Aberrant Open-ISM™

COMMUNICATION 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 PURPOSE

This policy aims to establish ground rules for communication within the company, customers, and external entities.

2 SCOPE

This policy applies to all <<Company Name>> employees and contractors.

3 POLICY

3.1 INTERNAL COMMUNICATION

In a modern work environment, there are numerous channels for transmitting and receiving information. As a result, it's essential to maintain a methodology for how and when to communicate over different communications media. Ultimately, the internal communication policy aims to ensure that internally communicated information is prioritized correctly and acted on in a timely manner.

3.1.1 GUIDELINES FOR PRIORITIZATION AND TIME SENSITIVITY

In an effort to minimize the amount of information so that employees don't confuse the priority of communication or miss important communication, it's important to select the appropriate medium for communicating with co-workers. Using the right channel depends on the prioritization and time-sensitivity of the message.

	High Priority	Low Priority
High Time Sensitivity	SMS, Phone call, In-person	Email, Instant Messaging (IM)
Low Time Sensitivity	Email, with importance set at 'high.'	Instant Messaging (IM), Email

3.1.2 INQUIRIES

As a guideline, you shouldn't have to ask the same question more than once. If you do ask a question, ask yourself if others might have the same question in the future. If the answer is a resounding yes, then take the time to create or update the documentation in the learning management system.

It's always okay to ask questions, but inquiries regarding operational tasks between employees should be kept to a minimum. Prior to initiating a communication employees should research the company's knowledge management system and review relevant documentation. If the employee is unable to resolve their questions, it's permissible to ask for help; however, the

employee should then document, or update, the answer to their question in the company's learning management system.

3.1.3 ESCALATION

It's the employee's discretion as to whether or not to escalate the number of recipients on a message. As a guideline, escalation should be avoided if possible unless absolutely necessary.

3.1.4 BROADCAST MESSAGES

As a guideline, employees should get management approval prior to transmitting or broadcasting an email to the company. Employees should also refrain from replying to broadcast emails unless their contribution adds value to the communication.

3.1.5 MEMORIALIZING COMMUNICATION

As per the Record Retention Policy, different communication mediums have different retention requirements—email is the most stringent. As a result, if you need to memorialize information for posterity email is the best communication medium.

As a guideline, it's often helpful to recap meetings or phone conversations in an email that summarizes decisions or action items. When providing a summary be sure to include product owners and delivery dates, also ensure that you send the email all of the meeting participants. Documenting meetings can be forensically useful when trying to reconstruct events or decisions.

3.1.6 ALERTING

Communication of system alerts should use Instant Messaging when possible. As a strong guideline, email should be used as the medium of last resort for automated alerts.

3.1.7 MANAGEMENT COMMUNICATION WITH REPORTS

This policy isn't prescriptive about how managers communicate with reports; however, in-person communication is best when possible.

3.2 EXTERNAL COMMUNICATION

3.2.1 AUDIENCE

3.2.1.1 COMMUNICATION WITH VENDORS

Communication with vendors is the purview of management. Discussions involving the transfer of detailed information require a signed NDA with the vendor before proceeding with a more detailed discussion. Even if an NDA is in place, employees that need to interact with a vendor should get permission from management before initiating a substantive conversation or negotiation.

3.2.1.2 OUTBOUND CUSTOMER OR INVENTOR COMMUNICATION

Outbound communication with customers is the responsibility of executive management and marketing.

3.2.2 MEDIUM OF COMMUNICATION

3.2.2.1 PHONE/TEXTS

Never discuss confidential information unless you can verify the caller's identity on the other end of the phone. Consider using Instant Messaging or Email as a second factor if you need to verify the speaker's identity.

Take notes during the call and follow up with a summation of the discussion via email. In some cases, it may be beneficial to update the CRM.

3.2.2.2 VIDEO CONFERENCING

Ensure that an NDA is in place if you share proprietary or confidential information. If video is turned on, ensure that sensitive information isn't displayed in your background. Take notes during the call and follow up with a summation of the discussion via email. In some cases it may be beneficial to update the CRM.

3.2.2.3 INSTANCE MESSAGING

Avoid discussions that include confidential information with outside parties via Instant Messaging applications. Email is a better medium for secure communications.

3.2.2.4 EMAILS

Confidential emails must be sent via secure email. The following disclaimer must be included on all outbound email communications:

> **CONFIDENTIALITY NOTICE: The contents of this email message and any attachments are intended solely for the addressee(s) and may contain confidential and/or privileged information and/or may be subject to copyright or other intellectual property protection and be legally protected from disclosure. If you are not the intended recipient of this message or their agent, or if this message has been addressed to you in error, please immediately alert the sender by reply email and then delete this message and any attachments. If you are not the intended recipient, you are hereby notified that any use, dissemination, copying, or storage of this message or its attachments is strictly prohibited.**
>
> **Confidentiality of email cannot be guaranteed since the message traverses public networks unless the message has explicitly used secure email. Please DO NOT reply to this message with any sensitive or personal information if not using the secure email portal. If this type of information needs to be shared, please let us know so that we can arrange a more secure transmission method with you.**

4 RECOURSE

All employees and contractors must adhere to this policy. Violation is grounds for being reprimanded, suspended or terminated.

5 POLICY ACKNOWLEDGE

As part of the onboarding procedure employees and contractors must acknowledge that they've read and understand the Communication Policy.

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