[Company Name] Access Control Policy and Procedures

Official Policy Title:	
Responsible Party:	
Approval Party:	
Effective Date:	
Last Update:	
Version Number:	
Policy Framework:	**Developed in accordance with NIST Special Publication (SP) 800 Series - https://csrc.nist.gov/publications/sp800 (NIST SP 800-53, rev. 5)**
Mapping	**NIST AC-1 to NIST AC-25**

Introduction

The Access Control policy and procedures referenced within this document define the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, this policy and procedures document is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Access Control policy and procedures are to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Access Control policy and procedures is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity.*
- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

Policy

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within this policy, or within a separate set of standard operating procedures (SOP), as needed:

Access Control Policy and Procedures [NIST AC-1]
The organization is to a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System Level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Account Management [NIST AC-2]
Management is vitally aware of the importance of proper account management regarding access control as this ultimately ensures only authorized users gain access to [company name] information systems, which in turn helps ensure the safety and security of organizational assets. Authorized personnel within [company name] are therefore responsible for a wide range of account management initiatives, beginning with properly identifying and documenting the relevant information system accounts to support, to ensuring users are removed from account access as needed. As such, [company name]'s account management initiatives consist of the following:

Define and Document the Types of Information System Accounts [NIST AC-2(a)]
Information system accounts used to access [company name]'s [name of information systems in scope] are to consist of all necessary account types that allow users to perform their necessary roles and responsibilities. Having different accounts that allow for varying levels of access is essential for ensuring the confidentiality, integrity, and availability (CIA) of the organization's information systems. The following types of accounts are utilized for [company name]'s [name of information systems in scope]:

[It is essential to provide a comprehensive overview of the main types of accounts used within the scope of the information systems being examined. Thus, you have individual accounts, shared/group accounts, administrator accounts, etc. Simply listing them below and providing any additional notes and comments will suffice. You do not have to be system specific. For example, it is not necessary to list administrator account information for servers and administrative account information for firewalls – just provide a brief overview in the "description" column as to what this account entails, what privileges is it afforded, etc.]

Business Function	List of Information System account types supporting the Business Function	Additional Notes and Comments
Describe the business function in brief detail, which is effectively the description of the information systems in scope.	(1). Individual Accounts	
	(2). Shared/Group Accounts	
	(3). Administrator Accounts	
	(4). Super-User Accounts	
	(5). Guest Accounts	
	(6). Vendor Accounts	
	(7). Temporary Accounts	
	(8). Other	
	(9). Other	
	(10). Other	

Assigning Account Managers [NIST AC-2(b)]

Assigning account managers is critical for ensuring that access control initiatives relating to [company name]'s information systems are assigned to knowledgeable and competent personnel. Account managers are critical to the overall access control lifecycle, as they assist in establishing roles, provisioning and deprovisioning users, along with many other essential initiatives. Account managers are to be selected

based on their experience, knowledge, and overall understanding of the information systems, and must also possess necessary expertise for performing various account management activities.

[The above information serves as an excellent starting point or placeholder, thus please change/modify as necessary, or simply leave as your answer if you feel it is a fair representation of the control.]

Establishing Conditions for Group and Role Membership [NIST AC-2(c)]

Establishing conditions for group and role membership onto information systems ensures that all levels and types of necessary access have been assessed and implemented, and that users have defined roles and responsibilities for the information systems they access. Authorized personnel, those with the requisite experience, knowledge, and overall understanding of the information systems, are to assess, determine, and then implement the necessary conditions for group and role membership. This is to be performed – when allowable – via group policy through directory services. Furthermore, group and role membership are a strict requirement that must be performed on isolated systems that do not utilize directory services.

[The above information serves as an excellent starting point or placeholder, thus please change/modify as necessary, or simply leave as your answer if you feel it is a fair representation of the control.]

Specifying Authorized Users of Information Systems [NIST AC-2(d)]

Authorized users are to have undergone [company name]'s provisioning process for new hires, which also is to include being assigned access rights to information systems. As such, select personnel are responsible for determining the systems for which users are to access, the type of access granted and the specific roles and responsibilities and overall access afforded, along with other attributes relating to their access rights. A critical element of access control is ensuring that users have the minimum access necessary for performing their mandated tasks, a concept known as Role Based Access Control (RBAC).

[The above information serves as an excellent starting point or placeholder, thus please change/modify as necessary, or simply leave as your answer if you feel it is a fair representation of the control.]

Approvals for Creating Information System Accounts [NIST AC-2(e)]

Creating information system accounts requires an assessment of the need for such an account, itss purpose, justification, and overall rationale. With a standardized set of information system accounts already in place – such as individual, group/shared, and administrator accounts – any additional accounts are to be created and implemented only if the current account types do not satisfy the information systems in question. All appropriate parties are to be involved in assessing and implementing any new information system accounts. If necessary, temporary/emergency accounts are to be created for the short term when there is a need for such accounts.

[The above information serves as an excellent starting point or placeholder, thus please change/modify as necessary, or simply leave as your answer if you feel it is a fair representation of the control.]

Creating, Enabling, Modifying, Disabling and Removing Information System Accounts [NIST AC-2(f)]

[Company name] system accounts for accessing information systems have been assessed for ensuring all necessary access rights are afforded to such systems, thus any changes – such as creating, enabling, modifying, and disabling information system accounts – is to be performed only when a noted technical, security, or operational justification exists. While there are many reasons for creating changes regarding

information system accounts – ranging from de-provisioning a legacy system to having a group of users de-provisioned from a certain account type – such actions are to be assessed and ultimately performed by authorized personnel. For any temporary/emergency accounts created, they are to be used only for short-term, then removed.

[The above information serves as an excellent starting point or placeholder, thus please change/modify as necessary, or simply leave as your answer if you feel it is a fair representation of the control.]

Monitoring Use of Information System Accounts [NIST AC-2(g)]

Information system accounts are to be monitored on a regular basis for ensuring such monitoring activities are commensurate to the needs of the organization, and that accounts are valid, justified, and accounts have not been created, enabled, modified, or disabled without the consent and knowledge of authorized personnel at [company name]. The monitoring of information system accounts is to include a regular review of all accounts being used for accessing information systems. Any discrepancies identified during this process are to be handled accordingly by appropriate personnel. For any temporary/emergency accounts created, they are to be used only for short-term, then removed. For any temporary/emergency accounts created, they are to be monitored also.

[The above information serves as an excellent starting point or placeholder, thus please change/modify as necessary, or simply leave as your answer if you feel it is a fair representation of the control.]

Notification to Account Managers [NIST AC-2(h)]

Account managers are to be notified when critical actions are performed on information system accounts, such as when accounts are no longer required, when accounts are modified, disabled, or added. Additionally, account managers are to be notified when users on such accounts are added, terminated, transferred, and when system individual users' roles have changed. System notifications are to be generated and reviewed by account managers to ensure they are aware of all activities, and that the associated actions are valid and justified. Any discrepancies identified during this process are to be handled accordingly by the appropriate personnel.

[The above information serves as an excellent starting point or placeholder, thus please change/modify as necessary, or simply leave as your answer if you feel it is a fair representation of the control.]