🔒 **SecureFlow Inc.**

Security Requirements Engineering Best Practices

Internal Standards & Guidelines for Enterprise Software Development

Welcome to SecureFlow's Security Requirements Framework:

This document outlines the mandatory best practices and standards that SecureFlow engineers must follow when specifying security requirements for any product or system. Our goal is to ensure that all security requirements are precise, testable, and aligned with industry standards (NIST SP 800-53, ISO 27001, OWASP ASVS). This framework helps us build more secure, compliant, and robust systems.

1. Core Principles of Security Requirements

Every security requirement at SecureFlow must adhere to these fundamental principles. These are non-negotiable guidelines that ensure consistency and quality across all product lines.

1.1 Principle of Clarity & Specificity

What It Means

Security requirements must be written with absolute clarity. Vague terminology like "secure," "protected," "strong," or "highly available" is forbidden. Instead, specify exact technical mechanisms, algorithms, configurations, and thresholds.

Examples

The system must be secure.

All customer data classified as PII shall be encrypted using AES-256 in GCM mode with randomly generated 256-bit keys. Encryption key storage in dedicated HSM (Hardware Security Module). Key rotation every 90 days.

Why It Matters

Vague requirements lead to implementation ambiguity, making it impossible to test, audit, or enforce consistently. Specific requirements enable clear acceptance criteria.

1.2 Principle of Testability & Measurability

What It Means

Every security requirement must include concrete acceptance criteria that can be objectively verified through testing, audit, or measurement.

Template: "The system shall..."

[WHAT] shall [ACTION] [MECHANISM] [PARAMETER/THRESHOLD] for/within [SCOPE/TIMEFRAME].

Example Breakdown

All failed authentication attempts shall be logged with timestamp, source IP, username, and failure reason, retained for minimum 180 days, and automatically deleted after that period.

- **WHAT:** Failed authentication attempts
- **ACTION:** logged
- **MECHANISM:** timestamp, source IP, username, failure reason
- **PARAMETER:** 180 days retention
- **SCOPE:** all authentication events

Test Case Derivation

From the above requirement, we can derive:
1. Log file contains: timestamp, IP, username, failure reason
2. Attempt to login with wrong password → entry appears in logs
3. Logs older than 180 days are deleted
4. Verify deletion happens automatically

1.3 Principle of Completeness (CIA Triad)

What It Means

Every product must have security requirements covering all three dimensions of the CIA (Confidentiality, Integrity, Availability) triad, appropriate to its risk profile.

Mapping Requirements to CIA

CIA Dimension	Focus Area	SecureFlow Requirement Areas
Confidentiality (C)	Preventing unauthorized access to data	Encryption (at rest, in transit), Access Control, Authentication, Data Classification
Integrity (I)	Preventing unauthorized modification	Data Validation, Checksums, Digital Signatures, Audit Logging, Input Sanitization
Availability (A)	Ensuring authorized access and function	SLA/Uptime guarantees, Failover, Disaster Recovery, DDoS Protection, Rate Limiting

SecureFlow Policy

Every product release must include explicit requirements from all three CIA categories. Security requirement reviews will check for this completeness before release approval.

2. Domain-Specific Best Practices

2.1 Access Control & Authentication

Standards Referenced: NIST SP 800-53 (AC: Access Control, IA: Identification & Authentication), OWASP ASVS V2/V3

AC-001 Role-Based Access Control (RBAC)

Requirement: All systems handling sensitive data must implement Role-Based Access Control with clearly defined roles, permissions matrices, and enforcement mechanisms.

SecureFlow Standard Template

The system shall implement RBAC with the following roles: [LIST ROLES]. Each role shall have explicit permissions for [READ/WRITE/DELETE/EXECUTE] on [specific resources/data types]. Access decisions shall be logged with timestamp, user ID, resource ID, action, and decision (allow/deny). Access logs shall be retained for minimum [PERIOD] and protected against modification using [PROTECTION MECHANISM].

Example at SecureFlow

SalesDB System (Product: Sales Management Platform):
The system shall implement RBAC with four roles: Admin, Sales Manager, Sales Rep, Viewer. Admins: full access to all customer records and configuration. Sales Manager: read/write access to records of their team's customers only. Sales Rep: read/write to their own customer records. Viewer: read-only access to non-sensitive summary reports. All access decisions logged with timestamp, user ID (AD domain), resource ID, action (read/write/delete), and decision. Logs retained 2 years in tamper-proof archive.

Checklist for AC Requirements

Before Approval

- All roles explicitly listed (no vague role names)
- Permissions matrix exists and is signed off by product owner
- Cross-functional access (admin to user data) explicitly denied
- Logging mechanism specified (which system, which fields)
- Retention period defined
- Tamper protection mechanism for logs defined

IA-001 Multi-Factor Authentication (MFA)

Requirement: All accounts with administrative or sensitive data access must require Multi-Factor Authentication.

SecureFlow Standard

All accounts with access to [SENSITIVE DATA/ADMIN FUNCTIONS] shall require multi-factor authentication (MFA) using [METHODS: TOTP/SMS/Push/Hardware Key]. MFA implementation must follow NIST SP 800-63B standards. Session timeout after [DURATION] of inactivity. Account lockout after [N] failed attempts for [DURATION].

Example Implementation

CloudDeploy Admin Console (Internal Tool):
All admin accounts shall require MFA using TOTP (Google Authenticator, Authy) or hardware U2F keys (FIDO2). Passwords must be 16+ chars, include uppercase/lowercase/numbers/symbols, prevent reuse of last 10 passwords. Session timeout: 15 minutes for Tier-1 admins, 30 minutes for operations staff. Account lockout: 5 failed attempts → 60-minute lockout. MFA setup enforced at first login.

2.2 Cryptography & Data Protection

Standards Referenced: NIST SP 800-53 (SC: System & Communications Protection), ISO 27001 Annex A, OWASP ASVS V6

SC-001 Encryption at Rest

Requirement: All data classified as Confidential or Restricted must be encrypted at rest using approved encryption standards.

SecureFlow Approved Standards

- **Algorithm:** AES-256 (256-bit key length mandatory)
- **Mode:** GCM (Galois/Counter Mode) for authenticated encryption
- **NOT allowed:** AES-128, ECB mode, proprietary algorithms, MD5 for hashing
- **Key Storage:** Hardware Security Module (HSM) or Key Management Service (KMS)
- **Key Rotation:** Every 90 days minimum, retain 3 previous keys for decryption

Example Requirement

Customer Database Encryption:
All personally identifiable information (PII) including names, email, phone, SSN stored in CustomerDB shall be encrypted using AES-256-GCM. Encryption keys stored in AWS KMS with access restricted to application service role. Automatic key rotation every 90 days. Previous 3 keys retained for archive data decryption. Key access audited and logged per entry.

SC-002 Encryption in Transit (TLS)

Requirement: All data transmitted over networks must be encrypted using TLS.

SecureFlow Standard

All data transmitted between client and server, or between internal services, shall use TLS 1.3 or higher. Cipher suites must use 256-bit encryption strength. Perfect Forward Secrecy (PFS) required. Certificate pinning for mobile clients. HSTS header min. 31536000 seconds. No plaintext HTTP allowed; all HTTP requests redirected to HTTPS.

Approved Cipher Suites (TLS 1.3)

- TLS_AES_256_GCM_SHA384 ✓ RECOMMENDED
- TLS_CHACHA20_POLY1305_SHA256 ✓ Acceptable
- TLS_AES_128_GCM_SHA256 ✓ Acceptable (minimum)

Not Allowed (TLS 1.2 & below)

- Any SSL 3.0, TLS 1.0, TLS 1.1 ✗
- DES, RC4, MD5 ✗
- Self-signed certificates (except local dev) ✗

2.3 Input Validation & Injection Prevention

Standards Referenced: OWASP ASVS V5 (Validation, Sanitization, Encoding), OWASP Top 10 #3 Injection

IV-001 Input Validation Framework

Requirement: All user-supplied input must be validated against strict whitelists before processing.

SecureFlow Validation Levels

Level	Validation Type	Example Fields
L1: Character Set	Whitelist allowed characters (a-z, 0-9, specific symbols)	Username, Product ID, API Keys
L2: Format	Regex match, RFC compliance	Email (RFC 5322), Phone (E.164), URL
L3: Semantic	Business logic validation	Order quantity > 0, Valid enum value
L4: Encoding	Proper output encoding per context (HTML, URL, SQL)	HTML entities, URL encoding, parameterized queries

Example Requirement

User Registration Form:
Username field shall accept only alphanumeric characters and underscores, max 32 characters. Email field shall match RFC 5322 format. Password: minimum 12 chars, must contain uppercase, lowercase, digit, and symbol. All fields trimmed of whitespace. On validation failure: reject request, log attempt with timestamp/IP/field/attempted value (first 100 chars), return generic error message (no field-specific hints).

2.4 Logging, Audit & Incident Response

Standards Referenced: NIST SP 800-53 (AU: Audit & Accountability, IR: Incident Response), ISO 27001 Annex A.12

AU-001 Security Event Logging

Requirement: All security-relevant events must be logged with sufficient detail for forensic investigation and audit.

Mandatory Log Fields (SecureFlow Standard)

timestamp (UTC, millisecond precision) event_type (authentication, authorization, data_access, config_change, etc.) user_id / service_principal source_ip_address action (read/write/delete/execute/authenticate/authorize) resource_id (file, API endpoint, database record, etc.) result (success/failure) error_code (if applicable) additional_context (e.g., reason for denial, data classification)

Example Requirement

API Gateway Logging:
All API requests shall be logged to centralized log system with: timestamp (UTC-0, nanosecond), HTTP method, endpoint path, query parameters (sanitized, no secrets), source IP, authentication method used (API key, OAuth token, mTLS), authenticated principal ID, response status code, response time (milliseconds), request/response size (bytes). Logs stored in tamper-proof append-only archive. Log integrity verified via chained HMACs (each entry includes HMAC of previous entry). Logs retained 2 years hot storage, 7 years archive.

IR-001 Incident Detection & Alert

Requirement: Critical security events must trigger automated alerts and incident response processes.

SecureFlow Alert Thresholds

- **CRITICAL (Alert <5 minutes):** Brute-force attack detected, unauthorized privilege escalation, encryption key compromise
- **HIGH (Alert <1 hour):** Multiple failed authentication attempts (>10 in 1 hour), suspicious data access pattern, configuration tampering
- **MEDIUM (Alert <24 hours):** Policy violations, missing patches, log deletion attempts

Example

API Rate Limiting & DDoS Protection:
System shall detect and alert on: >100 failed auth attempts from single IP in 5 minutes (immediate alert to security team). >1000 requests/second from single IP to public endpoints (trigger rate limiting: 100 req/sec for that IP, 1-hour ban after 3 violations). All DDoS events logged with timestamp, source IP, request rate, and response action.

2.5 Availability & Disaster Recovery

Standards Referenced: NIST SP 800-53 (CP: Contingency Planning), ISO 27001 Annex A.17

AV-001 Service Level Agreements (SLA)

Requirement: All production systems must have defined, measurable availability targets and recovery objectives.

SecureFlow SLA Classes

Class	Availability Target	RTO	RPO	Typical Usage
Tier 1	99.99%	<1 min	<1 min	Payment processing, Critical customer systems
Tier 2	99.95%	<5 min	<5 min	Main product, Core APIs
Tier 3	99.9%	<15 min	<15 min	Admin tools, Batch processes

Example Requirement (Tier 2)

Primary Product SLA:
System shall maintain 99.95% uptime monthly (max 21.6 minutes unplanned downtime). RTO for complete datacenter failure: 5 minutes. RPO: 5 minutes (max data loss). Measured via synthetic monitoring from 3 geographically distributed probes. Automated failover to secondary region triggered within 2 minutes of primary failure detection. Backup RPO: every 5 minutes (continuous replication). Disaster recovery drills quarterly with documented results.

3. Requirements Review Checklist

All security requirements must pass this checklist before product release approval.

Pre-Release Security Requirements Checklist

- All requirements use "shall" (mandatory) vs "should" (optional)
- Zero vague terms: no "secure," "strong," "protect," "robust," "sufficient"
- Each requirement includes specific algorithm/mechanism (AES-256, TLS 1.3, TOTP, etc.)
- Quantifiable thresholds defined (timeouts, key lengths, uptime %, retention periods)
- CIA coverage verified: Requirements address Confidentiality, Integrity, AND Availability
- Test cases derivable from each requirement (yes/no decision possible)
- Standards mapping completed (NIST control ID, OWASP ASVS section, ISO 27001 reference)
- Scope clearly defined: which data types, which users, which systems affected
- Logging requirements explicit: which events logged, which fields, retention period
- Enforcement mechanisms specified: how is compliance monitored/audited
- No contradictions between requirements
- Terminology glossary attached (PII, Confidential, etc. defined)
- Compliance certification sign-off from: Product Owner, Security Team, Compliance

4. Real-World Examples from SecureFlow Products

4.1 Product: "VaultLock" - Password & Secrets Management

VaultLock is a enterprise password vault. Here's how we applied SecureFlow best practices to 3 critical requirements.

REQ-VL-C-001: Encryption of Stored Secrets

All secrets stored in VaultLock vault (passwords, API keys, certificates) shall be encrypted at rest using AES-256-GCM. Master encryption key stored in AWS KMS with access restricted to VaultLock service role (no human access). Key rotation automatic every 60 days. Previous 5 keys retained for legacy secret decryption (encrypted and archived separately). Each decryption operation requires audit log entry with timestamp, user ID, secret ID, and reason code.

REQ-VL-A-001: Access Audit Trail

All secret access attempts (successful and failed) shall be logged to immutable audit log with: timestamp (UTC), user ID, secret ID, action (view/edit/delete), client IP, MFA method used, and decision (allow/deny with reason). Logs retained indefinitely. Log integrity verified via HMAC-SHA256 chaining. Admin access to audit logs requires explicit approval from CISO with MFA.

REQ-VL-I-001: Secret Integrity Verification

On every secret retrieval, system shall verify integrity via HMAC-SHA256 computed at storage time. If integrity check fails: deny retrieval, log critical event, alert security team within 1 minute, preserve evidence for forensic analysis.

4.2 Product: "SecureAPI" - API Gateway & Rate Limiting

SecureAPI protects customer APIs from unauthorized access and DDoS attacks.

REQ-SA-A-001: DDoS Detection & Mitigation

SecureAPI shall detect distributed denial-of-service (DDoS) attacks via: (1) Source IP request rate threshold: >1000 requests/sec per IP → immediate rate limiting to 100 req/sec; (2) Geographic anomaly: >80% traffic from non-whitelisted country → investigation alert; (3) User-agent anomaly: >100 different user-agents per IP in 1 hour → temporary IP block. All DDoS detection logged with timestamp, source IP, request pattern, and response action.

REQ-SA-C-001: API Key Rotation

All API keys shall expire after 90 days of creation. 30 days before expiration, system shall notify key owner via email with rotation instructions. After 90 days: key disabled (returns 401 Unauthorized). No exceptions. Key rotation enforcement monitored and reported monthly to CISO.

Conclusion

These best practices represent SecureFlow's commitment to building secure, compliant, and robust systems. All product teams must adhere to these standards before release. Regular training and security reviews ensure continuous improvement of our security posture.

Document Information
Organization: SecureFlow Inc.
Document Version: 2.1
Last Updated: January 2026
Classification: Internal Use
Next Review: July 2026
Maintained by: Security Engineering Team