ACME ROCKETS LTD.

ACCESS CONTROL POLICY

Revision: r1.0

Effective Date: 01-JAN-20

Classification: INTERNAL

INTERNAL INFORMATION

This is a proprietary document and is the property of Acme Rockets Ltd.; 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 Acme Rockets Ltd..

Table of Contents

1. Introduction

1.1 Document Definition

This document is a Policy.

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

1.2 Objective

The objective of this policy is to provide global information security requirements to:

- Protect against unauthorised access to data owned by or in the custody of Acme Rockets Ltd. (ARL);
- Protect against unauthorised access to computer systems, applications, or operating systems;
- Allow only authorised users the appropriate level of access to the information or portion of the system, application or operating system necessary to accomplish designated responsibilities, i.e., business need to know
- Ensure users are accountable for safeguarding their authentication information

This Policy applies to all systems and applications that utilise an access control system to protect resources from unauthorised access including all development, staging and production environments.

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 Policy applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

1.3.1 Applicability to External Parties

Relevant Policy 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 Policy 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-004 - Data Classification Policy*
- *ARL-POL-010 - Remote Access Policy*
- *ARL-STD-008 - Authentication Standard*
- *ARL-PRC-017 - Policy Exception Procedure*

2. Policy Statements

2.1 Access Authorisation

Access to ARL's internal and external Information System Assets must be protected through a combination of security controls, including network segmentation, authentication mechanisms and other security controls to prevent and detect unauthorised access while providing secure access to authorised users and systems.

2.2 Role-Based Access Control

All access to ARL systems and resources will be based on 'least privilege' to perform the individuals' job function and/or classification, and be in accordance with ARL Policies.

All access not explicitly allowed and documented will be denied.

2.3 Non-Interactive Accounts

Automated accounts used for system-to-system interfaces (service accounts) must be controlled tightly and managed in accordance with the InfoSec Department security Standards.

These accounts must have a designated and accountable owner and must not be used by individuals.

2.4 Group / Shared Accounts

Group or shared accounts are strictly prohibited unless mechanisms are in place to tie all access and actions taken to an individual.

2.5 Non-Password Authentication

Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be:

- assigned to an individual account and not shared among multiple accounts
- controlled (physically and/or logically) to ensure that only the intended account can use that mechanism to gain access.

2.6 Access Notification / Login Banner

Prior to accessing systems, a user must be notified that access is for authorised use only. The IT Department will ensure that login banners are implemented to display on all ARL workstations, servers, network components and applications to inform users that the system is for ARL use and that user activities may be monitored.

2.7 Third Party / Vendor Accounts

Third Party/vendor access to systems and data must be enabled only when required (and specified in the contractual Service Level Agreements) and all activity must be monitored in accordance with applicable ARL Standards.

2.8 Database Access

Access to ARL databases containing data of RESTRICTED of above must comply to the following rules:

- all non-DBA access to, queries of, and actions on databases are through programmatic methods
- application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

2.9 *User Registration and De-Registration*

Access to systems or system functions must be limited to authorised users only. Access to systems must be based on a valid, unique user identity in order to ensure traceability and accountability.

Procedures for the registration and de-registration of users shall be established by teams performing user administration tasks and must conform to the security standards set forth by the InfoSec Department.

2.10 *User Access Provisioning*

Information Asset Owners must ensure that prior to the creation and granting of access, or change of access privileges, user identities are subject to an authentication and authorisation process that tracks and documents access request detail and final approval.

Privileges assigned in conjunction with access IDs will be based on the principle of least privilege, meaning users will be granted only the minimum level of permissions required to perform the duties of their job.

The process will incorporate separation of duties (requestors, approvers, and implementers must be separate individuals) and shall restrict the assignment of explicit permissions based on those granted to an existing user ID except where the use of role-based access groups is used.

2.11 *User Identity Authentication*

User identities must be authenticated prior to system access.

2.12 *Management of Privileged Access Rights*

The allocation of privileged access (e.g., local administrator, domain administrator, super user, root access) must be restricted and controlled and not provided by default. Authorisation for the use of such accounts shall be provided explicitly on the required ticket approval workflow process.

The emergency use of privileged access rights must follow a documented credentials/account release process consistent with InfoSec Department Standards and be limited to the duration of the emergency.

InfoSec Department will investigate suspected misuse of privileged access promptly in conjunction with members of the IT Department, where appropriate, and in compliance with applicable law. Abuse of privileged access will be subject to disciplinary action in accordance with ARL Policies.

2.13 *User Repository*

A file or database containing details of all authorised users must be established and maintained by designated individuals, such as system administrators, and protected against unauthorised change or disclosure.

2.14 *User Identity & Access Reviews*

Details of authorised user identities and access rights must be reviewed at least semi-annually, and after any status change such as promotion, demotion and transfer to ensure that access privileges remain appropriate to the user’s current role.

Reviews of user identities and access rights for privileged (“super user”) accounts must take place semi-annually.

Account reviews of selected systems must take place after an incident or when ordered by the Governance Committee or Internal Audit.

2.15 Access Modification

A process for modifying the access privileges of users must be established to ensure that authentication details and access privileges are updated within a reasonable time-period and unnecessary access is removed (e.g. for movers and leavers).

2.16 Access Termination

A process for terminating the access privileges of users must be established to ensure that authentication details and access privileges are revoked promptly.

2.17 Use of Authentication Data

Where not programmatically supported, all users are responsible for creating strong passwords and for ensuring the confidentiality of their passwords.

All users are prohibited from storing passwords in an unsecure manner or sharing their passwords with another person. Actions taken on behalf of others need to utilise appropriate delegation tools and mechanisms and must not be accomplished by sharing individual passwords.

Any use of another’s identity and authentication for logging into any ARL network or computer system is considered masquerading and is prohibited.

2.18 Authentication

The minimum level of user authentication is username and password.

System and organisational controls must be in place to enforce the selection of strong passwords and the secure handling and management of passwords, including:

- Password length and complexity
- Password change and re-use
- Minimum and maximum password age
- Password history
- System Lockout

Full password specifications can be found in the *ARL-STD-009 - Authentication Standard*.

Where other authentication mechanisms are used (physical or logical security tokens, smart cards, certificates, badges, keys), use of these mechanisms must be:

- Assigned to an individual account and not shared among multiple accounts
- Controlled (physically and/or logically) to ensure that only the intended account can use that mechanism to gain access

These ARL-provided access control hardware devices are the property of ARL and subject to return immediately upon request, separation of employment, or termination of a working agreement.

2.19 Inactivity Timeout

User inactivity time-outs must be implemented, where technically feasible, for terminals and workstations which access COMMERCIAL IN COMFIDENCE or RESTRICTED information, as defined by the *ARL-POL-004 - Data Classification Policy*. The time-out interval should be based on business need, risk level and exposure, or compliance requirement.

2.20 Unattended Devices

Unattended information system assets (e.g. computers or mobile devices) must be protected from unauthorised use by a key lock or an equivalent control.

2.21 Disabling Access for Misuse

In specific cases when misuse of a user identity is suspected, user access must be disabled immediately.

2.22 Alerting

Access violations above a pre-defined threshold must be identified and must trigger an alert. Alerts must be followed by an effective response.

2.23 Access Logging & Monitoring

Relevant details regarding successful and unsuccessful system access attempts must be logged. Logs must be reviewed and reliably retained in accordance with local standards/procedures and retention periods. The review must be followed by an effective response.

2.24 Authentication Credential Encryption

Where applicable, any form of authentication in place must conform to best business practices related to encryption of credential both in transit, and in storage.

2.25 Authentication Management Systems

Systems used to manage authentication processes must conform to [INFOSEC_DEPT_NAME] security Standards.

2.26 Special Access and Use of Privileged Utility Programs

Special access privileges and system/administration utilities which override system or application controls must be controlled tightly and restricted to a limited number of approved individuals.

Where an automated access control mechanism cannot be employed, dual knowledge/split control must be enforced.

2.27 Access Control to Program Source Code

Access to program source code, designs, specification, and related artefacts must be strictly controlled in order to protect against unauthorised changes to functionality as well to maintain the confidentiality of valuable intellectual property.

Source code shall be retained in a centralised repository designated by the Head of IT.

Segregation of duties controls must be applied to ensure that the same person does not have access to program source code and write access to the production systems executing the same code.

2.28 Access Control Review

At least annually, the access control mechanisms and processes used within the ARL environment will be reviewed for continued suitability and appropriateness.

2.29 Authentication Mechanism Review

At least annually, the authentication mechanisms used within the ARL environment will be reviewed for continued suitability and appropriateness.

3. Policy Compliance & Enforcement

3.1 Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. 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 sample of systems, user lists and evidence authorising those users for access to the respective systems or system functions.	• Identity management system configuration and/or workflow • Approved user access request forms
Evidence that a notification of authorised use is presented prior to system access.	• New hire training materials • Email notification with system credentials • System logon banners
For a sample of systems and system functions, evidence that access is restricted to authorised users based on authentication.	• System / network device configuration information • Screen shots evidencing an authentication failure
Evidence of user identity authentication requirements.	• System / network device configuration information • Authentication syntax policy / rule information
For a selection of terminal or workstations with access to sensitive information, evidence of the time-out configuration and evidence that the time-out value is operating effectively.	• System / network device configuration information • Example time-outs (screen shots)
Evidence of access blocking tools or configurations and a test of their effectiveness.	• System / network device configuration information
Evidence of system access alert threshold and trigger configuration and a test of their effectiveness.	• System / network device configuration information • Audit logging tool output • Intrusion detection / prevention tool output
For a selection of system access logs, evidence of relevant details, log review schedules, completed reviews, and action items resulting in reviews.	• System / network device configuration information • Audit logging tool output • Log review tool output • Manual log review sign-off • Configuration of exception-based reporting
A sample of the identity database or file, configuration of the database or file, and relevant protection measures.	• System / network device configuration information
For a selection of special access identities or utilities, a list of authorised users with special access privileges, the associated approvals for such access, and evidence of access reviews.	• Identity management system configuration and/or workflow • System generated access reports • Approved user access request forms, emails, etc. • Periodic review sign-off on system generated access reports or within Identity management system or other tool
For a selection of user identities, evidence that access reviews are completed on a periodic basis.	• Identity management system configuration and/or workflow • System generated access reports • Periodic review sign-off on system generated access reports or within Identity management system or other tool

Evidence of an approved identity termination procedure.	• Identity management system configuration and/or workflow • System generated access reports • Workflow ticketing system output

3.2 Enforcement

This Policy applies to all Acme Rockets Ltd. employees, officers, members of the Board of Directors, and all consultants and contractors. Violations of this Policy 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 Policy 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

RBAC	Role-Based Access Control

5. Document Management

5.1 Document Revision Log

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

5.2 Document Ownership

This Policy is owned by the COO.

5.3 Document Coordinator

This Policy is coordinated by the IS Manager.

5.4 Document Approvers

Approver Name	Signature	Date
R. Runner/COO	[SIGNATURE HELD ON FILE]	01-Jan-20