# User Authorization, Identification, & Authentication 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.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# 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.

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 be compromised.

Where feasible, federated identity mechanisms should be used to integrate access controls of cloud services and mobile devices with internal 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 User Authorization, Identification, & Authentication Policy applies to all users of all information systems that are the property of [Company Name]. Specifically, it includes:

* 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 and clients of [Company Name] that access [Company Name]’s non-public information systems.
* Access to desktops, laptops, smart phones, tablets, and other devices that provide distributed computing capabilities.
* Access to cloud services leased or purchased by [Company Name], including but not limited to, infrastructure as a service, platform as a service, and/or software as a service.

# 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. 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.
2. 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.
3. Should an information system user’s account be disabled for any reason, the user’s identifier and authenticator will also be disabled, where applicable.

**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.

**Procedure 1**

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

* + - * + As part of the on-boarding process, employee identity should be verified through the use of government-issued identification documents that include the following information:

Full name.

Signature.

Photograph.

**Procedure 2**

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

* + - * + 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 name, initial, and last name.

First name and last name.

First name, underscore, and last name.

First name, period, and last name.

* + - * + Authenticators must be unique to each individual and to each system; however, a master authenticator may be used to access individual system authenticators (a single sign-on system).

**Procedure 3**

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.

**Procedure 4**

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.

# 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. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Agreement

Include a section that confirms understanding and agreement to comply with the policy. Both signatures and dates are required. A sample statement is provided below.

I have read and understand the [name of policy]. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

# Revision History

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.