distriBind

Access Control Policy

distriBind

Access Control Policy for distriBind

1. Purpose

The purpose of this Access Control Policy (ACP) is to ensure that access to all electronic and physical data within distriBind is controlled and limited to authorized personnel only. This policy aims to protect the confidentiality, integrity, and availability of our data and information systems.

2. Scope

This policy applies to all employees, contractors, and third-party vendors of distriBind who have access to our data and information systems, regardless of their location.

3. Policy Details

3.1 User Access Management

Authorization: Access to information systems is granted based on job roles and responsibilities. The Executive Management Team is responsible for granting, altering, and revoking access rights.
Minimum Necessary Access: Users are given the least amount of access necessary to perform their duties.
Review of Access Rights: User access rights are reviewed at least quarterly to ensure they are still appropriate.

3.2 User Responsibility

Secure Authentication: Users must secure their credentials. Passwords must be strong and changed regularly. Multi-factor authentication (MFA) is required where feasible.
Unauthorized Access: Users must not attempt to gain unauthorized access to information systems or data.

3.3 Information Classification and Handling

Data Classification: Data is classified into categories such as Public, Internal, Confidential, and Highly Confidential. Access controls are based on these classifications.
Data Handling and Storage: Data must be handled and stored according to its classification level. Sensitive data, especially pertaining to insurance information, should be encrypted in transit and at rest.

3.4 Access Control Measures

Physical Access Control: Physical access to facilities housing critical information systems is restricted to authorized personnel.
Remote Access: Secure VPN access is required for remote access to the company network. Endpoint security measures must be in place.
Application Access Control: Applications, especially those handling insurance data, must implement role-based access control (RBAC) to ensure users can only access data and functionalities necessary for their job roles.

3.5 Monitoring and Review

Audit Logs: Access to sensitive systems and data must be logged. Audit logs are reviewed regularly for unauthorized or suspicious activity.

Incident Response: Any instances of unauthorized access or breaches must be reported immediately to the Executive Management Team for investigation.

4. Policy Enforcement

Violation of this Access Control Policy may result in disciplinary action, up to and including termination of employment or contracts. It is the responsibility of all employees, contractors, and third-party vendors to comply with this policy.

5. Policy Review and Modification

This policy will be reviewed annually or as needed to respond to changes in regulations, threats, or business processes. Any modifications will be communicated to all affected parties.

Last Reviewed: 11 March 2024

Next Review Date 11 March 2025

Reviewer: Dave Connors