# MFA 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.

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. [Company Name] is using [insert technologies] to centralize account/identity management.

While passwords are still the primary form of user authentication used to grant access to [Company Name]’s information systems, multi-factor authentication methods are being introduced, such as tokens. To ensure the proper usage of both, the following must be considered:

* Passwords must be carefully created and used.
* Tokens, hard or soft, must be handled carefully, with proper processes in place for replacements.
* Other multi-factor authentication methods, such as OOB SMS or email options, must be treated similarly. Monitor and update frequently as user-related changes are required.

# 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 Multi-Factor Authentication Management Policy applies to the following user communities, information systems, and information system components:

* On-premise sensitive applications (users with admin rights)
* Cloud-based applications (users with admin rights)
* Sensitive databases (users with admin rights)
* Core routers and switches (users with admin rights)
* Sensitive AIX servers (users with admin rights)
* Sensitive windows servers (users with admin rights)
* Active Directory servers (users with admin rights)
* Critical security appliances, other than VPN (users with admin rights)
* IPSEC VPN (all users from remote access)

# 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, including the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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]*.
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.
8. 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 that they are received only by the authorized user. To minimize risk, identifiers and authenticators for critical information systems will not be provided together.
9. Revocation of tokens: Inappropriate handling of tokens, such as token sharing, will result in an initial warning. Upon a repeated offence, the token will be revoked and an alternative must be established.
10. Token replacement: If the token is no longer functioning properly, the token authorizer must be notified prior to a new token being issued for records to be updated.
11. Reporting loss and theft: The token authorizer must be notified before any related investigation is initiated, and replacements are provided.
12. 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.
13. Passwords will have a 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]*.
14. 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.
15. 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]*.
16. 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.
17. Passwords are to be obscured during entry into information system login screens and are to be transmitted in an encrypted format.
18. Passwords are to be individually owned and kept confidential and are not to be shared under any circumstances.
19. 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.

# 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.