Aberrant Open-ISM™

ACCEPTABLE USE 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 4
1.1 Scope of Policy 4
2 Policy 5
2.1 Acceptable Use 5
2.1.1 Explicit Management Approval to Use the Technologies 5
2.1.2 Use of All Technology Resources Must be Authenticated 13
2.1.3 Accessing via a User Account 13
2.1.4 Portable Device Labels 14
2.1.5 Bring Your Own Device (BYOD) 14
3 Terms of Acceptable Use 15
3.1 General Guidelines, Responsibilities and Acceptable Use for the Technology 15
3.2 Unacceptable Use and Behavior 15
3.3 Acceptable Network Locations for the Technology 16
3.4 Company-Approved Products 16
3.5 Additional Usage Policy Requirements 16
4 Recourse 17
5 Policy Acknowledge 17
6 Contact Information 18
7 Document RACI 18
8 License Information 19
Appendix A: Employee AUP Acknowledgment Form 20

1 OVERVIEW

This Acceptable Use Policy (otherwise referred to as the "Policy") of <<Company Name>>, Inc. ("the Company") establishes the acceptable use policies of <<Company Name>>'s resources. In accordance with regulations, the organization has established a Policy and supporting procedures regarding usage policies for critical employee facing technologies. This Policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding the organization's needs and goals. This Policy is to be implemented immediately and the provisions below set forth the framework for usage policies for critical employee facing technologies.

1.1 SCOPE OF POLICY

Usage policies and the supporting Acceptable Uses policies (commonly known as AUP or Acceptable Usage Policies) are known as the policies and supporting procedures that define proper use of critical employee facing technologies within an organization. These technologies generally consist of the following system components and additional Information Technology (IT) resources deemed critical by the organization:

- Network devices;
- Operating systems;
- Applications;
- Databases;
- Remote access technologies;
- Wireless technologies;
- Removable electronic media;
- Desktops;
- Laptops;
- Personal mobile devices;
- Internet use;
- E-mail use;
- Blogging;
- Social media forums.

This Policy applies to all users of resources owned or managed by <<Company Name>>. Individuals covered by the policy include, but are not limited to, <<Company Name>> employees, guests, contractors, and organizations accessing network services via the <<Company Name>> network.

2 POLICY

The organization will ensure that the usage policies for critical employee facing technologies will adhere to the following conditions for purposes of complying with regulations:

- Usage policies require explicit management approval to use the technologies;
- Usage policies require all technology use be authenticated with user ID and password or other authentication item (for example, token);
- Usage policies require a list of all devices and personnel authorized to use the devices;
- Usage policies require labeling of devices with owner, contact information and purpose;
- Usage policies require acceptable uses for the technology;
- Usage policies require acceptable network locations for the technology;
- Usage policies require a list of company-approved products;
- Usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity;
- Usage policies require activation of remote-access technologies used by vendors only when needed by vendors, with immediate deactivation after use;
- Usage policies prohibit copying, moving or storage of non-anonymized data onto local hard drives or removable electronic media when accessing such data via remote-access technologies.

2.1 ACCEPTABLE USE

The organization has developed and implemented comprehensive usage policies for critical employee facing technologies, which encompass the following categories and supporting activities. These policy directives and supporting procedures will be fully enforced by the organization for ensuring the usage policies for critical employee facing technologies are executed in a formal manner and on a consistent basis for all system components within the data environment and all other IT resources deemed critical by the organization.

2.1.1 EXPLICIT MANAGEMENT APPROVAL TO USE THE TECHNOLOGIES

Due to the abundance of technologies afforded by today's technology environment, the organization requires explicit management approval for the use of these technologies in conjunction with one's professional roles and responsibilities. The phrase, explicit management approval, consists of the following approval mechanisms and initiatives for the technologies listed below, along with an explicit Usage policy for each respective technology:

2.1.1.1 NETWORK DEVICES

All system administrative users of network devices (Firewalls, Routers, Switchgear, Load Balancers, Intrusion Detection Systems) and other related network devices must gain management approval via the following formalized and documented process:

1. All network devices are to be configured and used strictly for business operations.
2. All network devices are to be appropriately hardened and secured in accordance with industry standards and for applicable business requirements.
3. Network components may not be added, removed or modified unless explicit consent is given by appropriate personnel.
4. Any network devices obtained without proof of purchase and licensing rights will not be allowed onto the network.
5. All users (system administrative users) must be responsible for the proper use of these devices.
6. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these devices will not be tolerated.
7. All network system administrative rights and subsequent activities are subject to audit and review as needed.
8. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.2 OPERATING SYSTEMS

All system administrative users and end-users of operating systems (Windows, UNIX, Linux) and other related Operating Systems must gain management approval to use these systems devices via the following formalized and documented process:

1. All operating systems are to be configured and used strictly for business operations.
2. All operating systems are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed.
3. Operating systems may not be added, removed or modified unless explicit consent is given by appropriate personnel.
4. Any operating system obtained without proof of purchase and licensing rights will not be allowed onto the network.
5. All users (system administrative users) must be responsible for the proper use of these operating systems.
6. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these operating systems will not be tolerated.
7. All system administrative rights and subsequent activities are subject to audit and reviews as needed.
8. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.3 APPLICATIONS

All users of applications (coders/developers, end-users of applications, etc.) must gain management approval to use these applications via the following formalized and documented process:

1. All applications (internally developed and commercially purchased) are to be configured and used strictly for business operations.
2. All applications are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed.
3. Applications may not be added, removed or modified unless explicit consent is given by appropriate personnel.
4. Any application obtained without proof of purchase and licensing rights will not be allowed onto the network.
5. All users (coders/developers, end-users) must be responsible for the proper use of these applications.
6. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these applications will not be tolerated.
7. All users and their respective functions for any applications are subject to audit and reviews as needed.
8. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.4 DATABASES

All users of databases (database administrators, end-users of databases, etc.) must gain management approval to use these databases via the following formalized and documented process:

1. All databases are to be configured and used strictly for business operations.
2. All databases are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed.
3. Databases (and their representative elements, such as database files) may not be added, removed or modified unless explicit consent is given by appropriate personnel.
4. Any databases obtained without proof of purchase and licensing rights will not be allowed onto the network.
5. All users (database administrators, end-users of databases, etc.) must be responsible for the proper use of these technologies.
6. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these technologies will not be tolerated.

7. All database system administrative rights and subsequent activities are subject to audit and reviews as needed.
8. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.5 REMOTE ACCESS TECHNOLOGIES

All end users of remote access technologies (VPN, Remote Desktop Protocols, etc.) must gain access to use these remote access technologies via the following formalized and documented process:

1. All remote access technologies are to be configured and used strictly for business operations.
2. All remote access technologies are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed.
3. Remote access technologies may not be added, removed or modified unless explicit consent is given by appropriate personnel.
4. Any remote access technologies and their supporting protocols obtained without proof of purchase and licensing rights will not be allowed onto the network.
5. All end-users must be responsible for the proper use of these technologies.
6. Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity is required.
7. Activation of remote-access technologies used by vendors occurs only when needed by vendors and with immediate deactivation after use.
8. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these remote access technologies will not be tolerated.
9. All end users and subsequent activities are subject to audit and reviews as needed.
10. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.6 WIRELESS TECHNOLOGIES

All end users of wireless technologies (Wi-Fi/hotspots) must gain access to use these wireless technologies via the following formalized and documented process: wireless access is provided to laptop users after completion of the new user process and signing of the AUP.

1. All wireless technologies are to be configured and used strictly for business operations.
2. All wireless technologies are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed.
3. Wireless technologies may not be added, removed or modified unless explicit consent is given by appropriate personnel.

4. Any wireless technologies obtained without proof of purchase and licensing rights will not be allowed onto the network.
5. All end-users must be responsible for the proper use of these technologies.
6. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these wireless technologies will not be tolerated.
7. All end users and their subsequent activities are subject to audit and reviews as needed.
8. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.7 REMOVABLE ELECTRONIC MEDIA

All users of removable electronic media (external hard drives, USB drives, memory sticks, etc.) are prohibited unless explicitly authorized by the CISO.

1. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of removable electronic media devices will not be tolerated.
2. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.8 DESKTOPS

All users of desktops must gain access to use these computers via the following formalized and documented process: a desktop or laptop is provided to all employees after completion of the new user process and signing of the AUP.

1. All desktops are to be configured and used strictly for business operations.
2. All desktops are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed.
3. Desktops may not be added, removed or modified unless explicit consent is given by appropriate personnel.
4. Any desktop obtained without proof of purchase and licensing rights will not be allowed onto the network.
5. All end-users must be responsible for the proper use of these technologies.
6. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of desktops will not be tolerated.
7. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.9 LAPTOPS

All users of laptops must gain access to use these computers via the following formalized and documented process: a desktop or laptop is provided to all employees after completion of the new user process and signing of the AUP. Remote access is not automatically provided to laptop users, but must be authorized as a separate process.

1. All laptops are to be configured and used strictly for business operations.
2. All laptops are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed.
3. Any laptop obtained without proof of purchase and licensing rights will not be allowed onto the network.
4. All end-users must be responsible for the proper use of these technologies.
5. Users must protect their company-issued laptop from loss, theft and damage, and must also report loss or theft to designated personnel in a timely manner.
6. Users must protect from snooping or shoulder surfing when possible in public situations.
7. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of laptops will not be tolerated.
8. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.10 PERSONAL MOBILE DEVICES

All users of personal mobile devices must gain access to use these devices via the following formalized and documented process:

1. All personal mobile devices must be explicitly permissioned to access company resources and must be configured with software that allows them to be managed remotely—e.g. via <<Company Name>>'s MAM/MDM.
2. The passcode must be reconfigured to use at least six (6) digits.
3. Users must immediately report if their personal mobile device is lost or stolen so that the device can be remotely wiped via a mobile device manager.
4. Users must protect from snooping or shoulder surfing when possible in public situations.
5. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of personal mobile devices will not be tolerated.
6. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.11 INTERNET USE

All users of the internet must gain access to use this technology via the following formalized and documented process: The internet is provided to all employees after completion of the new user process and signing of the AUP.

1. All users are responsible for their internet activity and are always encouraged to use the internet in a judicious and ethical manner.
2. The internet is to be used for business purposes, but may be used for personal necessities from time to time.
3. Connections to the internet are to be conducted through company-approved technologies and resources only.
4. Users are not allowed to visit any pornographic sites or download any offensive material including, but not limited to pornography and other material deemed offensive in nature.
5. Users may not use the internet to facilitate personal financial gain while at work.
6. Users may not use the internet to incite violence or conduct any other activity deemed criminal or offensive in nature.
7. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of the internet will not be tolerated.
8. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.12 E-MAIL USE

All users of e-mail must gain access to use this technology via the following formalized and documented process: email is provided to all employees after completion of the new user process and signing of the AUP.

1. All users are responsible for their e-mail activity and are always encouraged to use e-mail in a judicious and ethical manner.
2. E-mail is to be used for business purposes, but may be used for personal necessities from time to time.
3. To access <<Company Name>> E-mail from a personal mobile device users must agree to install <<Company Name>>'s MAM/MDM so that emails can be wiped remotely in the event of the loss of the device or termination of employment.
4. Users are not allowed to send or receive offensive material via e-mail including, but not limited to pornography and other material deemed offensive in nature.
5. Users may not use e-mail to facilitate personal financial gain (i.e. operate a personal business) while at work.
6. Users sending confidential information via email must send data using encryption.
7. Users may not use e-mail to incite violence or conduct any other activity deemed criminal or offensive in nature.

8. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of email will not be tolerated.
9. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.13 INSTANT MESSAGING (IM)

All user who use IM must gain access via the following formalized and documented process:

1. All users are responsible for their IM activity and are always encouraged to use IM in a judicious and ethical manner.
2. IM is to be used for business purposes, but may be used for personal necessities from time to time.
3. Users are not allowed to send or receive offensive material including, but not limited to pornography and other material deemed offensive in nature.
4. Users may not use IM to facilitate personal financial gain while at work.
5. Users may not use IM to incite violence or conduct any other activity deemed criminal or offensive in nature.
6. Users must not send confidential information via IM but must send data through alternate encrypted technologies.
7. Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of IM will not be tolerated.
8. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.1.14 SOCIAL MEDIA FORUMS AND BLOGGING

All users who interact and participate on social media forums or blogs must gain access to these forums via the following formalized and documented process:

1. Only individuals who are approved by the <<Company Name>> marketing team may utilize <<Company Name>>-sponsored social media sites or engage in blogging activity in the name of or on behalf of <<Company Name>>. Those approved individuals may only use <<Company Name>>-sponsored social media or blogs for business purposes.
2. Individuals who wish to engage in social media use or to blog outside of <<Company Name>>-sponsored social media sites or blogs and outside their capacity as <<Company Name>> employees must comply with the following guidelines:

- Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or

business threat to the organization because of misuse of social media will not be tolerated.

- Employees should be judicious about the time and resources they use for personal social media activities while working at <<Company Name>>.
- Employees must not conduct <<Company Name>> business or otherwise purport to represent or speak on behalf of <<Company Name>> without approval of <<Company Name>>'s CMO.
- An employee may include in their public profiles that he or she is an employee of <<Company Name>> and the capacity in which they are employed, so long as he or she keeps the employment status updated and factually accurate. If an employee identifies him or herself as a <<Company Name>> employee, each employee must make clear that he or she is writing for him/herself on his/her own behalf and not on behalf of <<Company Name>>.
- Employees are personally responsible for their own use of social media or blog content and are expected to adhere to all applicable laws, rules, guidelines and policies, including without limitation, those rules, guidelines and policies of <<Company Name>> and any applicable social media providers, with a particular emphasis on: respecting co-workers' privacy; respecting client privacy; protecting confidentiality and security; and safeguarding <<Company Name>>'s information and assets.
- Employees must avoid being obscene, inflammatory, confrontational, slanderous, defamatory, harassing, threatening, offensive or disparaging in any comments or actions on social media sites or blogs.

1. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

2.1.2 USE OF ALL TECHNOLOGY RESOURCES MUST BE AUTHENTICATED

Accessing system components and any other IT resources deemed critical by the organization requires the use of a user ID and a password.

2.1.3 ACCESSING VIA A USER ACCOUNT

The following guidelines are in place for proper account and credential usage:

- User accounts must adhere to the conventions that align with account management policy.
- User 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 for the employee to perform that 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.

- Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the IT Manager or executive team, or as required by applicable regulations, or third-party agreements.

2.1.4 PORTABLE DEVICE LABELS

Portable devices such as laptops should be labeled and recorded in the asset inventory prior to assignment to an employee.

2.1.5 BRING YOUR OWN DEVICE (BYOD)

In some cases the <<Company Name>> may employ a BYOD policy—such as with mobile devices. Employees that use their own devices must adhere to the Acceptable Use Policy prior to using their device for work.

3 TERMS OF ACCEPTABLE USE

The organization‘s technology resources provide users the ability to communicate for personal and professional reasons. These resources and the ability to use them are considered a privilege and, as such, users are always expected to act responsibly and professionally. Users utilizing the organization’s technology resources must respect the rights of other users, the integrity of the systems and related physical resources, and they must obey all applicable laws and regulations (local, state and federal). Technology resources have vast capabilities of sending, receiving and storing electronic data; therefore, users must be particularly careful to protect these technology resources and the associated data, and they must strictly adhere to software licensing agreements and copyright laws.

3.1 GENERAL GUIDELINES, RESPONSIBILITIES AND ACCEPTABLE USE FOR THE TECHNOLOGY

- The primary purpose and use of technology resources is for the organization’s business activities only.
- Users do not own any accounts; rather they are granted access commensurate with their roles and responsibilities within the organization.
- Users are to never share their accounts with others and must keep all password information confidential.
- It is the responsibility of any user given access rights to the account to protect its access.
- Users must strictly adhere to licensing agreements and copyright laws that govern all material accessed or stored using the organization‘s technology resources.
- Users are not permitted to develop or use programs that may cause harm to the organization’s computer systems.
- Users are not permitted to use any type of services that result in restricting network access from other users.
- Users are not permitted to use any type of services that significantly impair access to other networks connected to the organization.
- Users remotely accessing the organization‘s systems are responsible for using protocols for remote access approved by the organization.
- Users shall not intentionally seek information on, or represent themselves as, another user unless permitted to do so by that user or by authorized personnel.
- Users are not permitted to obtain information belonging to other users. This includes, but is not limited to the following: passwords, data files and other sensitive and confidential information.

3.2 UNACCEPTABLE USE AND BEHAVIOR

- Using or attempting to use another user’s account to access resources.

- Using or attempting to use the organization‘s technology resources to gain unauthorized access to company-wide systems.
- Using or attempting to use the organization‘s technology resources for the purpose of sexual harassment, threats against the organization or any other type of civil or criminal misconduct.
- Violating any copyright laws by obtaining any form of media or resources using the organization‘s technology resources.
- Spamming or mass solicitation of company material to known or unknown third parties.
- Releasing prohibited and classified company information to the public through the use of the organization‘s technology resources.
- Intentionally installing any unapproved equipment to the organization’s infrastructure.

3.3 ACCEPTABLE NETWORK LOCATIONS FOR THE TECHNOLOGY

All the organization‘s technology resources are to be appropriately configured, hardened and physically and logically placed within the network so as not to create any inherent security weaknesses for the respective system or any other supporting systems.

3.4 COMPANY-APPROVED PRODUCTS

The organization is the legal owner of all technology resources purchased or leased with company funds. The overall responsibility for administering and overseeing these technology resources rests with the highest-ranking role on the Information Security team i.e. Chief Technology Officer, VP of Information Security, etc. The highest-ranking Information Security team member is also responsible for providing documented approvals, be it through email or ticketing system, for any additional software installations for employees to complete their job duties and responsibilities.

3.5 ADDITIONAL USAGE POLICY REQUIREMENTS

- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity;
- Activation of remote-access technologies used by vendors only when needed by vendors, with immediate deactivation after use;
- The prohibition of copying, moving or storing data that has not been anonymized onto local hard drives or removable electronic media when accessing such data via remote-access technologies.

4 RECOURSE

Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of social media will not be tolerated. Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

All employees, contractors or third parties granted custody of <<Company Name>> or any other company-owned information assets shall return such assets, intact and in their entirety, at the termination of their relationship with the company.

5 POLICY ACKNOWLEDGE

As part of the onboarding procedure employees, contractors, and third parties must acknowledge that they've read and understand the AUP.

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: EMPLOYEE AUP ACKNOWLEDGMENT FORM

The following form is required to be completed prior to an employee be onboarded by HR.

Name of Employee / Contractor / Third Party	
Date of Hire	
Hiring Manager	

I acknowledge that I have read the Acceptable Use Policy and understand <<Company Name>>'s policies as it relates to acceptable use. I also understand that violation of the Acceptable Use Policy may result in disciplinary action in the form of a reprimand, suspension, or termination.

Signature	
Date	