Processing Integrity Policy

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	PI1.1, PI1.2, PI1.3, PI1.4, PI1.5

Table 2: Document history

Date	Comment
Apr 21 2026	Completed policy in full to satisfy SOC 2 Processing Integrity TSC

1 Purpose and Scope

a. The purpose of this policy is to ensure that CredX's system processing is complete, valid, accurate, timely, and authorized, in order to meet the organization's processing integrity objectives.

b. This policy applies to all production systems, applications, and data processing activities within CredX's information security program.

c. This policy applies to all employees, contractors, and third parties involved in the design, operation, and maintenance of CredX's production systems.

2 Background

a. Processing integrity means that system processing is complete, accurate, timely, and authorized. Failures in processing integrity can result in incorrect outputs, corrupted data, or unauthorized transactions that may harm customers and the organization. This policy establishes controls to detect and prevent processing errors and ensure the reliability of CredX's services.

3 Policy

3.1 Information and Communication (PI1.1)

a. CredX must obtain, generate, and communicate relevant, quality information to support processing integrity objectives. This includes:

   i. Clear specifications for data inputs, processing logic, and expected outputs for all production systems.

   ii. Documentation of product and service specifications maintained and accessible to relevant personnel.

   iii. Procedures for communicating processing errors, anomalies, or exceptions to appropriate stakeholders in a timely manner.

b. Changes to system specifications or processing logic must be communicated to affected teams before implementation, in accordance with the System Change Policy.

3.2 Input Controls (PI1.2)

a. All production systems must implement controls over inputs to ensure completeness and accuracy:

   i. **Input Validation:** All data inputs must be validated against defined formats, ranges, and business rules before processing. Invalid inputs must be rejected with appropriate error messages.

ii. **Completeness Checks:** Systems must verify that required data fields are present and non-null before processing transactions.

iii. **Duplicate Detection:** Where applicable, systems must implement controls to detect and prevent duplicate transaction processing.

iv. **Authorization Controls:** Inputs must be authorized by appropriate parties before processing. Unauthorized or unauthenticated inputs must be rejected.

v. **Error Logging:** All input validation failures and rejected inputs must be logged for review and investigation.

3.3 Processing Controls (PI1.3)

a. CredX must implement controls over system processing to ensure accuracy, completeness, and authorization:

i. **Processing Validation:** Systems must verify that all processing steps complete successfully. Failed or incomplete processing must generate alerts and be logged.

ii. **Segregation of Duties:** Critical processing steps must be segregated so that no single individual can initiate and complete a high-risk transaction without a second authorization.

iii. **Exception Handling:** Systems must define and implement exception handling procedures for unexpected conditions. Exceptions must be logged, alerted, and reviewed by responsible parties.

iv. **Reconciliation:** Where processing involves financial or critical operational data, reconciliation controls must be implemented to verify that outputs match expected totals and that no data is lost or duplicated during processing.

v. **Audit Trails:** All processing activities must generate audit trail records sufficient to reconstruct the sequence of events and identify responsible parties.

3.4 Output Controls (PI1.4)

a. CredX must implement controls to ensure that system outputs are delivered completely, accurately, and in a timely manner:

i. **Output Validation:** Outputs must be validated against specifications before delivery to customers or downstream systems. Anomalous or unexpected outputs must be flagged for review.

ii. **Timely Delivery:** Outputs must be delivered within defined service-level timeframes. Delays beyond acceptable thresholds must generate alerts and be tracked to resolution.

iii. **Output Authorization:** Outputs containing sensitive or confidential information must be delivered only to authorized recipients.

iv. **Delivery Confirmation:** For critical outputs, delivery confirmation mechanisms must be implemented to detect and remediate non-delivery.

v. **Output Logging:** All system outputs must be logged, including timestamps, recipients, and content identifiers, to support traceability and investigation.

3.5 Storage and Backup of Processing Data (PI1.5)

a. All inputs, items in processing, and outputs must be stored completely, accurately, and in a timely manner, in accordance with system specifications:

i. **Data Storage Integrity:** Systems must implement checksums, hashing, or equivalent mechanisms to detect data corruption in storage.

ii. **Backup of Processing Data:** All critical processing data (inputs, intermediate state, outputs) must be backed up in accordance with CredX's Availability Policy. Backups must be tested for recoverability at least twice per year. **No restore test has yet been performed.**

iii. **Retention:** Processing records must be retained for the periods defined in the Data Retention Policy. Records required for regulatory compliance or audit purposes must be retained for the applicable legal retention period.

iv. **Recovery Testing:** The ability to restore processing data from backup must be tested at least annually to confirm that data can be fully recovered within defined recovery time and recovery point objectives.

4 Monitoring and Review

a. Processing anomalies, errors, and exceptions must be reviewed by system owners on at least a monthly basis.

b. Metrics related to processing integrity (e.g., error rates, failed transactions, output delivery failures) must be monitored continuously and reported to management quarterly.

c. Any systemic processing integrity failures must be treated as security incidents and handled in accordance with the Security Incident Response Policy.

5 Enforcement

a. System owners are responsible for implementing and maintaining processing integrity controls within their systems.

b. Violations of this policy may result in disciplinary action up to and including termination. Systemic violations must be reported to the ISM and escalated to the Leadership Team.