Aberrant Open-ISM™

# DATA CLASSIFICATION 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 SCOPE

The <<Company Name>> information security program has as its primary goal the "protection of the confidentiality, integrity and availability of information in all forms". This standard supports that goal by providing specific instructions on the classification and handling of information across its lifecycle. As such, the primary objective of this document is to educate and inform the reader about information classification, how that classification determines the requisite protections (including guidelines for how long certain records should be kept and how they should be destroyed), and how to avoid unauthorized disclosure of the information either generated by, or entrusted to, the care of the organization.

# 2 PURPOSE

The purpose of this data classification policy is to provide a system for protecting information that is critical to the organization. All workers who may come into contact with confidential information are expected to familiarize themselves with this data classification policy and to consistently use it.

# 3 POLICY

The organization's data classification system has been designed to support the 'need to know' so that information will be protected from unauthorized disclosure, use, and modification. Consistent use of this data classification system will facilitate business activities and help keep the costs for information security to a minimum. Without the consistent use of this data classification system, <<Company Name>> unduly risks loss of customer relationships, loss of public confidence, internal operational disruption, excessive costs, and competitive disadvantage.

## 3.1 APPLICABLE INFORMATION

This data classification policy is applicable to all information in the <<Company Name>>'s possession. For example, confidential information from suppliers, business partners and others must be protected with this data classification policy. No distinctions between the words data, information, knowledge, and wisdom are made for purposes of this policy.

## 3.2 CLEAR LABELING

When possible information assets should be labeled with their data classification type clearly visible.

#### 3.2.1 DOCUMENT LABELING

The classification type should be included in bold in the footer—preferably in a noticeable color. Documents marked as 'Confidential' should only ever be sent via secure mail.

#### 3.2.2 EMAIL LABELING

Emails should be clearly labeled with their data classification level. Confidential emails should only ever be sent via secure mail.

### 3.3 DATA INVENTORY

The organization will create an maintain a data inventory, based on the enterprise's data management process. Review and update inventory annually, at a minimum, with a priority on sensitive data.

### 3.4 CONSISTENT PROTECTION

Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology was used to handle it, or what purpose(s) it serves. Although this policy provides overall guidance, to achieve consistent information protection, workers will be expected to apply and extend these concepts to fit the needs of day-to-day operations.

### 3.5 INTERNAL ACCESS TO DATA

Access to data should be based on a 'need to know' basis only—employees that have access to confidential information should only ever have access to the information that they need to perform their job functions. The principle of 'least privilege' is predicated on job function, however, there are instances where an employee need elevated temporary elevated permissions to perform his / her job function. In such case, the employee she be granted access to information on a time bound basis. Elevated permissions should be scavenged after the expiration of the time period. Data access is applied to local and remote file systems, databases and applications. Changes to employee permissions must adhere to the company's Access Control Policy and Change Control Policies.

### 3.6 DATA SHARING WITH EXTERNAL ENTITIES

In the course of doing business it is often necessary to share information with other customers or vendor organizations. Prior to sharing information that is proprietary or confidential to <<Company Name>> an NDA must be signed and counter-signed by an authorized signatory.

The NDA in this case functions as a security control. The NDA should be considered to be an information asset and adhere to the company's data retention requirements.
When sharing data with an external entity the following guidelines should be adhered to:

- Access to information should be shared digitally via a URL, not sent as a PDF.
- Access to information should be timebound.
- Access should be granted to individuals who are represented in our system as 'guest' users—adding users should be done in accordance with the company's Access Control Policy and Change Control Policies.
- Information should be versioned.
- Information should only ever be transmitted in an encrypted form that aligns with the company's Encryption Policy.

Sending information in files such as a PDF files should be done as a last resort—it is recognized that in some cases sending files is unavoidable. The following guidelines apply when sending digital files to an external entity:

- Confidential information should be sent only through an encrypted medium: e.g. encrypted email, etc.
- Confidential files must incorporate a password. The password should communicated to the client via a secondary medium, such as SMS or over the phone.

## 4 DATA CLASSIFICATION

The following data classification apply to all company data.

| **Category** | **PUBLIC** | **PROPRIETARY** | **CONFIDENTIAL** |
|---|---|---|---|
| **Risk Sensitivity & Control Level** | **No Risk**<br>**No Controls** | **Low Risk**<br>**Moderate Controls** | **High Risk**<br>**Extensive Controls** |
| **DEFINITION** | Information that is freely available outside of <<Company Name>> and would cause no harm to the Company or its customers if disclosed. | Information that is freely and commonly shared within <<Company Name>>, is not intended for public use and would cause minimal loss to <<Company Name>> or its customers if lost, stolen or breached. An NDA should be in place prior to disclosure of proprietary information— | Information that could cause material harm to <<Company Name>> or its customers if lost, stolen or breached. Such harm includes financial loss, damage to the Company's reputation, loss of business, contractual liability and potential legal and regulatory sanctions, |

| | | | |
|---|---|---|---|
| | | this requirement is discretionary. | penalties or fines. An NDA must be in place prior to disclosure of confidential information—this requirement is mandatory. |
| **EXAMPLES** | Company data, such as:<br>- sales demos,<br>- marketing brochures,<br>- marketing data based on aggregated customer or vendor data.<br>- "Code of Conduct Policy,"<br>- "Code of Ethics Policy,"<br>- white papers,<br>- press & news releases,<br>- "Acceptable Use Policy,"<br>- "Terms of Use,"<br>- "Non-Disclosure Agreement." | Customer or vendor data, such as:<br>- Aggregated data that cannot be reversed engineered.<br>Company data, such as:<br>- organization charts that have sensitive information elided,<br>- the employee handbook,<br>- policies that are categorized as proprietary and have sensitive information elided—e.g. IP addresses, etc.,<br>- administrative office documents<br>- routine internal correspondence and announcements (unless designated as Confidential) internal phone directories<br>Adherence to the SDLC mandates a separation of concerns between source code and configuration. As a result it's permissible to share technical information subject to restrictions under | Personally identifiable information (PII) of customers or vendors such as:<br>- name,<br>- maiden name,<br>- mother's maiden name,<br>- address,<br>- phone number,<br>- e-mail address,<br>- user name.<br>Customer, employee, contractor, or vendor identification numbers, such as:<br>- SSN,<br>- passport,<br>- driver's license number,<br>- taxpayer identification,<br>- account numbers.<br>Personal characteristics or biometric information including:<br>- photographic image (especially of face or other identifying characteristic),<br>- fingerprints,<br>- handwriting, |

| | | | |
|---|---|---|---|
| | | a nondisclosure agreement, such as:<br>• source code,<br>• code repositories,<br>• artifacts,<br>• architectural diagrams,<br>• network topology,<br>• deployment diagrams,<br>• scripts,<br>• end points,<br>• API documentation,<br>• SDK documentation,<br>• user documentation | • other biometric data.<br>Information about an individual that is linked or linkable to one the data types above (e.g., date or place of birth, race, religion, weight, activities, geographical indicators, or employment, medical information or education information).<br>Financial information such as:<br>• account activity,<br>• balances, transactions,<br>• credit rating, etc.<br>Corporate, partnership, or governmental Customer data, such as:<br>• Financial account numbers, account activity,<br>• balances and transactions,<br>• Marketing, trading,<br>• investment and business strategies; and<br>Employee or contractor information, such as:<br>• Date of birth,<br>• home address,<br>• SSN,<br>• gender, |

| | | | |
|---|---|---|---|
| | | | • ethnicity,<br>• marital status,<br>• health and medical information,<br>• drug screening,<br>• background and credit checks,<br>• compensation information,<br>• performance evaluations.<br>Company data, such as:<br>• organization charts,<br>• source code that contains hard-coded configuration data.<br>• configuration data<br>• financial records,<br>• trade secrets,<br>• marketing,<br>• trading,<br>• investment and business strategies,<br>• merger,<br>• acquisition and securities offering information,<br>• earnings estimates,<br>• research or other sensitive company information prior to release to the public.<br>• system and network diagrams that incorporates sensitive information, |

| | | | |
|---|---|---|---|
| | | | • risk and vulnerability assessments,<br>• audit and regulatory reports,<br>• security incident investigations, etc. |

## 5 HANDLING PROCEDURE

The following table provides guidance on sending classified data over different mediums of information exchange.

| CATEGORY | PUBLIC | PROPRIETARY | CONFIDENTIAL |
|---|---|---|---|
| **FAX** | No restrictions | Recipient should be asked to confirm receipt of the fax. | Recipient should stand by the fax machine during transmission and confirm receipt. |
| **COPIERS & PRINTERS** | No restrictions | Remove as soon as practicable from copiers, printers and fax machines. | Directly monitor the printing, faxing or copying of Confidential documents and immediately move the documents to a secure, controlled environment upon completion. |
| **MAIL** | No restrictions | May be sent through interoffice or external mail with no special handling. | Must be hand carried by company personnel, sent through interoffice mail or sent by an overnight courier approved by <<Company Name>>. When sent by overnight courier, the package must be securely packaged and traced with a record of receipt. Recommendation: Mark and seal any envelopes containing Confidential Information that are sent outside the office. |
| **PRINTED DOCUMENTS** | No restrictions | **In the Office** – Should not be left in open or public areas. Documents should be placed in locked cabinets, drawers, or offices at the end of work day.<br>**Outside the Office** – May be removed only with supervisor's approval. You must maintain reasonable | **In the Office** – Should not be left unattended in open or public areas, copy rooms, printers, fax machines, etc. Should be locked in cabinets, drawers or offices when not in your direct control.<br>**Outside the Office** – May be removed from office only with your Department Head approval. The document must be continually controlled while |

| | | | |
|---|---|---|---|
| | | control over the documents, including storing in a locked environment when unattended. | outside of the office (either in your direct physical control or locked in a secure area). |
| **DISPOSAL** | Normal waste disposal | Hard-copy documents should be placed in a secure disposal container or cross-cut shredder. Electronic media must be irretrievably erased as per the company's destruction policy.<br>Contact Tech Support for assistance if you need assistance. | Hard-copy documents should be placed in a secure disposal container or cross-cut shredder. Electronic media must be irretrievably erased as per the company's destruction policy.<br>Contact Tech Support for assistance if you need assistance. |
| **EMAIL** | No restrictions | May be sent internally or externally without encryption, but must be transmitted using in accordance with the company's Encryption Policy. | **In the Office** – Confidential email may be sent unencrypted, but only to individuals with clear authorization to see the information.<br>**Outside the Office** – Confidential email must be encrypted and transmitted using a secure mail. |
| **WIRELESS & INTERNET** | No restrictions | Proprietary information must be encrypted when sent over the internet or wireless networks in accordance with the company's Encryption Policy. | Confidential information must be encrypted when sent over the Internet or wireless networks in accordance with the company's Encryption Policy. |
| **VOICEMAIL & TELEPHONES** | No restrictions | Make sure the person you are calling is authorized to hear Proprietary information. | Make sure the person you are calling is authorized to hear confidential information. Do not leave Confidential information on external voicemail systems. |

| | | | |
|---|---|---|---|
| **ELECTRONIC DATA STORAGE** | No restrictions | Proprietary electronic records must be encrypted at rest in accordance with the company's Encryption Policy. | Confidential electronic records must be encrypted at rest in accordance with the company's Encryption Policy. |
| **SMART PHONES, & TABLET COMPUTERS** | No restrictions | Proprietary information must be encrypted when stored on a smart phone, tablet computer or other mobile device. No proprietary information may be stored on a personal mobile device, unless the device is approved, configured and managed by <<Company Name>>. | Confidential information must be encrypted when stored on a smart phone, tablet computer or other mobile device. No confidential information may be stored on a personal mobile device, unless the device is approved, configured and managed by <<Company Name>>. |
| **Laptops** | No restrictions | Proprietary information must be encrypted when stored on a company provided laptop. Personal computers are not authorized to store proprietary information. | Confidential information must be encrypted when stored on a company provided laptop. Personal computers are not authorized to store confidential information. |
| **PORTABLE ELECTRONIC STORAGE MEDIA** | Information of any sort should not be stored on Portable Electronic Storage Media without the express approval of Information Technology and written approval from designated executive level officer.<br>This restriction applies regardless of whether the | Proprietary information should not be stored on portable electronic media. | Confidential Information must not be stored on Portable Electronic Storage Media. |

| | | | |
|---|---|---|---|
| | media is used within Company premises or not. | | |

## 6 COMPLIANCE

Failure on the part of employees to follow this policy can result in possible civil and criminal sanctions against <<Company Name>> and its employees and possible disciplinary action against responsible individuals. <<Company Name>> will annually review these procedures with to ensure that they are in compliance with new or revised regulations.

## 7 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

## 8 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<br>Other parties affected by the change |

# 9 LICENSE INFORMATION