Policy Name	Information Security Policy
Responsible Party	David Trost
Contact	security@compto.com
Status	Under Review
Effective Date	
Revision Date	February 2025

Compto Public Benefit Corporation Information Security Policy: Compliance and Supervisory Procedures

1. Purpose and Scope

This policy establishes the organization's commitment to safeguarding its information assets against unauthorized access, loss, or compromise. It encompasses:

1. The processes for identifying and mitigating information security risks.
2. Standards for handling and protecting sensitive data.
3. Procedures for monitoring systems and responding to incidents.
4. Physical and logical security measures to ensure continuous protection of business operations.

Scope:

- All information systems, networks, and devices used for business purposes (including cloud infrastructures, on-premises resources, and endpoints protected by an industry-standard security platform).
- All personnel and third parties authorized to access or handle company data.
- All categories of data, from routine operational records to more sensitive customer or business information.

2. Roles and Responsibilities

Executive Management:

Provides strategic direction and allocates resources for the overall security program. Approves major changes to security policies and procedures.

Chief Security Officer (CSO):

Oversees daily security operations, including monitoring, incident response, and policy enforcement. Regularly reviews and updates security controls to align with best practices and evolving

threats.

All Personnel:

Must understand and comply with the Information Security Policy. Must report any suspicious activity or potential security incidents to the CSO.

3. Physical Security

Controlled Access:

Offices and secured areas require appropriate access mechanisms (e.g., keys, electronic locks). Only authorized individuals should enter restricted spaces containing critical infrastructure or confidential documents.

Visitor Protocol:

Visitors or vendors are permitted only when they have a legitimate business need. Sensitive information should not be visible, and unattended equipment must be locked or logged off.

Device Safeguards:

Workstations must be locked when not in use. Equipment is stored securely (e.g., locked cabinets) when not actively in operation.

4. Device Management and Endpoint Security

Endpoint Protection:

All company devices run an advanced security agent for real-time threat detection. Operating systems and critical applications are kept current with vendor-released patches.

Data on Devices:

Storing large volumes of sensitive data locally is discouraged; cloud services should be used instead. If business needs require offline data storage, appropriate encryption or secure methods are strongly recommended.

Device Lifecycle:

Deployment: New devices are configured in accordance with security guidelines, including strong access credentials.

Decommissioning: Prior to disposal or reassignment, devices undergo secure data erasure to prevent unauthorized recovery.

5. Data Classification and Retention

Data Categories:

- **Sensitive Data:** Personally identifiable information (PII), financial records, or intellectual property.
- **Internal Data:** Business plans, operational records, or non-public financials.
- **Public Data:** Materials intended for external distribution or marketing.

Retention Periods:

Sensitive records and required documentation (such as those under applicable U.S. regulations) are retained for the minimum legally mandated duration or as needed for business continuity. Non-critical data is retained only as long as it serves a valid business purpose.

Deletion and Disposal:

Systems must be configured to delete or archive data that has reached the end of its retention period. Physical records are shredded or otherwise destroyed to ensure they are unreadable, and digital records are securely wiped.

6. Access Management for Production Assets

Request and Approval:

Access to production environments or critical data is granted only upon a documented request stating the legitimate business need. The CSO (or a delegated manager) reviews and approves all such requests, ensuring least-privilege principles are followed.

Provisioning and Logging:

Approved permissions are recorded in an access control list or ticketing system for audit and compliance. Access credentials must not be shared; each user has unique credentials.

Periodic Review:

The CSO conducts scheduled reviews (e.g., quarterly) to confirm that access rights remain aligned with current roles and responsibilities. Any identified excess or outdated permissions are promptly revoked or adjusted.

Revocation:

Access is immediately revoked when no longer needed or if there are security concerns. All revocation actions are logged for audit purposes.

7. Monitoring and Logging

Network and Endpoint Monitoring:

The organization uses a comprehensive endpoint security solution to monitor devices for malicious activities or policy violations. System logs and security alerts are consolidated to facilitate rapid detection and correlation of potential threats.

Cloud Monitoring:

Production assets (e.g., within Firebase, Google Cloud, or other providers) rely on built-in logging and alerting features (e.g., abnormal traffic spikes, error rates). The organization uses Security Command Center or equivalent to highlight misconfigurations or vulnerabilities.

Audit Trails:

All critical systems log administrative actions, authentication events, and configuration changes. Logs are retained securely for a defined period to support incident investigations.

8. Incident Response

Detection and Classification:

The CSO monitors alerts and user reports to identify potential incidents (e.g., unauthorized access, malware infiltration). Incidents are classified by severity (Critical, High, Medium, Low) to prioritize response.

Containment Measures:

Infected or compromised endpoints are quarantined using the organization's endpoint security solution. Compromised credentials are reset; any affected cloud services may be paused or reconfigured to block further intrusion.

Investigation and Recovery:

The CSO gathers logs and forensic artifacts to determine the root cause, scope, and impact. Systems are restored from clean backups or re-imaged; patches and configuration fixes are applied to prevent recurrence.

Post-Incident Review:

A root cause analysis is documented, and lessons learned inform updates to security controls, policies, or training programs. Management reviews the incident report to ensure that corrective actions are implemented.

9. Training and Awareness

Mandatory Security Training:

All personnel complete **annual** security training, which covers:

- Recognizing phishing and social engineering tactics
- Proper handling of sensitive data
- Incident reporting procedures

Refresher and Specialized Sessions:

Additional sessions may be scheduled for new hires or to address emerging threats. Records of training completion are maintained for compliance and quality assurance.

Policy Acknowledgment:

Employees must read and acknowledge this Information Security Policy upon joining and after each significant update.

10. Third-Party and Vendor Management

Vendor Assessment:

Before granting vendors access to systems or data, the organization evaluates their security posture and contractual obligations. Clear agreements specify confidentiality requirements, breach notification timelines, and compliance commitments.

Limited Access:

Vendors receive only the privileges necessary for their function, with credentials revoked upon project completion or if security issues arise. The CSO keeps records of all third-party authorizations.

External Integrations:

Payment or blockchain integrations must align with the organization's security standards and any applicable regulatory obligations. External services are monitored for potential vulnerabilities affecting the organization's data or systems.

11. Auditing and Policy Review

Internal Audits:

Security controls, logs, and access rights may be periodically audited to verify adherence to this policy. Audit findings, along with recommendations, are presented to Executive Management.

Documentation:

Records of access changes, incident reports, and other key security artifacts are retained in a secure repository. Retention periods align with business or regulatory requirements.

Policy Maintenance:

This policy undergoes an annual review or is updated whenever significant changes occur (e.g., new technologies, regulatory shifts). Revisions are communicated promptly to all staff, and version control is applied to maintain a clear update history.

12. Enforcement and Exceptions

Compliance Enforcement:

Violations of this policy may lead to disciplinary action, up to and including termination or legal measures if warranted. All employees and vendors are expected to report any non-compliance concerns to the CSO for prompt investigation.

Exceptions:

Any exceptions must be documented, with clear justifications, scope, and duration. The CSO, in consultation with Executive Management, approves or denies exception requests.

13. Conclusion

This Information Security Policy serves as the foundation for protecting corporate assets, maintaining operational continuity, and aligning with best practices. By adhering to these principles—covering device management, data classification, secure access controls, robust incident response, and ongoing training—the organization can mitigate risks effectively and adapt as new challenges or opportunities arise. All employees and relevant stakeholders are responsible for upholding the standards set forth in this policy.

14. Senior Manager Approval

I have approved this Information Security Policy as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of information security standards and regulations. Additionally, this policy reflects our commitment to safeguarding our customers' data and ensuring their privacy and trust in our services.

Signed:
Name:
Title:
Date:

Revision	Revision Date	Effective Date	Description of Changes	Approved By
v1.0	January 2025	January 2025	- Initial Release	David Trost
v1.1	February 2025		- Switch to md - add revisions - fix approval	