AUTOMATED SYSTEM USER ACCESS CONTROL POLICY

AUTOMATED SYSTEM USER ACCESS CONT

Effective Date: January 15, 2024

Document Number: POL-SEC-2024-001

Version: 2.0

Supersedes: Version 1.4 (March 2023)

Policy Owner: Information Security Department

Approved By: Board of Directors, Polar Dynamics Robotics, Inc.

1. PURPOSE AND SCOPE

1 This Automated System User Access Control Policy ("Policy") estab

2 This Policy applies to all employees, contractors, consultants, tempo

2. DEFINITIONS

1 "Automated Systems" means all Company-owned or operated comp

2 "Access Rights" means the level of system privileges granted to a U

3 "Critical Systems" means systems directly involved in the operation

3. ACCESS CONTROL PRINCIPLES

1 Least Privilege: Users shall be granted the minimum level of access

2 Need-to-Know: Access to Critical Systems shall be granted only to U

3 Segregation of Duties: No single User shall be granted access rights

4. ACCESS AUTHORIZATION PROCEDURES

1 Access Request Process

a) All access requests must be submitted through the Company's Acc System

b) Requests must include business justification and manager approva

c) Critical Systems access requires additional approval from the Chief Officer

2 Access Review and Approval

a) Information Security shall review all access requests within 48 hour

b) Temporary access shall not exceed 90 days without renewal

c) Emergency access procedures require CTO or CISO approval

5. AUTHENTICATION REQUIREMENTS

1 All Users must authenticate using:

a) Multi-factor authentication for Critical Systems access

b) Complex passwords meeting NIST standards

c) Biometric verification for physical access to robot testing facilities

2 Password Requirements

a) Minimum 14 characters

b) Combination of uppercase, lowercase, numbers, and symbols

c) Changed every 90 days

d) No reuse of previous 12 passwords

6. ACCESS MONITORING AND AUDIT

1 System Access Logs

a) All access attempts shall be logged and retained for 12 months

b) Failed access attempts shall trigger security alerts

c) Quarterly access audit reviews shall be conducted

2 Compliance Monitoring

a) Automated monitoring of access patterns

b) Regular penetration testing of access controls

c) Annual third-party security assessments

7. TERMINATION AND MODIFICATION OF ACCESS

1 Access Termination

a) Immediate revocation upon employment termination

b) 24-hour maximum for contractor access removal

c) Documented verification of access removal

2 Access Modification

a) Review required for role changes

b) Annual recertification of access rights

c) Automated removal of dormant accounts after 60 days

8. POLICY VIOLATIONS AND ENFORCEMENT

6

1 Violations of this Policy may result in:

a) Immediate access suspension

b) Disciplinary action up to termination

c) Legal action where applicable

2 All violations must be reported to:

a) Information Security Department

b) Human Resources

c) Legal Department for review

9. POLICY REVIEW AND UPDATES

1 This Policy shall be reviewed annually by the Information Security D

a) Industry best practices

b) Regulatory requirements

c) Technology changes

d) Business needs

10. APPROVAL AND EXECUTION

This Policy is approved and executed by the undersigned authorized representatives of Polar Dynamics Robotics, Inc.

APPROVED BY:

Dr. Elena Frost

Chief Executive Officer

Date: January 15, 2024

Marcus Chen

Chief Technology Officer

Date: January 15, 2024

Victoria Wells

Chief Financial Officer

Date: January 15, 2024