System Change Policy

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC8.1, CC3.4

Table 2: Document history

Date	Comment
Nov 28 2024	Updated controls & process

1 Purpose

Effective change management within CredX's production product and engineering environments is critical to ensuring the consistent delivery of high-quality software and services. It also ensures compliance with SOC 2 standards and mitigates risk. Any introduction of new systems or major changes to existing systems must follow established processes for documentation, specification, testing, quality control, and controlled implementation.

The objective of these procedures is to provide safeguards for developers and testers who have access to production systems, reducing the risk of unauthorized or untested code being deployed. This includes protecting against the inadvertent disclosure of confidential data, ensuring data integrity, and preventing availability issues.

By formalizing a change management process across the system development lifecycle, from initial design to ongoing maintenance, this policy ensures the confidentiality, integrity, and availability of information systems.

A "change" in this context refers to any intentional modification, addition, or removal of approved, supported, or baselined software, services, or associated documentation.

2 Scope

This policy applies to all systems and platforms in the CredX product and engineering environments that support our products and services. This includes operating systems, software, databases, applications, system configurations, and jobs associated with product and engineering environments.

The following are out of scope:

- Individual employee hardware
- Disaster recovery
- Changes to development and testing environments
- Administrative tasks, such as password resets, user provisioning, and file permission changes

3 Policy

All changes to CredX's product and engineering environment must follow a standardized process, categorized based on risk. The CTO owns this policy, ensuring it is updated annually or whenever there are significant business changes. The CTO will also make this policy accessible to all employees, ensuring changes are made appropriately without adverse effects on company operations.

3.1 Change Management Process

The change management process consists of the following key steps:

1. Planning:
    i. Assess and plan the change, including design, scheduling, dependencies, and associated risks.
2. Communication:
    i. Inform relevant stakeholders of the proposed change.
3. Testing:
    i. Perform necessary testing, including user acceptance testing (UAT), code reviews, and security assessments.
4. Authorization:
    i. Ensure only authorized changes are deployed.
5. Implementation:
    i. Implement the change according to the approved plan.
6. Documentation:
    i. Maintain comprehensive documentation for each change, capturing planning, testing, approval, implementation, and contingency procedures.
7. Post-Change Review:
    i. Conduct a post-implementation review to assess the effectiveness and identify opportunities for improvement.

3.2 Change Controls & Evidence

Change management procedures are documented and reviewed annually.

i. **Evidence**: Document history indicating the last review and approval within the past year.

ii. Changes must be approved before implementation. Evidence of approval includes business owner sign-off or reasonable checks by the Tech Team. Approvals are stored within the team's change management tool.

iii. **Testing Evidence**: For deployable software, testing scripts, UAT acknowledgments, and other testing-related documents are maintained.

iv. Changes must be documented, approved, and verified in production environments.

3.3 Security & Privacy Considerations

i. Baseline settings should only be altered if there's a valid security or privacy reason.

ii. **Evidence**: Changes must include specific acknowledgment within the build ticket.

3.4 Segregation of Duties

i. Users are restricted by role from deploying changes to production.

ii. Developers and business users do not have access to production code repositories or environments.

iii. **Evidence**: Roles are assigned, and periodic access reviews are performed.

3.5 Environment Separation

i. Development, testing, and production environments are kept separate to minimize the risk of cross-environment issues.

ii. Changes are tested in staging environments before being deployed to production. In exceptional circumstances, testing may occur in production with proper approvals.

3.6 Backup and Rollback Procedures

i. Rollback-ready backups are created for each production deployment, with the last four backups stored in the production environment.

ii. **Evidence**: Code is stored in version-controlled Git repositories and tagged before release. Daily backups are taken of the production database.

4 Types of Changes

Changes are classified as follows:

a. **Minor Change**:

   i. Low-risk, well-understood changes affecting isolated code components.

   ii. Changes like text updates, minor styling adjustments, or non-impactful code updates.

   iii. All steps of the change process must be documented, including code review and testing.

b. **Routine Change**:

i. Medium to high-risk changes with multiple dependencies or affecting critical services.

ii. Includes changes to core code captured by a Build ID.

iii. All steps documented, with testing and code review. Change is verified in the production environment after deployment.

c. **HotFix**:

i. Urgent fixes needed for customer-facing workflows or critical errors.

ii. Testing, code review, and explicit approval required.

iii. Deployment is documented, and stability is monitored post-release.

d. **Emergency Change**:

i. Critical changes required immediately to mitigate significant risks or prevent downtime.

ii. Testing may not occur prior to implementation, but a post-implementation review is required within two business days.

e. **Vendor-Initiated Change**:

i. Changes proposed by vendors (e.g., patching, updates).

ii. Follows all standard change procedures with appropriate testing and communication.

5 Document Management

This policy is subject to regular management review and annual updates. Changes must be properly communicated, documented, and acknowledged by stakeholders.

6 Enforcement

Failure to comply with this policy may result in disciplinary action, including termination of employment or contracts.