Security Audit Checklist

Pre-Deployment Security Review for AI Workflows

Audit Information

Project Name:	
Audit Date:	
Auditor:	
Workflow Name:	

1. Credential Security

- ☐ All credentials encrypted at rest
- ☐ Credentials only accessible to authorized users
- ☐ No raw API keys/passwords in workflow nodes
- ☐ Credentials referenced by name only
- ☐ No sensitive data in plain text anywhere

Notes: _____

2. Webhook Security

- ☐ All webhooks use HTTPS
- ☐ Signature verification implemented (where applicable)
- ☐ No sensitive data in webhook URLs
- ☐ Rate limiting configured
- ☐ Authentication checks in place

Notes: _____

3. Data Privacy

- ☐ Data minimization applied (only necessary fields processed)
- ☐ Access to execution logs restricted
- ☐ Legal basis for data collection confirmed
- ☐ Data Processing Agreement in place (if required)
- ☐ Workflow supports data subject requests
- ☐ Execution pruning configured
- ☐ Data flow documented

Notes: _____

4. AI-Specific Security

- ☐ Prompt injection guardrails implemented
- ☐ Jailbreak protection in place
- ☐ System prompts not exposed in outputs
- ☐ Private information not leaked in AI responses
- ☐ Self-hosted AI models used (for privacy-sensitive data)

Notes: _____

5. Error Handling

- ☐ Error workflow configured
- ☐ Errors don't expose sensitive information
- ☐ Graceful timeout handling
- ☐ Error logging doesn't contain sensitive data

Notes: _____

6. Access Control

- ☐ Workflow access restricted to authorized users
- ☐ Execution history access limited
- ☐ Admin permissions properly assigned
- ☐ Test accounts removed from production

Notes: _____

Audit Summary

Total Items Checked: _____ / 28
Issues Found: _____
Critical Issues: _____

Approved for Deployment: ☐ Yes ☐ No ☐ Conditional

Auditor Signature: _____ Date: _____