accounts and for network access to non-privilege accounts.[24] [25].
PR.AC-4	3.5.4	Employ replay-resistant authentication mechanisms for netw access to privileged and non-privileged accounts.
PR.AC-4	3.13.3	Separate user functionality from system management functi

PR.AC-4	3.13.4	Prevent unauthorized and unintended information transfer v shared system resources.
PR.AC-6		Identities are proofed and bound to credentials and asserted interactions
PR.AC-7		Users, devices, and other assets are authenticated (e.g., sin factor, multi-factor) commensurate with the risk of the transa (e.g., individuals' security and privacy risks and other organizational risks)
PR.DS-5	3.1.4	Separate the duties of individuals to reduce the risk of malev activity without collusion.
PR.DS-5	3.9.2	Ensure that organizational systems containing CUI are prote during and after personnel actions such as terminations and transfers
PR.IP-11	3.9.2	Ensure that organizational systems containing CUI are prote during and after personnel actions such as terminations and transfers

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related BU Policies, Procedures, and Guidelines

- Data Protection Standards
  - Data Classification Policy
  - Data Access Management Policy (*This policy supersedes the previous versions entitled* "Data Management Guide")

- Identity and Access Management [current webpage]
- Data Lifecycle Management Policy (*This policy supersedes the previous versions entitled "*Data Protection Requirements")
- Minimum Security Standards
- Cybersecurity Training, Compliance, and Remediation Policy (*This policy supersedes the previous versions entitled* "Education, Compliance, and Remediation")

BU Websites

- Information Services & Technology

BU Resources

- Additional Guidance on Data Protection Standards
  - 1.2.D.1 – Destruction of Paper Records and Non-Erasable Media -CD-ROMs, DVDs (Data Protection Standards Guidance)
  - 1.2.D.2 – Destruction of Individual Files on Reusable Media (Data Protection Standards Guidance)
  - 1.2.D.3 – Securely Erasing Entire Reusable Storage Devices (Data Protection Standards Guidance)
  - 1.2.D.4 – Physically Destroying Reusable Storage Devices (Data Protection Standards Guidance)

Categories: Employment, Information Management, Privacy and Security, Workplace
Keywords: Data Protection Standards