Aberrant Open-ISM™

ACCESS CONTROL POLICY

Property	Description
Document Version	1.0
Status	DRAFT
Last Update	2022-03-25
Document Owner	Risk Management
Next Scheduled Review	

PROPRIETARY

Document Approvals		
Approver Name	**Title**	**Date**
???	???	???

Revision History			
Version	**Date**	**Description of Changes**	**Revised by**
1.0	2022-03-25	DRAFT	Aberrant

TABLE OF CONTENTS

1 OVERVIEW

Consistent standards for network access and authentication are critical to the company's information security and are often required by regulations or third-party agreements. Any user accessing the company's computer systems has the ability to affect the security of all users of the network. An appropriate Access Control Policy reduces risk of a security incident by requiring consistent application of authentication and access standards across the network.

2 SCOPE AND PURPOSE

2.1 SCOPE OF POLICY

The scope of this policy includes all users who have access to company-owned or company-provided computers or require access to the corporate network and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the corporate network. Public access to the company's externally-reachable systems, such as its corporate website or public web applications, are specifically excluded from this policy.

2.2 PURPOSE OF POLICY

The purpose of this policy is to describe the steps that must be taken to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with company standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

3 POLICIES

3.1 USER ACCOUNT MANAGEMENT

Users should only be provided with access to the network, network services and applications that they have been specifically authorized to use.
Network based account management requires creating or modifying records in our domain controller. Network accounts are enabled to use internal web-based resources using Integrated Authentication via Kerberos.

3.1.1 ACCOUNT REGISTRATION

A new account requires a change control request. During initial account setup, certain checks must be performed to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID and coordination with Human Resources is required.
- Accounts must be created using a standard format: [first initial] + [last name] all lowercase.
- Accounts must be distinct—identical account names must not be allowed.
- fUsers will be initially granted the least amount of network access required to perform their respective job function.
- Users will be granted access only if he or she accepts the Acceptable Use Policy.
- Access to the network will be granted in accordance with the Acceptable Use Policy.

3.1.2 USER SECRETS

- If an administrator creates a new user account on the network this will initially create a one-time password that the user who takes possession of the account must use to logon to the network. Once the user has logged on he / she is required to create a new password.
- User secrets are stored in encrypted hashes that are salted for each user and conform to <<Company Name>>'s encryption policy.
- If an account is locked, or if the user forgets his / her password, the user is provided with a mechanism that will allow them to reset their password in a way that allows them to keep their new password secret.
- One-time passwords disseminated over the network should always be transmitted via secure means.

3.1.3 ACCOUNT USE

Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be password protected (refer to the Password Policy for more detailed information).
- Accounts must be for individuals only. Account sharing and group accounts are not permitted.
- User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function.
- Occasionally guests will have a legitimate business need for access to the corporate network. When a reasonable need is demonstrated, temporary guest access is allowed.

3.1.4 ACCESS PROVISIONING

Logical access to stored data is restricted to authorized personnel. Modification of account permissions requires a change control request as relates to new hires, rights grant, or a role change of a user. The change control should be explicitly tagged as an 'Access Control' request for audit purposes, and must be approved by management.

3.1.5 REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS

<<Company Name>> adheres to a least privileges model that adheres to segregation of duties. Users are granted access to resources required to perform job duties. In the event that a user no longer requires specific access rights to perform work their access rights should be removed via the change control process. As a guideline, access rights should be time-bound when possible.

3.1.6 ACCOUNT DE-REGISTRATION

Removing an account requires a change control request. When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at the company, that employee's account can be disabled. Human Resources must create a process to notify the IT Manager in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.). Time based access control will also be utilized on accounts requiring finite access; the account will be configured to expire upon time period completion.

Account access should be deprovisioned within 24 hours when an user ends their employment with <<Company Name>>.

3.1.7 DORMANT ACCOUNT REMOVAL

Disable any dormant accounts after a period of 45 days of inactivity.

3.1.8 USER ACCOUNT REVIEW

- Review Change Control tickets for Access Control and correlate change requests to changes in user permissions at least monthly. Determination if changes were properly authorized or improperly modified.
- Review of any new accounts or generic accounts and their use.
- Analysis of modifications to existing accounts such as privilege escalation.
- Management of open user account issues.
- Determination if changes were properly authorized or improperly modified.

3.2 AUTHENTICATION

For internal users who utilize a Domain Controller or an SSO provider, where supported, we have implemented rules that enforce <<Company Name>>'s password security policy. For internal web-based applications that exist behind our firewall we support Integrated Authentication using Kerberos.
<<Company Name>>'s web-based application utilizes authorization tokens to ensure data integrity and the authentication of a request. Google Authenticator is used for two-factor authentication.

3.3 AUTHORIZATION MODEL

<<Company Name>>'s network conforms to the Windows Authorization Model. Access to resources on the <<Company Name>> network is managed by security groups (RBAC) on domain controller.
<<Company Name>>'s web-based application leverages ASP.NET Core's role-based authorization which utilizes a RBAC model for authorization.

3.3.1 DATA ACCESS AUTHORIZATION

Database user access is restricted via role-based security privileges defined within the access control system.

3.4 ADMINISTRATIVE ACCESS

<<Company Name>> adheres to the principle that the least required level of permissions should be assigned to each user based on their job function. User access permissions are reviewed at least quarterly by management.

3.4.1 MFA

All administrative account access whether managed on-site or through a third-party provider requires the use of two-factor authentication (such as smart cards, tokens, or biometrics).

3.4.2 DEDICATED ADMINISTRATOR ACCOUNTS

Administrator privileges are restricted to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

3.5 VPN

VPN user access is restricted via role-based security privileges defined within the access control system. The ability to administer VPN access is restricted to user accounts accessible by appropriate personnel. VPN users are authenticated via multifactor authentication prior to being granted remote access to the system.

3.6 USE OF PASSWORDS

When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to the company's password policy.

3.7 PASSWORD POLICY

In order to enforce strict adherence to the <<Company Name>> password policy, it is a requirement that password policy is enforced via application rules or group policies.

3.7.1 PASSWORD CREATION

- History: Passwords must be different that the previous 24 passwords.
- Length:
  - User Accounts: Passwords must be ten (10) or more characters in length.
  - Service Accounts: Passwords must be twenty (20) or more characters in length unless limited by the system.
- Complexity: Passwords must contain at least one of the following:
  - One numeric character.
  - One alpha character.
  - One uppercase character.
  - One non-alpha-numeric character.

3.7.2 PASSWORD PROTECTION

- Group passwords are prohibited with a few noted exceptions: e.g. access to the guest wireless account.
- Individual passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential <<Company Name>> information.
- Password should never be transmitted via unencrypted transport.
- Passwords, and other sensitive data such as password questions, should be stored using hashing and encryption. Crypto algorithms used must conform to <<Company Name>>'s most up to date encryption standard.

- If a password is compromised it should be reported immediately to the help desk and the password should be promptly changed.

3.7.3 TIME-BASED MANDATORY PASSWORD CHANGE

Users who authenticate directly against the <<Company Name>> network must change their password every 90 days—this requirement should be enforced via a GPO.

3.7.4 INITIATING A NEW PASSWORD OR PASSWORD RESET

When a new password or password reset is requested from a user via email or text the administrator who is performing the action should confirm the identity of the user prior to performing the task. This may require calling the user or sending a message via another channel of delivery prior to completing the request.

3.8 SERVICE ACCOUNT MANAGEMENT

Service accounts are accounts used by the system to perform tasks.

3.8.1 SERVICE ACCOUNTS CREATION / MODIFICATION

Service accounts are used to perform automated tasks and are used by programmatic processes to access assets to perform work. When service accounts are created they should only have one responsibility and their permissions should be highly circumscribed relative to their fundamental purpose to mitigate damage in the event a compromised password.
Any change to an existing service account requires the use of the change control process.

3.8.2 SERVICE ACCOUNTS ACCESS POLICY

Only employees with a 'need to know' should have access to service account information in adherence to maintain segregation of duties as a defense in-depth measure. As a guideline, when possible access to service account should be time-bound.

3.8.3 SERVICE ACCOUNT 'SINGLE RESPONSIBILITY PRINCIPLE'

Service accounts should only ever be assigned once to a single service. Accounts should never be reused in other contexts.

3.8.4 SERVICE ACCOUNTS REVIEW POLICY

Service accounts must adhere to the following:

- Service account passwords should be changed when employees with access to service account passwords have terminated employment. This must be included in the employee termination checklist as an action item.
- Service accounts should be included in at least monthly reviews of user access control by security staff designated by the CISO.
- Ensure that the 'Single Responsibility Principle' is being practiced.
- Ensure that attribute data is filled in and up to date: e.g. department owner, purpose, and review date.

3.8.5 USE OF SERVICE ACCOUNTS AND PRIVILEGED UTILITY PROGRAMS

The use of service accounts is restricted to Administrators and Authorized Users as a guideline to job automation where scale considerations come into play: e.g. when using a thread pool, etc. This applies equally to privileged utility programs.

3.9 ACCESS TO SOURCE CODE

3.9.1 EMPLOYEES OR CONTRACTORS

The ability to migrate changes into the production environment is restricted to authorized and appropriate personnel. Access to software source code, or administrative script, should be determined by job function. As a guideline access to source code should be limited based on the principle of least privilege.

3.9.2 SERVICE PROVIDERS

Source code is considered to be proprietary information. As a result, sharing source code with service providers is allowed as long as change control request is created and approved by the CTO.

3.10 REMOTE ACCESS

Due to the elevated risk, company policy dictates that when accessing the network or externally exposed applications remotely two-factor authentication (such as smart cards, tokens, or biometrics) must be used.

3.11 AUTOMATIC SESSION LOCKING ON ENTERPRISE ASSETS / SCREENSAVER PASSWORDS

Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle

computer. For this reason, screensaver passwords are required to be activated after 15 minutes of inactivity.

For mobile end-user devices, the period must not exceed 2 minutes. This requirement does not apply to BYOD devices.

3.12 ENCRYPTION

Industry best practices state that username and password combinations must never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to the company network or across a public network such as the Internet.

3.13 FAILED LOGON ATTEMPTS

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access an account. To guard against password-guessing and brute-force attempts, the company must incorporate lockout settings. This can be implemented as a time-based lockout or require a manual reset. In the event a manual reset is performed it should incorporate a second factor of authentication.

To protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

3.13.1 APPLICATION LOCKOUT

3.13.1.1 WEB-BASED APPLICATIONS

Web-based applications should incorporate two-factor authentication in conjunction with a lockout policy for defense-in-depth.

- The account lockout threshold should be 6 unsuccessful attempts.
- The account lockout duration should be 15 minutes.
- The account lockout counter reset should be 15 minutes, or after a successful login, whichever comes first.

3.13.1.2 SAAS AND PAAS APPLICATIONS

SaaS and PaaS applications used by the company should incorporate single-sign-on (SSO), see Network Account Lockout settings.

3.13.2 OPERATING SYSTEM LOCKOUT

Operating Systems must be joined to a domain, see Network Account Lockout settings.

3.13.3 NETWORK ACCOUNT LOCKOUT

- The account lockout threshold should be 6 unsuccessful attempts.
- The account lockout duration should be indefinite. A manual reset should be performed by operational personal. In the event a manual reset is performed it should incorporate a second factor of authentication.
- The account lockout counter reset should be 15 minutes, after a reset, or after a successful login.

3.13.4 DATABASE SYSTEM LOCKOUT

- The account lockout threshold should be 6 unsuccessful attempts.
- The account lockout duration should be indefinite. A manual reset should be performed by operational personal. In the event a manual reset is performed it should incorporate a second factor of authentication.
- The account lockout counter reset should be 15 minutes, after a reset, or after a successful login.

3.14 SECURITY INCIDENT EVENT MANAGEMENT (SIEM)

Network based events should be recorded and analyzed on a daily basis by the CISO and delegated security personnel. Namely:

- failed login attempts or account escalation;
- policy changes;
- system events;
- configuration changes, etc.

3.15 NETWORK ISOLATION

Network environments should be segregated when possible to ensure that damage from a breach is contained.

3.16 APPLICABILITY OF OTHER POLICIES

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

3.17 APPROPRIATE ACCESS GRANTING

Access is granted via change control request and review by the CISO or delegated personnel. The principle of least required permission is used to evaluate requests. Users should be initially granted the least amount of network access required to perform their respective job function. The principle of least required permission applies equally to physical access to facilities and protected information assets.

3.18 ACCOUNT REVIEW

Access will be reviewed on a quarterly basis by the CISO or delegated personnel. The following items should be reviewed and approved by the CISO or asset owners designated by the CISO:

- Firewall, WAF, and router rule sets.
- Domain Accounts & Security Groups
- Application required for operations

3.19 GPO REVIEW

GPOs should be reviewed on a quarterly basis.

4 SEGREGATION OF DUTIES

<<Company Name>> maintains a separation of duties to create a barrier between technical personnel who have access to modify application source code, and employees that can modify the production operational environment. <<Company Name>> upholds the segregation of duties by ensuring that all actions in the production environment are executed only by a limited set of personnel based on their roles. The determination of who works in source code and who doesn't is predicated on job description. As per <<Company Name>>'s Access Control Policy, roles and assignment of roles to personnel are reviewed and audited quarterly to verify appropriate systems access to staff. As a strict rule, only the following roles are granted access rights to Production on a permanent basis: Architects, DevSecOps and Network Engineers. All other roles do not have access and cannot make changes in Production unless explicitly granted temporary permission by the CTO or CISO.
User access reviews are completed by security personnel quarterly to ensure system access and access changes have been properly assigned and completed. By system design, system access changes are reviewed and confirmed by security personnel separate from the security personnel making the change; thus, safeguarding any one user from being able to make a change without review

5 ENFORCEMENT

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

7 DOCUMENT RACI

Responsible	Assigned to do the work	Security Program Manager
Accountable	Final decision, ultimately answerable	ISM Governance Committee
Consulted	Consulted BEFORE an action or decision is taken (proactive)	Executive Management
Informed	Informed AFTER a decision or action has been taken (reactive)	Named Participants in this document Other parties affected by the change

8 LICENSE INFORMATION

APPENDIX A: 'NEW ACCOUNT SUBMISSION' FORM

The new account form is submitted once an employee has processed the employees W-4. This form should be completed and attached to the account registration change control request.

SID		
Date of Hire (start date)		yyyy-mm-dd
Employee ID		
First Name		
Middle Name		
Last Name		
Job Title		
Manager		
Mobile Phone Number		
Email		
User has read the Acceptable Use Policy		YES | NO
Additional Group Membership(s)		
SaaS Applications		
HR Representative		
Submission Date		yyyy-mm-dd

APPENDIX B: 'ACCOUNT REMOVAL' FORM

This form should be completed and attached to the account de-registration change control request.

SID		
Date of Termination (end date)		yyyy-mm-dd
Employee ID		
First Name		
Middle Name		
Last Name		
HR Representative		
Submission Date		yyyy-mm-dd