next8n

SECURITY CHECKLIST

Workflow Automation Delivery Framework

ENTERPRISE EDITION

Version: 2.0

Date: December 28, 2025

Author: Mirza Iqbal

Contact: mirza.iqbal@next8n.com

Table of Contents

Table of Contents

Security Checklist

Complete Security Implementation Guide

Credential Security

Credential Ownership

Credential Setup

Credential Storage in n8n

Credential Rotation Plan

Webhook Security

HTTPS Enforcement

Authentication

Input Validation

Rate Limiting (If Applicable)

Data Protection

Data Minimization

Data in Transit

Data at Rest

Data Processing

AI-Specific Security

Prompt Security

Prompt Injection Prevention

Jailbreak Prevention

AI Output Safety

Access Control

n8n Access

Consultant Access

Multi-Factor Authentication

Compliance (If Applicable)

GDPR Checklist

Industry-Specific

Audit & Monitoring

Audit Logging

Security Monitoring

Incident Response

Pre-Deployment Security Review

Before Go-Live

Security Sign-Off

Post-Deployment Security

Ongoing Security

Offboarding Security

Quick Security Audit (5-Minute Check)

Security Checklist

Complete Security Implementation Guide

Credential Security

Credential Ownership

```
Client owns all API accounts
    OpenAI/Anthropic
    Google Workspace
    CRM (HubSpot, Salesforce, etc.)
    Other: _____________________________

Client pays for all API usage directly
No credentials billed through consultant
Credential ownership documented
```

Credential Setup

```
Secure transfer method used
    1Password shared vault
    Bitwarden send
    Other encrypted method: ______________
    NEVER: Email, Slack, text

One-time share links used (expire after use)
Credentials entered directly in n8n
No credentials stored in:
    Email
    Chat messages
    Plain text files
    Code/workflow JSON
    Sticky notes
    Documentation
```

Credential Storage in n8n

```
Credentials reference by name only
Raw values never visible in workflow
Credentials encrypted at rest (automatic)
Only decrypted at runtime (automatic)
Credential sharing restricted to necessary users
```

Credential Rotation Plan

```
Key rotation schedule documented
   Frequency: ____________________________
Process for rotating keys defined
Client knows how to rotate
No shared keys between environments
```

Webhook Security

HTTPS Enforcement

```
All webhooks use HTTPS
No HTTP webhooks in production
SSL certificate valid
TLS 1.2+ enforced
```

Authentication

```
Authentication method chosen:
    Header authentication
    Basic auth
    Query parameter token
    Signature verification

If signature verification:
    Secret configured
    Signature validation node added
    Invalid signatures rejected

If token authentication:
    Strong token generated
    Token stored securely
    Token never in URL (use header)
```

Input Validation

```
Payload structure validated
Required fields checked
Data types verified
Malformed requests rejected
Error messages don't leak info
```

Rate Limiting (If Applicable)

```
Rate limiting considered
Implementation method:
    n8n built-in (if available)
    External service (Cloudflare, etc.)
    Custom logic in workflow
Limits documented
```

Data Protection

Data Minimization

```
Only necessary data collected
Fields explicitly selected (not "select all")
Sensitive fields identified:
   Field: ____________ Handling: __________
   Field: ____________ Handling: __________
   Field: ____________ Handling: __________

Unnecessary data discarded
No data hoarding "just in case"
```

Data in Transit

```
TLS encryption for all connections
API calls use HTTPS
Webhooks use HTTPS
No sensitive data in URLs
```

Data at Rest

```
Execution logs reviewed
Sensitive data not logged
Log retention policy set
   Retention period: ____________________
Automatic log pruning enabled
```

Data Processing

```
Processing location understood
    n8n Cloud (EU/US)
    Self-hosted location: _______________
AI provider data policies reviewed
    OpenAI
    Anthropic
    Other: _____________________________
No training on client data (if applicable)
```

AI-Specific Security

Prompt Security

```
No secrets in prompts
    No API keys
    No passwords
    No internal URLs
    No sensitive business data

System prompts protected
Instructions not leakable
```

Prompt Injection Prevention

```
User input sanitized before AI
Clear separation of:
    System instructions
    User data
Output validated before use
Tested with adversarial inputs
```

Jailbreak Prevention

```
Guardrails in system prompt
Output filtering enabled
Sensitive topic handling defined
Tested with jailbreak attempts
```

AI Output Safety

```
Output validated before actions
Format checking implemented
Content filtering (if needed)
Fallback for invalid outputs
```

Access Control

n8n Access

```
Role-based access configured
   Owner: ________________________________
   Admins: _______________________________
   Editors: ______________________________
   Viewers: ______________________________

Principle of least privilege applied
Credential access restricted
No shared accounts
```

Consultant Access

```
Consultant has appropriate role (not owner)
Access scope limited to project needs
Access removal planned post-project
Access documented
```

Multi-Factor Authentication

```
MFA enabled for n8n access
MFA enabled for critical integrations
Recovery codes stored securely
```

Compliance (If Applicable)

GDPR Checklist

```
Lawful basis for processing identified
    Consent
    Contract
    Legitimate interest
    Legal obligation

Data Processing Agreement (DPA) in place
Data subject rights supported:
    Right to access
    Right to rectification
    Right to erasure
    Right to portability

Data minimization practiced
Processing purpose documented
Data retention policy defined
Breach notification process defined
```

Industry-Specific

```
HIPAA (healthcare): _____________________
PCI-DSS (payments): _____________________
SOC2 (service): ________________________
Other: _________________________________

Relevant controls documented
Compliance verified with client
```

Audit & Monitoring

Audit Logging

```
Execution history enabled
Who-did-what traceable
Logs not tamperable
Retention period set
```

Security Monitoring

```
Failed execution alerts
Unusual pattern detection
Error spike alerts
Unauthorized access attempts logged
```

Incident Response

```
Incident response plan exists
Contact list for incidents
   Primary: ______________________________
   Secondary: ____________________________
Escalation path defined
Communication templates ready
```

Pre-Deployment Security Review

Before Go-Live

```
All credentials are client-owned
No test credentials in production
Webhooks secured
Error handling doesn't leak data
Logging configured appropriately
Access control verified
All security items above addressed
```

Security Sign-Off

```
Security review completed
   Reviewed by: __________________________
   Date: _________________________________

Client informed of security measures
Any exceptions documented
Accepted risks documented
```

Post-Deployment Security

Ongoing Security

```
Regular security reviews scheduled
   Frequency: ____________________________
Credential rotation schedule
Access review schedule
Dependency updates monitored
```

Offboarding Security

```
Consultant access removed
Shared credentials rotated
Access audit performed
No orphaned permissions
```

Quick Security Audit (5-Minute Check)

```
All webhooks HTTPS?
Credentials encrypted (not in workflow)?
Error handling doesn't leak secrets?
Only necessary data collected?
Logs not storing sensitive data?
Access appropriately restricted?
AI prompts don't contain secrets?
```

If any answer is NO Address before go-live.

Next: See `04-qa-testing-checklist.md` for testing requirements.

Workflow Automation Delivery Framework | next8n | https://next8n.com

This document is confidential and intended for authorized use only.