Nayaone Information Security Policy

1. Introduction

1.1 Purpose

1.1.1 This policy establishes the framework for protecting Nayaone's information assets and ensuring compliance with applicable regulations and standards.
1.1.2 This policy ensures robust cybersecurity measures protecting organizational assets and maintaining regulatory compliance.

1.2 Scope

1.2.1 This policy applies to all Nayaone facilities, employees, contractors, and systems across:
a) Headquarters in Jakarta
b) Branch offices in Bandung and Surabaya
c) Manufacturing facility in Bogor
d) All digital and physical assets

1.3 Regulatory Compliance

1.3.1 This policy aligns with:
a) NIST SP 800-53 Security Controls
b) ISO 27001:2022 Information Security Standards
c) Indonesia Personal Data Protection Act
d) General Data Protection Regulation (GDPR)

2. Risk Management

2.1 Risk Assessment Framework

2.1.1 Conduct comprehensive threat analyses bi-annually.
2.1.2 Document and classify risks based on:
a) Probability of occurrence
b) Potential financial impact
c) Operational disruption potential
2.1.3 Develop and implement risk mitigation strategies for each identified risk.
2.1.4 Regular review and updates of risk assessments quarterly.

3. Access Control and Authentication

3.1 Session Management

3.1.1 Session generation requirements:

a) Use cryptographically secure random numbers

b) Include timestamp component

c) Bind to user context

d) Minimum 256-bit length

3.1.2 Session lifetime controls:

a) Maximum duration: 4 hours

b) Idle timeout: 15 minutes

c) Force renewal on privilege change

d) Immediate invalidation on logout

3.1.3 Session validation:

a) Verify on every request

b) Check IP binding

c) Validate timestamp

d) Verify user context

3.2 User Access Management

3.2.1 Implementation of role-based access control (RBAC).

3.2.2 Access granted based on principle of least privilege.

3.2.3 Quarterly access reviews conducted by department heads.

3.2.4 Immediate access revocation upon employment termination.

3.3 Authentication Requirements

3.3.1 Multi-factor authentication mandatory for all privileged access.

3.3.2 Password requirements:

a) Minimum 12 characters

b) Combination of uppercase, lowercase, numbers, and special characters

c) No dictionary words or sequential patterns

d) Regular password rotation every 90 days

3.3.3 Account lockout after 5 failed attempts.

3.3.4 Session timeout after 15 minutes of inactivity.

4. Network Security

4.1 Network Segmentation

4.1.1 Segregation of networks into:

a) Industrial Control Network (ICN)

b) Corporate Network

c) Guest Network

d) DMZ

4.1.2 Inter-network communication strictly controlled and monitored.

4.1.3 Regular network access audits conducted monthly.

4.2 Technical Controls

4.2.1 TLS 1.3 minimum for all communications.
4.2.2 Continuous network monitoring with 5-minute intervals.
4.2.3 Malicious traffic detection and automated response.
4.2.4 Implementation of IDS/IPS systems.
4.2.5 Regular certificate rotation every 12 months.

5. Data Protection

5.1 Physical Data Security

5.1.1 Restrict access to data centers with:
a) Biometric scanners
b) Security cameras with 24/7 monitoring
c) Access logs maintained for minimum 12 months
5.1.2 Environmental controls for temperature and humidity.
5.1.3 Fire suppression systems in all server rooms.

5.2 Data Encryption

5.2.1 Apply encryption for data at rest using AES-256.
5.2.2 Apply encryption for data in transit using TLS 1.3.
5.2.3 HTTPS mandatory for all web communications.
5.2.4 Secure key management and storage procedures.

5.3 Data Backup and Recovery

5.3.1 Regular automated backups performed daily.
5.3.2 Backups stored securely:
a) On-site encrypted storage
b) Off-site secure facility
c) Cloud backup with encryption
5.3.3 Backup integrity tested monthly.
5.3.4 Recovery procedures documented and tested quarterly.
5.3.5 Recovery time objective (RTO): 4 hours for critical systems.
5.3.6 Recovery point objective (RPO): 1 hour maximum data loss.

6. Device, IoT, and API Security

6.1 API Security

6.1.1 Authentication and Authorization:
a) OAuth 2.0 with PKCE for mobile applications
b) JWT configuration requirements:
- RS256 algorithm minimum
- Required claims: iss, sub, aud, exp, iat, jti
- Regular key rotation schedule every 6 months
c) MFA enforcement for sensitive operations
6.1.2 API Implementation:
a) Mandatory versioning for all APIs
b) Rate limiting implementation (1000 requests/hour per user)
c) Comprehensive input validation
d) Output data sanitization
e) Structured error handling without information disclosure
6.1.3 Mobile Application Security:
a) Certificate pinning implementation
b) Secure local storage encryption
c) Anti-tampering measures
d) Secure logging practices

6.2 Device Management

6.2.1 Comprehensive device inventory maintenance.
6.2.2 Secure device registration and authentication.
6.2.3 Regular firmware updates and security patches within 30 days.
6.2.4 Device-specific security controls implementation.
6.2.5 MAC address filtering and validation.

- Comprehensive device inventory maintenance
- Secure device registration and authentication
- Regular firmware updates and security patches
- Device-specific security controls
- MAC address filtering and validation

5.3 IoT Security Requirements

5.3.1 Device Hardware Security

- Implement secure boot with cryptographic verification
- Enable hardware-based security features (TPM/TEE if available)
- Disable unnecessary physical ports and interfaces
- Implement tamper detection mechanisms
- Protect debug interfaces and test points
- Implement secure firmware update mechanisms
- Ensure hardware entropy source for cryptographic operations

5.3.2 Device Software Security

- Enforce signed firmware validation
- Implement secure bootloader with signature verification
- Disable unnecessary services and ports
- Implement secure over-the-air (OTA) updates
- Regular security patches and updates
- Vulnerability remediation within 30 days
- Memory protection mechanisms enabled
- Secure storage of sensitive data
- Input validation for all data sources
- Secure logging practices
- Anti-rollback protection for firmware
- Regular security assessments and penetration testing

5.3.3 Authentication and Access Control

- Strong device authentication:
  - Unique device identifiers
  - Certificate-based authentication
  - Multi-factor authentication for admin access
  - No default credentials
  - Strong password policy enforcement
- Access Control:
  - Role-based access control (RBAC)
  - Principle of least privilege
  - Regular access reviews
  - Failed authentication monitoring
  - Account lockout mechanisms
  - Regular credential rotation

5.3.4 Data Protection

- Encryption:
  - Data in transit (TLS 1.3+ minimum)
  - Data at rest (AES-256 minimum)
  - Secure key storage
  - Regular key rotation
- Sensitive Data:
  - Protection of PII
  - Secure handling of video feeds
  - Encrypted sensor data
  - Secure storage of credentials
  - Data minimization principles
  - Secure data deletion procedures

5.3.5 Communication Security

- Network Security:
  - Isolation in separate VLAN
  - Controlled inter-VLAN routing
  - Network monitoring and IDS deployment
  - MAC address filtering and validation
  - Firewall rules for IoT traffic
- Protocol Security:
  - Secure MQTT over TLS
  - Certificate pinning for critical devices
  - Message signing for critical commands
  - Strong cipher suite requirements
  - Valid certificates from approved CAs
  - Regular certificate rotation and revocation checks

5.3.6 Cloud and Mobile Integration

- API Security:
  - Secure API endpoints
  - Rate limiting
  - Input validation
  - Output encoding
  - Error handling
- Mobile App Security:
  - App transport security
  - Certificate pinning
  - Secure local storage
  - Anti-tampering measures
  - Secure authentication
  - Secure session management

5.3.7 Physical Security

- Tamper-evident enclosures
- Secure storage of devices
- Physical access controls
- Environmental security controls
- Asset tracking and inventory
- Secure disposal procedures

5.3.8 Maintenance and Monitoring

- Regular security assessments
- Continuous monitoring:
  - Device behavior monitoring
  - Network traffic analysis
  - Security log analysis
  - Performance monitoring
- Incident Response:
  - Security incident detection
  - Incident reporting procedures
  - Incident investigation process
  - Recovery procedures
- Documentation:
  - Security configuration baseline
  - Change management procedures
  - Maintenance procedures
  - Security update procedures

7. Incident Response

7.1 Incident Classification and Reporting

7.1.1 Security incidents classified by severity:
a) Critical incidents: Report within 1 hour
b) High-severity incidents: Report within 4 hours
c) Medium-severity incidents: Report within 24 hours
d) Low-severity incidents: Report within 72 hours

7.2 Incident Handling Procedures

7.2.1 Immediate isolation of affected systems.
7.2.2 Investigation and root cause analysis within 48 hours.
7.2.3 Implementation of containment measures.
7.2.4 Documentation of incident response activities.
7.2.5 Post-incident review and improvements within 7 days.
7.2.6 Stakeholder notification per legal requirements.

8. Personnel Security

8.1 Pre-employment Security

8.1.1 Comprehensive background verification for all positions.
8.1.2 Security clearance assessment for sensitive roles.
8.1.3 Confidentiality agreement execution before employment start.

8.2 During Employment

8.2.1 Mandatory security awareness training:
a) Initial training within 30 days of employment
b) Annual refresher training
c) Specialized training for privileged users
8.2.2 Regular compliance monitoring and assessment.
8.2.3 Annual performance evaluations including security compliance.

8.3 Employment Termination

8.3.1 Return of all company assets within 24 hours.
8.3.2 Immediate access revocation to all systems.
8.3.3 Exit interview including security briefing.
8.3.4 Confidentiality reminder and agreement reaffirmation.

9. Compliance, Audit, and Enforcement

9.1 Internal Audits

9.1.1 Quarterly comprehensive internal audits conducted by IT security team.
9.1.2 Regular compliance assessments against policy requirements.
9.1.3 Unannounced spot checks performed monthly.
9.1.4 Documentation of findings and remediation tracking.

9.2 External Audits

9.2.1 Annual external compliance reviews by certified auditors.
9.2.2 Third-party penetration testing conducted annually.
9.2.3 Regulatory compliance assessments as required.
9.2.4 Independent security assessments for critical systems.

9.3 Policy Enforcement

9.3.1 Regular monitoring of policy adherence across all departments.
9.3.2 Documentation of violations in personnel files.
9.3.3 Implementation of corrective actions within specified timeframes.

9.4 Non-compliance Consequences

9.4.1 Progressive disciplinary actions:
a) Formal written warnings for first violations
b) Mandatory additional security training
c) Performance improvement plans
d) Suspension for repeated violations
e) Termination for serious or repeated violations

9.5 Policy Review and Updates

9.5.1 Regular policy review conducted annually.
9.5.2 Updates implemented based on:
a) Regulatory changes
b) Threat landscape evolution
c) Business requirement changes
d) Audit findings and recommendations
9.5.3 All policy changes approved by executive management.
9.5.4 Staff notification and training on policy updates within 30 days.

10. Accountability and Governance

10.1 Collaborative Approach

10.1.1 This policy represents collaborative effort involving:
a) IT Department
b) Human Resources
c) Legal Department
d) Executive Management
e) Department Heads

10.2 Responsibility Matrix

10.2.1 Chief Information Security Officer: Overall policy oversight
10.2.2 IT Department: Technical implementation and monitoring
10.2.3 HR Department: Personnel security and training
10.2.4 Legal Department: Regulatory compliance
10.2.5 All Employees: Daily compliance and reporting

Document Control:

- Version: 2.0
- Last Updated: [Current Date]
- Next Review: [Annual Review Date]
- Approved by: Chief Information Security Officer, Nayaone Ltd.

Distribution:

- All employees (mandatory acknowledgment required)
- Board of Directors
- External auditors
- Regulatory authorities (as required)