===
=======

NEXABRIDGE SOLUTIONS INC.

OPERATIONS & COMPLIANCE POLICY MANUAL

Document ID: OPS-POL-2024-11

Version: 2.7

Last Updated: February 14, 2025

Owner: Office of the COO (Sandra Vega)

Classification: Tier 2 — Internal

===
=======

1. PURPOSE AND SCOPE

This document defines the operational standards, compliance procedures, and performance benchmarks that govern day-to-day activities across NexaBridge Solutions Inc. It applies to all full-time employees, part-time staff, contractors, and third-party vendors with access to NexaBridge systems or facilities.

Non-compliance with the policies described herein may result in disciplinary action, contract termination, or legal liability depending on severity.

Questions regarding this document should be directed to the Operations team:

Operations Help Desk: ops-support@nexabridge.com
Direct Policy Contact: Sandra Vega, COO
Compliance Hotline: +1 (512) 800-4400 (available 24/7, anonymous)

This manual is reviewed quarterly and updated as needed. All employees are notified of material changes via the internal communications platform (Slack #policy-updates channel) and must acknowledge updates within 10 business days.

2. COMPLIANCE FRAMEWORK

NexaBridge adheres to the following frameworks and standards. All operational procedures in this document are designed to be consistent with these frameworks.

2.1 Primary Frameworks

- NIST Cybersecurity Framework (CSF) v2.0

  Applied across all IT operations, incident response, and vendor management.

- ISO 27001:2022

  Governs information security management. Annual external audits required.
  Last certification date: September 2024. Next audit: September 2025.

- SOC 2 Type II

  Covers security, availability, and confidentiality trust service criteria.
  Audit period: January 1 – December 31 annually.
  Last report issued: February 2025 (clean opinion, zero exceptions noted).

2.2 Regulatory Compliance

- GDPR: All EU customer data is processed under signed Data Processing

Agreements (DPAs). Data residency for EU customers is enforced in the AWS eu-west-1 (Ireland) region.

- CCPA: California customer rights requests (access, deletion, opt-out) must be fulfilled within 45 days. Escalation to Legal required for contested requests.

- FedRAMP (In Progress): Moderate authorization boundary defined. Package under review by the JAB. Target authorization: Q3 2025.

2.3 Annual Compliance Calendar

Month	Activity
January	Internal SOC 2 readiness review
March	GDPR data mapping refresh
April	CCPA rights request audit
June	ISO 27001 internal audit
July	Bi-annual penetration test (external vendor)
September	ISO 27001 external audit
October	SOC 2 audit begins (external auditor: Arkin & Partners LLP)
November	FedRAMP continuous monitoring review
December	Annual policy acknowledgment cycle

3. OPERATIONAL PROCEDURES

3.1 Change Management

All production system changes must follow the Change Advisory Board (CAB) process:

a) Change Request (CR) submitted in Jira with 5-business-day lead time for standard changes; 48-hour lead for urgent changes.

b) CAB review occurs every Tuesday at 2:00 PM CT.

c) Emergency changes (P1 incidents) bypass CAB but require post-incident documentation within 24 hours.

d) Rollback plans are mandatory for all Tier 1 and Tier 2 system changes.

3.2 Incident Management

NexaBridge uses a four-tier severity model:

Severity	Definition	Response SLA	Escalation
P1	Full platform outage or data breach	15 min	CEO, CTO, COO, CISO
P2	Major feature degradation (>25%)	1 hour	CTO, Engineering VP
P3	Minor degradation, workaround avail	4 hours	Engineering lead
P4	Cosmetic or low-impact issue	2 business days	Assigned eng team

All incidents are tracked in PagerDuty. Post-mortems required for P1 and P2. Post-mortem must be completed within 5 business days of resolution.

3.3 Access Control

- All production system access requires MFA (TOTP or hardware key).
- Privileged access (admin/root) requires just-in-time (JIT) provisioning via CyberArk PAM. Sessions are limited to 4 hours and fully logged.
- Quarterly access reviews are conducted for all Tier 3 and Tier 4 systems.
- Terminated employees must have all access revoked within 1 hour of HR notification.

3.4 Data Backup and Recovery

- Production databases: automated daily snapshots, 30-day retention.
- Critical configuration files: backed up hourly, 7-day retention.
- Recovery Time Objective (RTO): 4 hours (Tier 1 systems)
- Recovery Point Objective (RPO): 1 hour (Tier 1 systems)
- DR failover is tested bi-annually (last test: November 2024 — passed).

3.5 Vendor Onboarding

- Vendors with access to NexaBridge systems must complete a security questionnaire (CAIQ v3.1 format) before contract execution.
- Contracts exceeding $50,000 require legal review and CISO sign-off.
- All vendors must carry cyber liability insurance of at least $2 million.
- Annual vendor security reviews are required for active contracts exceeding $100,000.

4. KEY PERFORMANCE INDICATORS (KPIs)

The following KPIs are tracked monthly by the COO and reviewed in the

Executive Leadership Team (ELT) meeting on the first Monday of each month.

4.1 Platform Performance KPIs

KPI	Target	FY2024 Actual	Notes
API Uptime SLA	99.97%	99.96%	1 P1 incident in Aug 2024
Avg API Response Time	< 200ms	147ms	Measured at p95
Data Ingestion Success Rate	> 99.5%	99.71%	Excludes partner outages
Support Ticket Resolution	< 4 hours	4.2 hours	Slight miss; plan in Q2
Deployment Frequency	>= 2/week	2.4/week	CI/CD via GitHub Actions
Change Failure Rate	< 5%	3.1%	Industry avg is ~7%
MTTR (Mean Time to Recover)	< 2 hours	1.6 hours	P1/P2 incidents only

4.2 Security KPIs

KPI	Target	FY2024 Actual	Notes
Patch Compliance (critical)	100% / 48h	98.7%	2 servers missed window
Phishing Simulation Click	< 5%	6.1%	Training refreshed Q4
MFA Enrollment	100%	99.4%	7 contractors pending
Pen Test Critical Findings	0	0	External audit Jul 2024
Access Review Completion	100%	97.8%	Q3 had 2 late reviewers

4.3 Business Operations KPIs

KPI	Target	FY2024 Actual	Notes
Employee NPS (eNPS)	> 40	47	Exceeds target
Voluntary Attrition	< 12%	9.3%	Strong retention
Time-to-Hire (engineering)	< 45 days	52 days	Tight market in AI/ML
Training Completion	100%	94.2%	Mandatory compliance trng
Budget Variance	+/- 5%	+3.1%	Slight overspend in R&D

5. COMMUNICATION AND ESCALATION PROTOCOLS

5.1 Internal Communications

- Standard business communication: Slack (primary), Email (formal/external)
- Critical operational alerts: PagerDuty → Slack #incidents channel
- All-hands meetings: Monthly, first Thursday at 11:00 AM CT
- ELT meetings: Weekly, Mondays at 9:00 AM CT

5.2 External Communications

- Customer-facing incident notifications must be sent within 30 minutes of P1 declaration via the StatusPage (status.nexabridge.com).
- Press/media inquiries must be routed to: pr@nexabridge.com
- Regulatory notifications (e.g., GDPR breach): Legal must be notified immediately; 72-hour regulatory reporting window under GDPR applies.

5.3 Escalation Contacts (Internal Distribution Only)

Role	Internal Email	Extension
COO (Sandra Vega)	s.vega@nexabridge-internal.com	x4801
CISO	ciso@nexabridge-internal.com	x4810
Legal Counsel	legal@nexabridge-internal.com	x4820
HR Director	hr-director@nexabridge-internal.com	x4830

IMPORTANT: These contacts are for internal escalation only.
External parties must use: support@nexabridge.com or +1 (800) 639-2200.

6. TRAINING AND AWARENESS

All employees must complete the following training annually:

Training Module	Frequency	Completion Deadline
Security Awareness Fundamentals	Annual	January 31
GDPR & Data Privacy	Annual	February 28
Acceptable Use Policy Acknowledgment	Annual	January 31
Incident Response Tabletop (ELT)	Semi-annual	June 30, December 31
Phishing Simulation	Quarterly	End of each quarter
Role-specific Compliance Training	Annual	March 31

Employees who fail to complete mandatory training by the deadline will have system access suspended until completion. Repeat offenders will be escalated to HR for formal performance review.

7. DOCUMENT CONTROL

Owner: Office of the COO

Approved by: Sandra Vega (COO), Dr. Evan Strauss (CTO)

Review Cycle: Quarterly

Next Review Date: May 2025

Document History:

Version	Date	Author	Changes
1.0	Jan 2020	S. Vega	Initial release
2.0	Mar 2022	S. Vega	Added FedRAMP section
2.5	Sep 2023	Compliance Team	NIST CSF v2.0 alignment
2.6	Oct 2024	Compliance Team	SOC 2 scope update
2.7	Feb 2025	S. Vega	KPI table update, DR test results

==

END OF DOCUMENT

NexaBridge Solutions Inc. | Internal Use Only | Classification: Tier 2

For questions contact: ops-support@nexabridge.com | +1 (512) 800-4400

==