AUTHENTICATION STANDARD

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Standard Statements 4

2.1 Authentication Factors 4

2.2 Two-Factor & Multi-Factor Authentication 4

2.3 Authentication Minimums 4

2.4 Password Authentication 4

2.4.1 Password Secrecy 4

2.4.2 Password Syntax Requirements 5

2.4.3 Password Expiration 5

2.4.4 Password History 6

2.4.5 Password Change and Verification 6

2.4.6 System Lockout 6

2.5 Use of Tokens 6

3. Standard Compliance & Enforcement 7

3.1 Compliance Measures 7

3.2 Enforcement 7

4. Exception Process / Glossary 8

4.1 Exception Process 8

4.2 Glossary / Acronyms 8

5. Document Management 9

5.1 Document Revision Log 9

5.2 Document Ownership 9

5.3 Document Coordinator 9

5.4 Document Approvers 9

5.5 Distribution 9

# Introduction

## Document Definition

This document is a Standard.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Objective

The objective of this standard is to provide global information security requirements to help ensure that authentication parameters on XXXX (XXXX) systems are standardised in order to satisfy all relevant compliance and regulatory commitment and as it relates to best practices and general IT controls.

This standard covers all XXXX information technology assets in all Production, Staging (QA), and Development environments that require access control. This includes, but is not limited to, Identity and Access Management Systems (IAMS), applications (bespoke and CoTS), software and hardware.

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Standard applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Standard statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Standard applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-POL-ALL-009 - Access Control Policy*

# Standard Statements

## Authentication Factors

XXXX recognises 3 factors of authentication:

1. Knowledge: A secret known only to the end user. e.g. password or PIN
2. Possession: Something only the user has e.g. security token
3. Inheritance: A unique identifier of the end user themselves e.g. biometrics

## Two-Factor & Multi-Factor Authentication

While two-factor is a form of multi-factor authentication, XXXX recognises the following difference:

* Two-Factor Authentication (2FA) – The use of a single instance each of two of the three available Authentication Factors. *e.g. a username/password (knowledge), plus an RSA token (possession)*.
* Multi-Factor Authentication (MFA) – The use of a single instance of all three available Authentication Factors. *e.g. a username and password, AND an RSA token AND fingerprint, OR multiple instances of two or more factors. e.g. username/password AND PIN, plus RSA Token AND VPN certificates*.

## Authentication Minimums

The minimum authentication standard to be applied to access to all relevant XXXX assets is Username and Password, or equivalent.

## Password Authentication

### Password Secrecy

Passwords must:

* Be kept secret and never shared;
* Not be displayed on screen or on printouts
* It must NOT contain many consecutive characters (such as "abcd")
* It must NOT contain many repeating characters (such as "aaabbb")
* It must NOT contain dictionary words
* It must NOT contain proper names
* It must NOT contain the words XXXX or any derivation
* It must NOT be made of birth dates and other personal information such as addresses and phone numbers
* It must NOT be made up of names family members, co-workers
* Passwords must not be shared
* Passwords must NOT be inserted into email messages or other forms of electronic communication and must not be exchanged over the phone communication.
* Where the password complexity is not achievable then 2FA should be considered

### Password Syntax Requirements

Passwords must:

* Not be the same as, or contain the user ID;
* Contain a minimum of eight (8) characters;
* Contain a capital letter, number and a special character
* All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed at least every 90 days.
* All system-level administrative accounts should be renamed i.e. changed from the default username “administrator”
* All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
* User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
* All active vendor accounts must be monitored when not in use and ports deactivated when not in use.
* User accounts will be locked automatically after 3 invalid logon attempts until reset requested is granted.
* All default vendor passwords must be changed at installation to a unique password that follows the rules set in this policy.
* Standard defaults of "public," "private" and "system" and must be different from the passwords used to log in to the systems interactively. A keyed hash must be used where available (e.g., SNMPv2).
* Every user in the system must be distinctively identified with the assigned unique user-Id
* User account not used (inactive) within the period of 90 days MUST be deleted or disabled.
* Resigned or terminated employee’s account must be removed immediately after notification from HR by the System Administrator.
* Every user-ID established for a non-employee must have a specified expiration date. If the systems administrator setting-up such a user-ID is not provided with an expiration date, then a maximum of 5 working days shall be used as the default.

### Password Expiration

Passwords must expire after 90 days. Automatic notifications of the pending expiration should be provided to the user beginning at day seven (7) before the expiration date (where available).

### Password History

Password history must be maintained that prohibits users from:

* Using one of their previous 10 passwords;

### Password Change and Verification

Temporary and reset passwords that are issued to users must be a unique value and changed on first use.

New passwords must be verified before the change is accepted.

### System Lockout

Systems must allow only three (3) consecutive attempts to enter a valid password. After the fourth attempt using an incorrect password, an ID must be locked requiring the user to call IT helpdesk for a password reset or unlock automatically after 30 minutes

## Use of Tokens

Where applicable, soft tokens shall be in use for logon to applications and system resources. The complete token credentials will consist of a 4-digit pin and a 6-digit one-time password (OTP).

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| For a selection of passwords, evidence that the passwords are not or do not contain the user ID | * Screenshots of system password policy/configuration settings * Password security tool report data |
| For a selection of passwords, evidence that passwords have been changed every 45 days | * Screenshots of system password policy/configuration settings * Screenshots or logs of password change history |
| For a selection of passwords, evidence that the passwords contain a minimum of 8 alphanumeric and special characters | * Screenshots of system password policy/configuration settings * Password security tool report data |
| For a selection of passwords, evidence that the passwords have not been reused within a last 10 passwords | * Screenshots of system password policy/configuration settings * Screenshots or logs of password change history |
| For a selection of systems, evidence that the system locks after 3 invalid attempts and remains locked till reset by IT helpdesk or unlock automatically after 30 minutes | * Observe that 3 invalid login attempts lock the system * Observe that the system remains locked till reset by IT helpdesk |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Standard statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Glossary / Acronyms

|  |  |
| --- | --- |
| 2FA | Two-Factor Authentication |
| MFA | Multi-Factor Authentication |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |

## Distribution

Distribution is to all staff