Data Classification Policy

distriBind

Data Classification Policy for distriBind

1. Purpose

The purpose of this Data Classification Policy is to ensure that all data within distriBind is appropriately classified and protected based on its sensitivity, value, and criticality. This policy establishes a framework for classifying, handling, and securing data to prevent unauthorized access, disclosure, alteration, and destruction.

2. Scope

This policy applies to all employees, contractors, and third-party vendors of distriBind who handle company data, regardless of the format or medium in which the data is held.

3. Policy Details

3.1 Paperless standards

distriBind operates a paperless environment and no data of any type should be printed with the sole exception of contracts for wet signature and only then if the other contracting party cannot provide documents for digital signature.

3.2 Assumption of confidentiality

All distriBind staff are required to sign and NDA. The assumption of confidentiality is held against all data, that it must not be disclosed unless specifically authorised.

3.3 Data Classification Standards

Data within distriBind must be classified into one of the following categories based on its sensitivity and the impact to distriBind should that data be disclosed, altered, or destroyed:

- **Public**: Data not sensitive in nature and intended for public access.

- **Internal**: Data intended for internal use but not expected to cause harm if disclosed. All distriBind client data except for bordereaux (or equivalent) are considered internal.

- **Confidential**: Sensitive data that could cause harm to distriBind or its clients if disclosed. Client data such as bordereaux (or equivalent) is considered confidential.

- **Highly Confidential**: Data of the most sensitive nature, including trade secrets, regulated personal information, and data that could cause significant harm if disclosed or altered.

3.4 Data Handling and Protection

Each classification level has associated handling and protection guidelines to ensure that data is adequately protected:

- **Public**: Can be disclosed without authorization. No special handling required.

- **Internal**: Should not be disclosed outside of distriBind without authorization. Basic access controls apply.

- **Confidential**: Must be strictly controlled and disclosed only on a need-to-know basis. Requires encryption in transit and at rest.

- **Highly Confidential**: Requires the highest level of security controls, including encryption, access control, and physical security measures.

3.5 Roles and Responsibilities

The Executive Management Team is responsible for overseeing the implementation of this policy and ensuring compliance. All employees, contractors, and third-party vendors are responsible for classifying, handling, and securing data in accordance with this policy.

4. Compliance and Enforcement

Violations of this policy may result in disciplinary action, including termination of employment or contracts. Compliance with this policy is mandatory for all employees, contractors, and third-party vendors.

5. Policy Review and Modification

This policy will be reviewed annually or as necessary to reflect changes in legal, regulatory, or business requirements. Modifications will be communicated to all affected parties.

Last Review Date: 11 March 2024

Next Review Date: 11 March 2025

Reviewer: Dave Connors