

CORPORATE DATA PROTECTION POLICY

Policy Number: POL-2025-DATA-01

Effective Date: January 1, 2025

1. INTRODUCTION

This policy outlines the requirements for protecting personally identifiable information (PII) and ensures compliance with applicable data protection regulations including GDPR, CCPA, and HIPAA where relevant.

2. SCOPE

This policy applies to all employees, contractors, and third-party vendors who have access to corporate data systems and information.

3. DATA CLASSIFICATION

3.1 Confidential Data

Information that requires the highest level of protection, including:

- Personal health information covered by HIPAA
- Financial account information
- Authentication credentials
- Proprietary business information

3.2 Internal Data

Information that should be protected from external access but is generally available to authorized employees.

3.3 Public Data

Information that may be freely disclosed to the public.

4. COMPLIANCE REQUIREMENTS

All data handling procedures must comply with:

- GDPR requirements for EU personal data
- CCPA requirements for California residents' personal information
- SOX requirements for financial reporting data
- PCI DSS for payment card information

5. ENFORCEMENT

Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.

Document Owner: Information Security Department

Review Cycle: Annual

Last Review: December 15, 2024