ACME ROCKETS LTD.

AUTHENTICATION STANDARD

Revision: r1.0

Effective Date: 01-JAN-20

Classification: INTERNAL

Table of Contents

1. Introduction

1.1 Document Definition

This document is a Standard.

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

1.2 Objective

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

The scope of this standard includes all ARL 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.

1.3 Scope

1.3.1 Applicability to Employees

ARL refers to Acme Rockets Ltd. 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.

1.3.1 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.

1.3.2 Applicability to Assets

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

1.4 Related Documents / References

- *ARL-POL-001 - Information Security Policy Framework*
- *ARL-POL-009 - Access Control Policy*

2. Standard Statements

2.1 Authentication Factors

ARL 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

2.2 Two-Factor & Multi-Factor Authentication

While two-factor is a form of multi-factor authentication, ARL 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*.

2.3 Authentication Minimums

The following authentication minimums will be applied to access to all relevant ARL assets:

- PUBLIC – username and password
- INTERNAL – username and password
- COMMERCIAL IN CONFIDENCE - 2FA
- RESTRICTED - MFA

2.4 Password Authentication

2.4.1 Password Secrecy

Passwords must:

- Be kept secret and never shared
- Not be displayed on screen or on print-outs

2.4.2 Password Syntax Requirements

Passwords must:

- Not be the same as, or contain the user ID
- Contain a minimum of 8 (eight) characters
- Contain at least 3 of 4 factors

2.4.3 Password Expiration

Passwords must expire after 45 (forty-five) days. Automatic notifications of the pending expiration should be provided to the user beginning at day 6 (six) days (where available).

2.4.4 Password History

Password history must be maintained that prohibits users from:

- Using one of their previous 10 (ten) passwords
- Reusing a password within a 10 (ten) period

2.4.5 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.

2.4.6 System Lockout

Systems must allow only 15 (fifteen) minutes consecutive attempts to enter a valid password. After the fourth attempt using an incorrect password, an ID must be locked, requiring the user to either wait 30 (thirty) minutes before attempting to log in again or call IT Department for a password reset.

3. Standard Compliance & Enforcement

3.1 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 (forty five) days	• Screenshots of system password policy/configuration settings • Screenshots or logs of password change history
For a selection of passwords, evidence that the passwords contains a minimum of 8 (eight) alphanumeric characters	• Screenshots of system password policy/configuration settings • Password security tool report data
For a selection of passwords, evidence that the passwords contain at least 3 of 4 factors	• 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 10 (ten) period, or the last 10 (ten) 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 15 (fifteen) minutes invalid attempts and remains locked for 30 (thirty) minutes	• Observe that six invalid login attempts locks the system • Observe that the system remains locked for a minimum of one hour

3.2 Enforcement

As noted above, this Standard applies to all Acme Rockets Ltd. employees, officers, members of the Board of Directors, and all consultants and contractors. Violations of this Standard may result in disciplinary action, up to and including termination of employment and / or legal action.

4. Exception Process / Glossary

4.1 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 *ARL-POL-001 - Information Security Policy Framework*.

4.2 Glossary / Acronyms

2FA	2-Factor Authentication
MFA	Multi-Factor Authentication

5. Document Management

5.1 Document Revision Log

Date	Editor	Revision #	Description of Change
15-Dec-19	B. Bunny	r0.1	Initial draft.
29-Dec-19	B. Bunny	r1.0	Approved initial release.

5.2 Document Ownership

This Standard is owned by the CTO.

5.3 Document Coordinator

This Standard is coordinated by the IT Director.

5.4 Document Approvers

Approver Name	Signature	Date
Marvin Martian/CTO	[SIGNATURE HELD ON FILE]	01-Jan-20