INFORMATION SECURITY POLICY

Effective 11.25.25; Updated 2.14.26

1. Purpose

This Information Security Policy establishes the organization's commitment to protecting the confidentiality, integrity, and availability of information processed, stored, or transmitted through its systems and services.

2. Scope

This policy applies to all company systems, applications, and cloud infrastructure, as well as access by employees, contractors, and administrators. It covers institutional, customer, reporter, and personal data, and extends to remote work environments and company-managed systems.

3. Governance and Oversight

Information security is overseen by the Director of IT, with support from the General Counsel and external advisors as needed. Security responsibilities are assigned based on defined roles and least-privilege access principles. Policies and associated controls are reviewed periodically and updated as required to reflect evolving risks and operational needs.

4. Risk Management

Information security risks are identified, assessed, and managed on an ongoing basis. Risk considerations are incorporated into system design, configuration changes, and operational decisions. Security assessments and reviews are conducted annually and upon material changes to systems or infrastructure.

5. Access Control

Access to systems and data is restricted to authorized users based on job responsibilities. Privileged access is limited, reviewed periodically, and approved by the Director of IT. Authentication controls include strong password requirements and role-based access controls.

6. Asset and Data Protection

Data is protected through administrative, technical, and physical safeguards appropriate to its sensitivity and classification. Encryption and secure configuration practices are applied where applicable. Data retention and deletion practices are aligned with contractual obligations and regulatory requirements.

7. Secure Configuration and Change Management

Systems are configured using secure baseline settings. Changes to production systems are reviewed, tested, and approved prior to deployment. Emergency changes are documented and subject to post-implementation review.

8. Monitoring and Logging

Security-relevant system and user activities are logged and monitored to support incident detection, investigation, and response. Logs are protected from unauthorized access and retained in accordance with established data retention policies.

9. Incident Response

The organization maintains procedures for identifying, responding to, and resolving security incidents. Incidents are escalated to appropriate personnel and addressed promptly. Breach notification obligations are met in accordance with applicable legal and contractual requirements.

10. Security Awareness

Security awareness training is mandatory for all employees and covers data protection, secure system use, and incident reporting responsibilities. Training is provided upon onboarding and refreshed periodically thereafter.

11. Third-Party and Cloud Security

Cloud infrastructure is hosted on AWS and leverages AWS security controls in accordance with shared responsibility practices. Third-party services are reviewed for security and compliance impact prior to use and throughout the vendor relationship as appropriate.

12. Policy Review

This policy is reviewed at least annually and updated as necessary to reflect changes in business operations, technology, or regulatory requirements.