GOVERNANCE DOCUMENT

Information Security Policy

Nexa Systems Inc.

CONFIDENTIAL — INTERNAL USE ONLY

Document ID	NEXA-ISP-001
Version	3.2
Owner	Chief Information Security Officer (Elena Kowalski)
Classification	Confidential — Internal Use Only
Effective Date	15 January 2026
Last Reviewed	01 July 2026
Next Review	01 July 2027
Approved By	Board Risk & Audit Committee

This document defines mandatory information security requirements for Nexa Systems Inc. It is distributed to all employees, contractors, and vendors with system access, and supersedes all prior versions of the Information Security Policy.

1 Purpose and Scope

1.1 Purpose

This Information Security Policy (the "Policy") establishes Nexa Systems Inc.'s ("Nexa", "the Company") requirements for protecting the confidentiality, integrity, and availability of information assets. It defines the minimum controls that all business units, subsidiaries, and contracted third parties must implement, and it assigns accountability for maintaining those controls over time.

The Policy is issued under the authority of the Chief Information Security Officer (CISO) and is approved by the Executive Leadership Team. It is reviewed at least annually, or sooner if a material change in the threat environment, regulatory landscape, or business structure warrants it.

1.2 Scope

This Policy applies to:

- All employees, contractors, interns, and temporary staff engaged by Nexa;
- All information assets owned, leased, or processed by Nexa, including production systems, corporate endpoints, cloud infrastructure, and physical facilities;
- Third-party vendors and service providers with access to Nexa systems or data under a signed data processing or service agreement;
- All Nexa-branded products and the customer data they process, regardless of the hosting region.

Personal devices used solely for email and calendar access under the Bring-Your-Own-Device programme are in scope for the access-control and acceptable-use clauses of this Policy, but out of scope for the endpoint-management clauses, which apply only to Nexa-issued hardware.

1.3 Policy Owner

The CISO owns this Policy and is accountable to the Board Risk & Audit Committee for its currency, completeness, and enforcement. Day-to-day custodianship of individual control domains is delegated per the responsibility matrix in Clause 3.

2 Governance Principles and Policy Statement

2.1 Information Security Principles

Nexa's security programme is built on five principles that govern how controls are designed, and that take precedence when a control decision is ambiguous:

P1. Confidentiality, integrity, and availability are equal priorities. No control decision may improve one at the unconsidered expense of another.

P2. Least privilege by default. Access is granted only to the extent required to perform an assigned role, and is time-bound where the role is temporary.

P3. Defense in depth. No single control is assumed sufficient; overlapping preventive, detective, and corrective controls are required for critical assets.

P4. Risk-based prioritisation. Control investment follows the risk register, not the loudest incident; residual risk is accepted only by an accountable owner.

P5. Security is everyone's responsibility. Technical controls are necessary but not sufficient — every employee is a control point.

2.2 Policy Statement

> **Statement of commitment.** Nexa Systems Inc. is committed to protecting the information entrusted to it by customers, employees, and partners. We will maintain an information security management system aligned to recognised industry frameworks, allocate the resources necessary to operate it effectively, and hold every level of the organisation accountable for the controls assigned to them in this Policy.
>
> — *Grace Whitfield, Chief Executive Officer*

2.3 Relationship to Other Documents

This Policy is the top-level governance document for information security. It is supported by subordinate standards and procedures — including the Access Control Standard, the Incident Response Runbook, and the Vendor Risk Assessment Procedure — which provide implementation detail. Where a subordinate document conflicts with this Policy, this Policy prevails until the conflict is formally resolved by the CISO.

3 Roles and Responsibilities

3.1 Governance Structure

Accountability for information security runs from the Board Risk & Audit Committee, through the CISO, to line management and, ultimately, to every individual with access to Nexa systems. The CISO chairs a monthly Security Steering Committee comprising IT Operations, Data Protection, HR, and a rotating departmental representative, which reviews open risks, exception requests, and control metrics.

3.2 Responsibility Matrix

Table 1 defines who is Responsible, Accountable, Consulted, or Informed (RACI) for the core recurring security activities governed by this Policy.

Activity	CISO	IT Ops	Dept. Mgrs	All Staff	Int. Audit
Enterprise risk assessment	A	R	C	—	C
Access provisioning & deprovisioning	A	R	R	I	I
Security incident response	A	R	I	I	I
Security awareness training	A	C	R	R	I
Policy exception approval	A	C	C	—	I
Vendor security due diligence	A	R	C	—	C
Business continuity testing	A	R	C	I	C

Table 1: Responsibility matrix for recurring security activities.

R Responsible A Accountable C Consulted I Informed — Not applicable

3.3 Named Accountabilities

- **Elena Kowalski, Chief Information Security Officer** — overall policy ownership, risk acceptance above the Dept. Manager threshold, Board reporting.
- **Marcus Webb, Director of IT Operations** — identity and access management, endpoint management, network and cloud infrastructure controls.
- **David Chen, Data Protection Officer** — data classification, privacy impact assessments, regulatory notification decisions.
- **Priya Nair, Head of Internal Audit** — independent control testing, evidence sampling, findings tracking to closure.
- **Sofia Alvarez, Director of People** — background screening, onboarding and offboarding coordination, disciplinary process for policy violations.

4 Control Objectives

4.1 Framework Alignment

Nexa's control set is mapped to the Annex A controls of ISO/IEC 27001:2022 [4] and cross-referenced against the NIST Cybersecurity Framework 2.0 [6] and NIST SP 800-53 Rev. 5 [3] for customers requiring a US-federal control lineage. Contractual obligations under PCI DSS v4.0 [5] and the SOC 2 Trust Services Criteria [2] are satisfied as a subset of the objectives below; no separate control set is maintained for either.

4.2 Control Objectives Table

Table 2 states the objective for each control domain, the primary control that satisfies it, its Annex A reference, and the accountable owner.

Domain	Control Objective	Ref.	Owner
Access Control	Restrict logical access to systems and data to authorised, authenticated users operating under least privilege.	A.8.2–A.8.3	IT Operations
Cryptography	Protect data at rest and in transit using approved algorithms and managed key lifecycles.	A.8.24	IT Operations
Physical Security	Prevent unauthorised physical access to facilities and equipment hosting Nexa information assets.	A.7.1–A.7.14	Facilities
Operations Security	Ensure change management, capacity management, and malware defenses operate consistently across production environments.	A.8.16, A.8.19	IT Operations
Communications Security	Protect information in networks and enforce segmentation between trust zones.	A.8.20–A.8.23	IT Operations
Supplier Relationships	Assess and monitor the security posture of vendors and subprocessors before and during engagement.	A.5.19–A.5.23	Procurement / CISO
Incident Management	Detect, triage, and respond to security incidents within defined timeframes, with lessons captured and closed out.	A.5.24–A.5.28	CISO
Business Continuity	Maintain and test the capability to resume critical services within agreed recovery objectives.	A.5.29–A.5.30	IT Operations
Compliance	Monitor adherence to legal, regulatory, and contractual security obligations.	A.5.31–A.5.37	Internal Audit

Table 2: Control objectives mapped to ISO/IEC 27001:2022 Annex A.

Control exceptions

A control objective in this table may be met by a compensating control where the primary control is not technically feasible, provided the compensating control is documented, risk-assessed, and approved per the exception process in Clause 7.3.

5 Acceptable Use and Access Control

5.1 Acceptable Use of Assets

Nexa-issued accounts, devices, and network access are provided for business purposes. Incidental personal use is permitted where it does not incur cost, consume material resources, violate law, or create reputational risk to Nexa. Employees must not:

- Share credentials or authentication factors with another individual, including colleagues, under any circumstance;
- Install software from outside the approved catalogue on managed endpoints;
- Copy production customer data to unmanaged storage, personal cloud drives, or removable media;
- Disable, bypass, or attempt to circumvent an endpoint security control.

5.2 Access Control Requirements

1. All access to production systems requires multi-factor authentication; password-only access is disabled fleet-wide.
2. Access requests are approved by the requester's manager and provisioned by IT Operations against a documented role, per Table 1.
3. Access to production customer data requires an additional approval from the Data Protection Officer and is logged for audit.
4. Departmental access reviews occur quarterly; any account unused for 90 consecutive days is disabled pending manager confirmation.
5. All access is revoked within one business day of an employee's last working day, coordinated between People and IT Operations.

5.3 Data Classification

Every information asset is classified at creation and handled according to Table 3.

6 Incident Management

6.1 Reporting Obligation

Every employee and contractor must report a suspected security incident — a phishing email acted upon, a lost device, unexpected system behaviour, or unauthorised data access — to the security team (`security@nexasystems.example`) or the 24-hour hotline within one hour of discovery. Late reporting is treated as a policy matter in its own right, independent of the underlying incident.

Classification	Definition	Handling Requirement
Public	Approved for external release without restriction.	No special handling; standard version control.
Internal	Business information not intended for external release.	Access limited to employees and authorised contractors.
Confidential	Information whose disclosure would cause material harm — financial models, unreleased product plans, employee records.	Encryption at rest, access on a need-to-know basis, audit logging.
Restricted	Customer data, authentication secrets, and information subject to regulatory protection.	Encryption at rest and in transit, MFA-gated access, DPO approval, quarterly access recertification.

Table 3: Data classification levels and required handling.

6.2 Severity and Response Time

Incidents are triaged by the on-call security engineer against the definitions in Table 4 within 15 minutes of receipt.

Severity	Definition	Response Time
Sev-1 Critical	Confirmed breach of customer data, or a production outage caused by a security event.	1 hour, CISO paged
Sev-2 High	Active compromise of an internal system with no confirmed data exposure.	4 hours
Sev-3 Medium	Isolated policy violation or contained malware detection on a single endpoint.	1 business day
Sev-4 Low	Suspicious activity that does not indicate compromise, e.g. a reported phishing attempt with no interaction.	5 business days

Table 4: Incident severity classification and required response time.

6.3 Escalation Procedure

Sev-1 and Sev-2 incidents trigger the Incident Response Runbook: the on-call engineer declares the incident, the CISO assumes incident commander duties, and a bridge is opened within the response-time window. The Data Protection Officer determines within 72 hours of confirmation whether a regulatory notification obligation exists under GDPR [1] or an equivalent regime, consistent with the escalation contacts held by Internal Audit for Board notification. Every Sev-1 and Sev-2 incident closes with a blameless post-incident review, and resulting action items are tracked to closure by the control owner named in Table 2.

7 Compliance, Enforcement, and Review

7.1 Compliance Monitoring

Internal Audit performs a full control walkthrough against Table 2 twice yearly, and an external assessor performs an annual SOC 2 Type II examination [2]. Findings are logged in the risk register with a remediation owner and a target date; any finding open past its target date is escalated to the Security Steering Committee.

7.2 Enforcement and Sanctions

Violation of this Policy is addressed through the standard disciplinary process managed by the Director of People. Consequences scale with severity and intent, from a documented coaching conversation for a first inadvertent violation up to termination of employment or contract for deliberate or repeated violations, particularly those involving unauthorised access to customer data. Contracted vendors found in violation of their data processing agreement are subject to remediation timelines defined in that agreement, up to

termination of the contract.

7.3 Exceptions Process

Any deviation from a control objective in this Policy requires a written exception request describing the business justification, the compensating control, and an expiry date not exceeding twelve months. Requests are reviewed by the CISO and, for exceptions touching customer data, co-approved by the Data Protection Officer. Approved exceptions are logged in the exception register and re-assessed at expiry; there is no mechanism for a standing, indefinite exception.

7.4 Review Cycle and Revision History

This Policy is reviewed annually by the CISO and upon any material change to Nexa's infrastructure, regulatory obligations, or risk profile. The current version is **v3.2**, effective **15 January 2026**, last reviewed **01 July 2026**, with the next scheduled review due **01 July 2027**.

Version	Date	Author	Summary of Changes
1.0	01 Mar 2023	E. Kowalski	Initial Policy issued at Board request.
2.0	15 Jun 2024	E. Kowalski	Added vendor due-diligence clause; introduced RACI matrix.
3.0	01 Aug 2025	E. Kowalski	Re-mapped control set to ISO/IEC 27001:2022 Annex A structure.
3.1	15 Jan 2026	D. Chen	Tightened data classification handling requirements for Restricted data.
3.2	01 Jul 2026	E. Kowalski	Added incident severity table; clarified exception expiry limit.

Table 5: Policy revision history.

Approved by the Board Risk & Audit Committee • Distribution: all employees, contracted vendors on request

References

[1] Regulation (eu) 2016/679 (general data protection regulation). Official Journal of the European Union, 2016.

[2] SOC 2 trust services criteria. Technical report, American Institute of Certified Public Accountants (AICPA), 2017.

[3] NIST SP 800-53 Rev. 5 security and privacy controls for information systems and organizations. Technical report, National Institute of Standards and Technology, 2020.

[4] ISO/IEC 27001:2022 information security, cybersecurity and privacy protection — information security management systems — requirements. Technical report, International Organization for Standardization, 2022.

[5] Payment Card Industry Data Security Standard (PCI DSS) v4.0. Technical report, PCI Security Standards Council, 2022.

[6] NIST Cybersecurity Framework (CSF) 2.0. Technical report, National Institute of Standards and Technology, 2024.