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

Compto Public Benefit Corporation Security Incident Response Program: Compliance and Supervisory Procedures

1. Introduction

All security detection, triage, and response activities in our company are overseen and carried out by the Chief Security Officer ("CSO"). This process applies to protecting our work devices—managed through a centralized endpoint security platform—and securing our production assets in Firebase, which are monitored using a suite of cloud monitoring and security tools.

2. Monitoring and Detection

The CSO relies on several tools and configurations to identify potential security events. A dedicated endpoint security platform is installed on all work devices to detect suspicious behaviors such as malicious file executions, anomalous user activity, and questionable network traffic. It also provides automated alerts that indicate potential endpoint threats or policy violations. Meanwhile, a cloud-based logging and monitoring system centralizes logs from our Firebase production environment and related cloud services. These tools track performance metrics—such as CPU usage, network traffic, and error rates—and use alerting thresholds to flag abnormal patterns or spikes. Google Cloud Security Command Center further consolidates security findings and possible vulnerabilities across our cloud environment, highlighting misconfigurations, exposed services, or suspicious activities that might jeopardize production integrity.

Any alerts triggered by these systems are immediately reviewed by the CSO, who also encourages employees to report suspicious emails, login issues, or other anomalies. If such reports arise, the CSO investigates them alongside the automated alerts.

3. Incident Classification and Triage

Upon receiving an alert or notification, the CSO performs an initial assessment to determine the incident's severity and urgency:

Severity 1 (Critical):

Incidents indicating active data breach, high likelihood of data loss, or severe disruption to production services. Immediate action is required.

Severity 2 (High):

Incidents suggesting malicious activity (e.g., malware infection, unauthorized network access) with potential to escalate unless promptly contained.

Severity 3 (Medium):

Suspicious or anomalous behavior that may become more serious over time, such as unusual login attempts or traffic patterns.

Severity 4 (Low):

Minor policy violations, small misconfigurations, or benign anomalies that pose limited immediate threat.

After establishing the severity level, the CSO gathers log data from the organization's security platforms and any additional relevant sources. This triage helps confirm if the alert signals a legitimate threat and informs the next steps for containment.

4. Containment

If the incident requires immediate action to prevent further damage, the CSO initiates containment measures:

Endpoint Isolation:

Using the organization's security platform, the CSO can quarantine a compromised or suspicious device. This cuts off network connectivity except for secure communication with the endpoint security system for continued investigation.

Access Restriction:

If an account is suspected to be compromised, the CSO resets passwords, revokes API tokens, and enforces multifactor authentication as needed.

Cloud Environment Safeguards:

Potentially vulnerable or exploited services in Firebase or Google Cloud are paused, locked down, or reconfigured. Firewall rules are adjusted to block malicious IP addresses, and snapshots of suspect virtual machines or data stores are captured to preserve forensic evidence.

These steps ensure that the threat does not spread to additional systems or exfiltrate sensitive information during the investigation phase.

5. Investigation and Analysis

With the incident contained, the CSO conducts a comprehensive inquiry:

Gather Logs and Evidence:

Pulls logs from endpoint security agents, cloud-based logging tools, and any application logs.

Root Cause Assessment:

Determines if the source was a phishing attempt, unpatched vulnerability, stolen credentials, or system misconfiguration. Identifies which systems and data were affected, and whether sensitive information was accessed or exfiltrated.

Impact Evaluation:

Estimates the scope of any data or service compromise. Considers the potential need for legal or regulatory disclosures based on the type of data involved. The CSO documents these findings to decide on the best strategy for remediation and to ensure all compromised elements are addressed.

6. Eradication and Recovery

Once the investigation is complete and the scope of the threat is clearly understood, the CSO moves forward with eradication and restoration:

Removing Threats:

Cleans or re-images any compromised endpoints to ensure no malicious files, backdoors, or configuration changes remain. In the cloud environment, redeploys containers or services from secure, verified images.

Patching and Updating:

Applies relevant security patches to operating systems, applications, firmware, or dependencies that contributed to the incident. Disables or corrects any faulty configurations, particularly in Firebase and Google Cloud settings.

Verifying System Integrity:

Conducts scans or tests to confirm that systems are free of malware or vulnerabilities. Gradually returns isolated devices or services to normal operation, monitoring for signs of persistent

threats. The CSO may decide to maintain heightened monitoring to confirm that the threat has been completely eradicated and the environment is stable.

7. Post-Incident Activities

Following the successful containment and mitigation of the incident, the CSO reviews the response process to strengthen future readiness:

Lessons Learned Review:

Identifies what worked effectively, such as quick detection or efficient isolation, and what could be refined for speed or thoroughness. Investigates whether additional or improved logging, alert thresholds, or training is needed.

Documentation and Reporting:

Prepares a summary report detailing the timeline, severity classification, root cause, and corrective measures. Assesses if any regulatory or legal disclosures are required.

Policy Updates and Training:

Revises incident response documentation to incorporate new findings. Informs employees about any changes to security protocols, especially if user behavior was part of the root cause.

8. Ongoing Maintenance

The CSO ensures that the overall security posture remains robust by:

Regularly Reviewing Detection Rules:

Updates and refines endpoint security rules and configuration to keep pace with evolving threats. Enhances Google Cloud Monitoring and Security Command Center settings to spot new vulnerabilities.

Periodic Testing and Drills:

Conducts tabletop exercises or simulated attacks to evaluate the speed and efficacy of the incident response process. Validates that all endpoints remain protected, patched, and monitored.

Continuous Improvement:

Monitors industry threat intelligence for emerging attack vectors relevant to our environment. Ensures consistent alignment with best practices for endpoint security, cloud service configuration, and employee cybersecurity awareness.

Through this structured approach—encompassing vigilant monitoring, swift triage, meticulous containment, thorough investigation, decisive eradication, and ongoing refinement—the CSO maintains the security and resilience of our company's devices and production assets.

9. Senior Manager Approval

I have approved this Security Incident Response Process as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of security incident response standards.

Signed:
Name:
Title:
Date:

Revisions

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	