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

Compto Public Benefit Corporation Production Access Management Program: Compliance and Supervisory Procedures

1. Purpose and Scope

This process governs how individuals within the organization request access to production systems and data, how those requests are assessed and approved, how access is periodically reviewed, and how it is ultimately revoked when no longer necessary. The scope covers any production environment or sensitive data repository managed by the company, ensuring proper authorization and adherence to the principle of least privilege.

2. Roles and Responsibilities

- **CSO (Chief Security Officer):** Oversees the entire access control process, makes final determinations on high-risk requests, and ensures adherence to security policies.
- **Requestor:** An individual requiring access to production systems or data for legitimate business purposes.
- **System/Data Owner:** The person with primary responsibility for a given production asset or dataset. Reviews and recommends whether access should be granted.
- **Approver (could be the CSO or delegated manager):** Reviews access requests, validates business needs, and formally grants or denies requests.

3. Access Request

1. **Identify Need:** The requestor determines they require access to a specific production system or dataset for a clear, legitimate business purpose.
2. **Submit Request:** The requestor completes a standardized access request form (e.g., through a ticketing system or a designated email) that includes:
    - Name, role, and department of the requestor
    - Specific assets or data to which access is needed
    - Justification for the request (business need)
    - Duration of access if temporary

3. **Routing to Appropriate Owner/Approver:** The completed form is sent to the System/Data Owner and/or the designated Approver (who may be the CSO for critical assets).

4. Approval Process

1. **Verification of Business Need:** The Approver (in consultation with the System/Data Owner if needed) verifies that the access request is valid and necessary.
2. **Risk Assessment:** For sensitive systems or data, the Approver assesses the level of risk involved, considering factors such as data sensitivity and potential impact on production stability.
3. **Decision and Notification:**
    - If approved, the Approver documents the approval and notifies the requestor and relevant stakeholders (e.g., the CSO).
    - If denied, the Approver provides a brief explanation to the requestor.

5. Access Provisioning (Granting Access)

1. **Assign Permissions:** The approved level of access is applied according to the principle of least privilege, granting only the specific rights needed.
2. **Document Changes:** The CSO or a designated administrator records the new access level in an access control list or centralized management tool.
3. **Implementation Confirmation:** The requestor is notified that their access has been granted. They must verify that the permissions align with what was requested and approved (no more, no less).

6. Periodic Access Review

1. **Scheduled Reviews:** At predefined intervals (e.g., quarterly), the CSO or System/Data Owner reviews all user permissions.
2. **Verification of Ongoing Need:** Each permission is assessed to confirm that it still matches the user's job requirements.
3. **Adjustment:** If any access is deemed unnecessary, it is revoked or adjusted to align with current needs.
4. **Documentation:** The reviewer documents any changes made during the access review in the relevant tracking system.

7. Access Revocation

1. **Trigger for Revocation:** Access may be revoked due to role changes, project completion, contract termination, or periodic review findings.
2. **Notification and Logging:** When the decision to revoke is made, the user is notified if appropriate. The revocation is logged in the access tracking tool for audit purposes.
3. **Immediate Revocation for Security Risks:** If an urgent security concern arises (e.g., suspicious activity or policy violation), the CSO may revoke access immediately without prior notice.

8. Documentation and Audit

1. **Centralized Logging:** All access requests, approvals, and revocations are documented in a secure, centralized system for auditing and compliance purposes.
2. **Audit Trail Maintenance:** The CSO ensures that logs are retained for an appropriate period to support investigations, compliance reviews, or incident response activities.

9. Continuous Improvement

1. **Policy Updates:** Feedback and lessons learned from each access request or review cycle inform revisions to this process.
2. **Training and Awareness:** The CSO provides regular training for staff on how to request and manage access securely.
3. **Automation:** Where feasible, automated workflows and policy-based controls are adopted to streamline requests, approvals, and revocations, reducing the chance of human error.

By following these steps, the organization ensures that access to production assets and data is carefully controlled, granted only to those with a legitimate business need, regularly reviewed, and promptly revoked when no longer necessary.

10. Senior Manager Approval

I have approved this Production Asset Management Policy as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of Production Asset Management standards and regulations.

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	