# Identity and Access Management (IAM) Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

Information system accounts are the only legitimate method by which [Company Name] information systems may be accessed. Without active account management, the potential exists that legitimate users can use these accounts for illegitimate purposes. Additionally, the potential exists that these accounts can be usurped and used illegitimately to access [Company Name]’s information systems.

The use of authorization, identification, and authentication controls ensures that only known users make use of information systems. Without authorization, identification, and authentication controls, the potential exists that information systems could be accessed illicitly and that the security of those information systems can be compromised. [Company Name] is using [insert technologies] to centralize account/identity management.

Passwords are the primary form of user authentication used to grant access to [Company Name]’s information systems. To ensure that passwords provide as much security as possible, they must be carefully created and used. Without strict usage guidelines, the potential exists that passwords will be created that are easy to break. This would allow easier illicit access to [Company Name]’s information systems, thereby compromising the security of those systems.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This Identity and Access Management (IAM) Policy applies to all information systems and information system components as well as all users of all information systems and information system components of [Company Name]. Specifically, it includes:

* Mainframes, servers, and other devices that provide centralized computing capabilities.
* SAN, NAS, and other devices that provide centralized storage capabilities.
* Desktops, laptops, and other devices that provide distributed computing capabilities.
* Routers, switches, and other devices that provide network capabilities.
* Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.
* Applications (on-premise and Cloud).
* External information services (Cloud/XaaS).
* All employees, whether employed on a full-time or part-time basis by [Company Name].
* All contractors and third parties that work on behalf of and are paid directly by [Company Name].
* All contractors and third parties that work on behalf of [Company Name], but are paid directly by an alternate employer.
* All employees of partners.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. All information system accounts will be actively managed by appropriate administrative staff. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.
2. Information system accounts are to be constructed such that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with that account. Further, accounts shall be created such that no one account can authorize, perform, review, and audit a single transaction to eliminate conflicts of interest.
3. Information system accounts are to be reviewed to identify accounts with inappropriate privileges (either too high or too low) on an *[indicate frequency – suggest quarterly]* basis. Should information system accounts be discovered with inappropriate privileges, those privileges will be manually reset to the established level.
4. Information system accounts are to be reviewed to identify inactive accounts. Should information system accounts that are associated with an employee or third party be discovered that have been inactive for *[indicate interval – suggest 30 days]*, the owners of the account will be notified of pending disablement. Should the account continue to remain inactive for *[indicate interval – suggest 30 days]* it will be manually disabled.
5. Login attempts to information systems will be restricted such that after *[indicate count – suggest five]* failed attempts within *[indicate interval – suggest fifteen minutes]*, they will be locked out. Lockout will be automatically lifted after *[indicate interval – suggest one hour]* or may be manually lifted by *[indicate process – suggest an identity-authenticated call to the help desk]*.
6. Prior to being granted access to an information system, each user must be provided with formal authorization by an appropriate official (i.e. the owner of the information system, the custodian of the data housed within the information system, or a designee of these individuals). This authorization will be based on definitive and verifiable identification of the user and will be logged by the authorizing official.
7. Once authorization has been granted, the user will be provided with a unique information system identifier. Examples of identifiers include user IDs and employee numbers. Additionally, the user will be provided with a unique information system authenticator that is tied to the assigned identifier. Examples of authenticators include passwords and tokens. Identifiers and authenticators will be delivered to the authorized user in such a manner as to ensure they are received only by the authorized user. To minimize risk, identifiers and authenticators for critical information systems will not be provided together.
8. Passwords must be constructed according to set length and complexity requirements. As such, passwords must be *[indicate length – suggest 8]* characters in length and must include *[character type – suggest letters (either upper or lower case), numbers, and special characters]* characters.
9. Passwords will have both minimum and maximum lifespan. As such, passwords must be replaced at a maximum of *[indicate interval – suggest 90 days]* and at a minimum of *[indicate interval – suggest 30 days]*.
10. Passwords may not be reused any more frequently than every *[indicate frequency – suggest 12]* password refreshes. Reuse includes the use of the exact same password or the use of the same root password with appended or pre-pended sequential characters.
11. Passwords are to be used and stored in a secure manner. As such, passwords are not to be written down or stored electronically except in Corporate-authorized systems *[e.g. Password Safe, Firefox Password Manager – include requirements if these are authorized]*.
12. Clear text credentials must not be embedded in applications or any other system; use of corporate standard encryption or an explicit written exception is required.
13. Passwords are to be obscured during entry into information system login screens and are to be transmitted in an encrypted format.
14. Passwords are to be individually owned and kept confidential and are not to be shared under any circumstances.
15. Vendor-supplied default and/or blank passwords must be changed immediately upon installation of the application, device, or operating system.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

Identify users via external identity verification methods prior to the issuance of accounts:

* + - * + As part of the on-boarding process, employee identity will be verified by *[indicate responsible department]* through the use of government-issued identification documents that include the following information:

*Full name.*

*Signature.*

*Photograph.*

Create user accounts to optimize security:

* + - * + Accounts must be created with the minimal set of permissions (also known as least privilege) and functions (also known as job segregation) as required by the role. Accounts should be created with the following restrictions:

*System administrative access (install, configure, modify, and patch system software).*

*Account administrative access (create, delete, and modify accounts and permissions).*

*Review administrative access (review activities of other administrators).*

*Full content access (read, write, edit, and delete data).*

*Limited content access (read, write, and edit data).*

*Restricted content access (read and write data).*

*Minimal content access (read data).*

Each system user is to be provided with an identifier and an authenticator such that they can uniquely and individually access the system:

* + - * + Accounts must be created in *[indicate IAM system(s) where accounts will reside]* unless explicitly accepted in writing.

Any new applications or systems must be integrated with the Identity and Access Management system unless explicitly accepted.

* + - * + For grandfathered and excepted applications:

Identifiers must be unique to the individual, but can be common across systems.

User identifiers (User IDs) should be constructed in one of the following manners:

* + - * *First initial and last name (or first 8 characters).*
			* *First name and last name.*
			* *First name, underscore, and last name.*
			* *First name, period, and last name.*
			* *[Indicate preferred User ID construction method]*

Passwords must be unique to each individual and each system

The identifiers and authenticators associated with each account must be distributed in such a manner as to ensure they are delivered only to the personnel to whom they are assigned:

* + - * + Identifiers are to be distributed in a manner that eliminates repudiation of receipt.
				+ Authenticators are to be distributed in a manner that protects their secrecy and eliminates repudiation of receipt.

Actively manage user accounts on information systems:

* + - * + Perform user account review to ensure that users are provided with appropriate accounts and account permissions:

*Validate each system user’s role within the organization.*

*Review system accounts and account permissions for each user.*

*Validate that each user’s account and account permissions meet the requirements established by role.*

* + - * + Should account review determine that users have insufficient accounts or account permissions, the required accounts and/or permissions must be provided:

*Where accounts exist, but permissions are insufficient, modify the account to include appropriate permissions as per the requirements of the positional role.*

*Where accounts do not exist, create accounts with appropriate permissions as per the requirements of the positional role.*

*Review created accounts and assigned permissions to ensure they meet the requirements of the role.*

* + - * + Should account review determine that users have inappropriate accounts or account permissions, those accounts and/or permissions must be rescinded:

*Eliminate extraneous permissions in allowed accounts.*

*Revoke access to and eliminate permissions in extraneous accounts.*

*Review system logs to catalog the activity of the account.*

*Upon completion of all review and investigation, permanently delete any extraneous accounts.*

Once a system account is no longer required, it must be disabled to prevent its use and archived to provide for potential future investigation:

* + - * + Where account access is still required by any person, identifiers and authenticators will be reset.
				+ Where account access is no longer required, identifiers and authenticators will be deleted along with the account.

### Compliance

Each system owner is required to document all procedures related to access control. Owners must have that documentation on hand if required for auditing purposes. The following documentation must be available for auditing purposes: demonstration of account approval, termination, and any disabling of accounts.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of e-mail access;
2. Disciplinary action according to applicable [Company Name] policies;
3. Termination of employment; and/or
4. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |