Effective Date: **January 1, 2011** Revised: **April 1, 2019**

POLICY

EMPLOYMENT, INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Identity and Access Management Policy

RESPONSIBLE OFFICE

Information Security

Reviewed and Approved: April 28, 2022 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 electronic identities in use for systems and applications; criteria for creating identities and accounts; how identities should be authenticated; how authorizations should be managed; and how accounts and privileges should be deprovisioned.

Scope

Part 1 of the policy is applicable to individual account holders. It defines account holders' responsibilities to protect their accounts and properly use their authorizations.

Part 2 of the policy is applicable to Information System operators responsible for Identity and Access Management for information systems.
This policy focuses on requirements for systems and applications. While it is important to consider encrypting or password-protecting individual files or documents, especially if the files may be sent electronically or stored on a portable device, the intent of the policy is not to set requirements for such individual files or documents.

Part I: Responsibilities of the Individual

Every person with access to Boston University systems is responsible for selecting strong passwords, keeping the passwords secure, and reporting any unauthorized use of accounts. Users 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 system with any other person.
3. Not use passwords related to any University system 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. Use privileges associated with an account only for the purpose for which they were authorized and no more.
6. Use privileged accounts and authorizations only when such privilege is needed to complete a function.
7. Log off or use screen locking technologies that require authentication when leaving a device unattended.

Part II: Responsibilities of Information Systems Staff

This part of the policy applies to all university community members who configure and/or maintain devices and applications for the university.

A) Accounts

Account Types

There are three types of accounts at Boston University:

User Accounts: These are uniquely associated with a specific person. These accounts may either exist in a central repository to which systems may federate to consume the identity and authentication information or they may be created locally on a system or device where federation is not practical or possible. The use of the centrally created account with federated authentication is always the preferred method.

Shared Accounts: Shared accounts are created to support multiple users sharing the same identity. For example, these may be created when there is a need to share a set of resources or because a poor product implementation requires it. The use of shared accounts should be discouraged as it lacks accountability.

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 the purpose for them should be kept. Their use must be periodically reviewed. Further, the password requirements for service accounts must be no less stringent than user accounts. Finally, 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.

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 be added to any of the three account types. Having at least one account with privileges is generally unavoidable but the use of privilege should be limited and the direct use of shared accounts with privileges should be discouraged as it lacks accountability.

Enterprise Directory Services

Information about centrally created accounts and identities are stored in central directory run by Information Services and Technology. The most common implementations of the directory service are Active Directory (AD) and Lightweight Directory Access Protocol (LDAP).

University information systems should use enterprise directory services whenever possible and avoid creating local accounts and authorizations.

Boston University ID numbers

The primary identifier of a person in our Information Systems is the Boston University ID (BUID) number, which is a letter followed by eight numbers. The repository of BUIDs and the technology for assigning an ID number to an individual is maintained by Information Systems and Technology.

Every person with an account in the university's central directory (a User Account), must be associated with a BUID number that starts with the letter "U", also known as a "UID". **NOTE**: This is not the same as the Unix/Linux "user id" number which is also known as a "uid". The Unix/Linux "uid" is referred to as an "index_id". This number is assigned centrally as well as part of account creation.

Group Accounts, including Departmental Accounts, Student Organizational Accounts, and System or Administrator Accounts defined in the university's central directory, must be associated with a BUID number that starts with the letter "G", also known as a "GID". **NOTE**: This is not the same as the Unix/Linux "group id" number which is also known as a gid. The Unix/Linux gid is not part of a central repository and may be assigned locally according to need and preference. By default the Unix/Linux uid and gid should match.

Service Accounts defined in our central repository will also use GIDs as defined in the previous paragraph.

The process of obtaining a BUID number is defined by our Identity and Access Management Service.

Ensuring Uniqueness of a UID

A BUID number must be unique to a single person and each person must only have one UID. In rare cases a second ID number is required for testing Information Systems. The secondary accounts will be issued a GID instead. All exceptions must be approved by Information Security.

Centrally Managed Accounts

The process of requesting a centrally managed account is defined by Information Services &

Technology's Identity and Access Management Service and adhere to the following guidelines:

1. Limit the use of generic or shared accounts.
2. Systems storing Restricted Use and/or Confidential information must not be configured to allow access using shared or anonymous accounts.

Non-centrally Managed Accounts
When accounts or authorizations are created outside of the enterprise directory and/or enterprise authentication system, the unit creating the accounts must define the procedure by which they will be approved and created. The procedure must be consistent with the guidelines expressed for centrally managed accounts.

B) 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 and through which access to the requested resource is authorized. Strong authentication protocols help both to protect personal and University information and prevent misuse of University resources.
All accounts, centrally defined or not, must require authentication before use, except in rare cases when it is necessary to use an account that does not require authentication for "anonymous" access. Anonymous access may be used only for information classified as Public in the Data Classification.

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 and the most common form is fingerprint readers including Apple's Touch-ID.

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 called two-factor authentication (2FA).

Enterprise Authentication Services

Authentication credentials for centrally created accounts and identities are stored in central repositories run by Information Services and Technology. Passwords are stored centrally in a Kerberos database. We support multifactor authentication through the Duo service to which enrollment is centrally managed by Information Security.

Federated Authentication

Systems and applications may authenticate identities using our enterprise authentication services by *federating* with them. For systems and non-web applications, federation for password authentication is achieved through direct Kerberos authentication or by joining the system to our Active Directory. Systems and non-web applications may also federate with our Duo service. For web applications federation is achieved through Shibboleth which can be deployed with or without Duo.

Shared and Service Accounts

Credentials for accounts that are shared or used by systems or applications must be handled carefully. Follow the following rules when managing these credentials:

1. Ensure that only people with a need to know a password have access to it.
2. Where reasonable, use multifactor authentication for these accounts, especially on accounts that have privilege such as application or system administrator accounts.
3. Where reasonable, require the individual to authenticate to the system as an individual first and then switch to the administrator account, such as the capability provided by the Linux/Unix sudo utility.
4. Change the password associated with the account any time a person with knowledge of it ends their affiliation with the university.
5. Avoid saving passwords in scripts and configuration files that can be read by others.
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).

Application and System Administrator Responsibilities

Any person charged with the responsibility of setting up a system or application that requires authentication must configure the system to enforce our authentication policy (below) to the extent possible within the system or application. Variances from the stated authentication policy for Restricted Use systems must be approved by Information Security.

Authentication Policy

1. Whenever possible and reasonable, any application or system, whether on premise or in the cloud, should use federated authentication over local accounts and passwords.
2. The minimum password length is 8 characters. 10 or longer is recommended.
3. Passwords must be complex. The password must contain at least three of the following four character sets: Lowercase letters, Uppercase letters, Numbers, Special characters.
4. Use multifactor authentication for all Restricted Use systems and applications and where otherwise reasonable to do so. If a system or application that contains Restricted Use information cannot support multifactor authentication a compensating control must be used and the plan must approved by Information Security.

Additional Authentication Recommendations and Compliance Specific Requirements

1. Consider a policy requiring users to change passwords periodically. This is required for systems containing electronic Protected Health Information (ePHI) covered by HIPAA and credit card data per the Payment Card Industry Data Security Standards (PCI-DSS), regulation.
2. Consider a policy that prevents users from reusing the same password. This is required for systems containing credit card data per the PCI-DSS regulation.
3. Consider locking access to accounts after multiple failed authentication attempts within a period of time such as 30 failed attempts in 5 minutes. Locking accounts after 6 attempts is required for systems containing credit card data per the PCI-DSS regulation. Locked accounts should remain unusable for at least 30 minutes or until unlocked by a system or application administrator.

Local Application Development

Applications that are developed by Boston University for use at Boston University should be designed to support the requirements of our authentication policy.

C) 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 system, certain authorizations are immediately created with it, such as the ability to authenticate against our enterprise authentication systems, access to our network, 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 sometimes related to the individual user's affiliation with the university. For some types of guests it may be 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 users to make requests with the privileges of other users, or creating secondary authentication and authorization systems aimed at bypassing these controls.

System Level Authorizations: Once an account is created on a local system, the account is authorized to access the system and use software and services available to that system. In general, these authorizations are implicit in the creation of an account on the system rather than granted explicitly to the account once created. Some account types have special privileges associated, such as an "administrator", "super user", or "root" account that is responsible for administrative functions of the system including updating software and managing other accounts.

Application Level Authorizations: Similar to systems, accounts may have to be explicitly added to applications to enable access; a birthright allocation may be insufficient for an individual's job function and additional authorizations will have to be granted.

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 is dependent on the specific person's job duties, not the duties of the person's organizational unit. Information Security is solely responsible for authorizing privileged access to IS&T servers and applications that process or store client data and any university system containing Restricted Use information.

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 functions that may expose data is contained as much as possible.

Separation of Duties

When an 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 granted by "Data Custodians", who are entrusted with the maintenance of the 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 account

definition/modification/removal request, after validating that appropriate approvals have been granted.

Data Trustees

Data Trustees are leaders entrusted with the responsibility to ensure that university data is used appropriately by the institution. Their full jobs are defined in the Data Access Management Policy. Within authorization, they have a special role when approving access to data types that have an associated Trustee, also defined in the Data Access Management Policy Access Management Policy.

Administrative and Technical Approvers

All requests for 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 making a decision 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 making a decision and ensure Least Privilege is applied.

Information Security

Information Security is solely responsible for authorizing privileged access to IS&T servers and applications that process or store client data and any university system containing Restricted Use information. Information Security will confirm that the user to be authorized has signed the appropriate confidentiality agreement(s), taken appropriate training, and/or holds appropriate credentials for accessing the resource.

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 or not 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. See the Data Access Management Policy Access Management Policy for more details.
    c. All requests for access to a system or application containing Restricted Use information have been approved by Information Security.

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 time 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 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.

D) Deprovisioning

Systems and applications should be designed and deployed in a way that facilitates easy removal of a person's authorizations and accounts at appropriate times.

Centrally Managed Accounts and Authorizations
The enterprise level accounts or authorizations that are listed in the enterprise directory service and have authentication credentials in our enterprise authentication services shall be deprovisioned in accordance with the policies of our Identity and Access Management service, adhering to the principles that:

1. Individuals with no affiliation with the university should not have an account.
2. Accounts for individuals with no lasting associations with the University, identified as affiliates within our IAM policies, should only exist for a limited period of time without reauthorization.

Non-Centrally Managed Accounts and Authorizations
When accounts or authorizations are created outside of the enterprise directory and/or enterprise authentication system, the unit creating the accounts must define a mechanism to deprovision the account in a timely fashion (generally within a few business days unless a specific time frame is requested) and consistent with the conditions expressed for centrally managed accounts.

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 a number of factors that are beyond the control of the local systems and application administrators.

E) Auditing

Audit Trail
Data Custodians are responsible for ensuring that an audit trail of activity exists that includes the following:

- Ensuring that any account or authorization created, delete, removed, or changed under Section II, III, or IV of this document is audited in a system of record 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.

- Any system or application that authenticates or authorizes an account to take an action should log that activity to a standard location and format. The log should include both successful and failed authentications and authorizations.
- Ensuring that the system or application audit logs are properly configured and functioning normally over time.
- Conducting 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:
    - Provide a list of accounts with privileged access to the appropriate management approvers for review.
    - Support and encourage periodic review by Data Trustees for information covered under a Trustee's responsibilities.

Account and Authorization Audits

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 both by an administrative and technical manager;
3. The request is compliant with applicable regulation, policy, best practice;
4. The granted privileges were indeed required for the approved administrative use;
5. Requests for temporary privileges are expired on the agreed expiration date;
6. Every account is held by a person still 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 User to revocation of the privilege to use University Data or Information Technology or disciplinary action, up to and including termination of employment.

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