NEC XON HOLDINGS (Pty) Ltd and its subsidiaries ("NEC XON")

NEC XON Information Security and Privacy Policy

File name	Information Security and Privacy Policy
File reference	IS_POL_000300
Last change	February 2025
Author of the last change	Durandt Eksteen
Contact	Durandt.Eksteen@nec.xon.co.za
Confidentiality Level	Internal Use
Status	Finalised
Version	5.0

INFORMATION SECURITY AND PRIVACY POLICY

INLINE WITH ISO 27001, 27032, 27701, SOC2 & NIST CSF

Document Details

		Signatures
Title	Information Security and Privacy Policy v5.0	
Version	5.0	
Classification	Internal Use	
Release Date	14 February 2025	
Description	This Information Security and Privacy Policy establishes the framework for protecting NEC XON Holdings Group and its subsidiaries ("NEC XON")'s information assets.	
Review Date	14 February 2026	
Approved By	Chief Executive Officer	JC Conradie (Feb 18, 2025 11:42 GMT+2)
Reviewed By	Chief Information Officer	Durandt Eksteen
Reviewed By	Chief Operating Officer	Barry Vd Buynder (Feb 18, 2025 10:22 GMT+2)
Reviewed By	Group Head: Sustainability, QHS & Lead ISO Auditor	
Owner	Information Security Officer	Jitesh Ramduth Jitesh Ramduth (Feb 15, 2025 20:22 GMT+2)

Distribution List

Name
Public

1. Purpose

This Information Security and Privacy Policy establishes the framework for protecting NEC XON Holdings Group and its subsidiaries ("NEC XON")'s information assets. It demonstrates management's commitment to implementing, maintaining, and continuously improving information security and privacy within NEC XON. This policy serves as the cornerstone document that defines NEC XON's approach to information security and privacy management and provides the basis for all subsequent information security and privacy procedures and standards.

2. Scope

This policy applies to all information assets owned, operated, or managed by NEC XON, regardless of location or format. This includes all employees, contractors, consultants, temporary staff, and third-party entities who have access to, or responsibility for, NEC XON's information assets. The policy encompasses all information systems, applications, infrastructure, business processes, and physical facilities involved in the processing, storage, and transmission of information, as well as privacy considerations.

3. Information Security and Privacy Policy Statements

3.1 Information Security and Privacy Management System (ISPMS)

NEC XON shall establish, implement, maintain, and continually improve upon an Information Security and Privacy Management System in accordance with ISO/IEC 27001:2022, ISO 27032:2023 and ISO 27701:2019. The ISPMS shall encompass all business functions, locations, and information assets within the defined scope. Management shall demonstrate leadership and commitment by ensuring the integration of information security requirements into the organization's business processes, providing necessary resources, and promoting continuous improvement. The effectiveness of the ISPMS shall be measured through defined metrics, reviewed at planned intervals, and reported to senior management at least quarterly. All employees and relevant external parties shall be made aware of their role in maintaining the effectiveness of the ISPMS through regular communication and training programs.

3.2 Risk Management

NEC XON shall implement and maintain a comprehensive risk management framework that identifies, assesses, and treats information security and privacy risks in alignment with business objectives and stakeholder requirements. Risk assessments shall be conducted at planned intervals, at least bi-monthly, and whenever significant changes to the business environment, technology infrastructure, or threat landscape occur. The risk assessment methodology shall consider both threats and vulnerabilities, evaluate potential impacts to confidentiality, integrity, and availability of information, and document the rationale for risk treatment decisions. Risk treatment plans shall be developed and implemented based on NEC XON's defined risk acceptance criteria, with regular monitoring and reporting of risk treatment effectiveness to relevant stakeholders.

3.3 Access Control Management

NEC XON shall implement and maintain a comprehensive access control framework based on the principles of least privilege and need-to- know. All access to information systems and data shall be controlled through formal user registration and de-registration procedures. Access rights shall be granted only after documented approval from both the resource owner and the information security team. Multi-factor authentication (MFA) shall be mandatory for all remote access and

privileged account access. Regular access reviews shall be conducted at least quarterly, with immediate revocation of access rights upon termination or role change. The organisation shall maintain audit logs of all access control changes, with automated alerts for suspicious access attempts or unauthorised privilege escalations. Password policies shall enforce strong authentication requirements including minimum length, complexity, with technical controls preventing password reuse.

3.4 Asset Management and Classification

NEC XON shall maintain a comprehensive inventory of all information assets, including both physical and logical assets, with clearly assigned ownership and defined security responsibilities. All information assets shall be classified according to their sensitivity, criticality, and legal requirements using NEC XON's defined classification scheme. Asset owners shall be responsible for ensuring appropriate handling procedures are implemented based on the asset's classification level. The asset inventory shall be reviewed and updated at least quarterly, with formal reconciliation processes to identify and address any discrepancies. Media handling procedures shall be implemented to protect against unauthorised disclosure, modification, or destruction throughout the asset lifecycle, including secure storage, transmission, and disposal methods.

3.5 Cryptography and Key Management

NEC XON shall implement and maintain cryptographic controls to protect the confidentiality, integrity, and authenticity (as well as privacy) of information throughout its lifecycle. All sensitive data shall be encrypted both in transit and at rest using industry-standard encryption algorithms and protocols. NEC XON shall maintain a formal key management policy covering the entire cryptographic key lifecycle, including generation, distribution, storage, use, archival, and destruction. Cryptographic keys shall be protected against unauthorised access, loss, and compromise through the use of hardware security modules (HSMs) or equivalent secure key storage mechanisms. Regular assessments of cryptographic implementations shall be conducted to ensure alignment with current industry standards and best practices, with documented procedures for transitioning to stronger cryptographic controls when required.

3.6 Physical and Environmental Security

NEC XON shall implement and maintain appropriate physical and environmental security controls to prevent unauthorised physical access, damage, theft, compromise, or interference to information assets and information processing facilities. Security perimeters shall be clearly defined and protected through layered security controls including (as an example) access card systems, surveillance cameras, and security personnel where appropriate. All physical access shall be logged and monitored, with regular reviews of access logs and immediate investigation of security and privacy incidents. Environmental controls shall be implemented to protect against environmental threats such as fire, flood, or power failure, with regular testing and maintenance of all environmental protection systems. Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel can gain access, with additional controls for areas containing sensitive information or critical systems.

3.7 Operations Security

NEC XON shall establish and maintain documented operating procedures for all information processing facilities to ensure correct and secure operations. Change management procedures shall be implemented to control all changes to information processing facilities and systems, with appropriate testing, documentation, and approval requirements. Development, testing, and operational environments (as an example) shall be separated to reduce the risks of unauthorised access or changes to operational systems. System and security monitoring controls shall be implemented to detect unauthorised information processing activities, with regular review and analysis of system logs. Protection against malware shall be implemented through a defense-in-depth approach including endpoint protection, email filtering, web filtering, and regular security awareness training for all users.

3.8 Communications Security

NEC XON shall implement and maintain controls to ensure the security of information in networks and its supporting information processing facilities. Network security controls shall include network segregation, encryption of sensitive traffic, regular vulnerability assessments, and intrusion detection/prevention systems. All external network connections shall be identified, documented, and secured through formal agreements that include specific security requirements. Information transfer policies and procedures shall be established to protect the transfer of information through the use of all types of communication facilities, including requirements for encryption, digital signatures, and non-repudiation where appropriate.

3.9 Supplier Relationships

NEC XON shall establish and maintain information security and privacy requirements for relationships with suppliers to mitigate risks associated with supplier access to organisational assets. Formal contracts or agreements shall include specific security and privacy requirements, including incident reporting obligations, data protection requirements, and right-to-audit clauses. Supplier service delivery shall be regularly monitored and reviewed, with formal assessments of security and privacy controls implemented by suppliers conducted at least annually. Changes to supplier services shall be managed through formal change management procedures, with impact assessments conducted for significant changes.

3.10 Information Security and Privacy Incident Management

NEC XON shall implement and maintain an information security and privacy incident management process to ensure a consistent and effective approach to the management of information security and privacy incidents. All employees and contractors shall be required to report any observed or suspected security incidents immediately through defined reporting channels. The incident response team (CSIRT) shall be properly trained and equipped to handle various types of security incidents, with defined procedures for incident detection, reporting, assessment, response, and recovery. Lessons learned from security and privacy related incidents shall be documented and used to improve security and privacy controls and incident and privacy response procedures. Regular testing of incident response procedures shall be conducted through tabletop exercises and simulated incidents.

3.11 Threat Intelligence

NEC XON shall establish and maintain a Threat Intelligence Program to proactively identify, analyse, and respond to evolving security and privacy related threats. Threat intelligence shall be gathered from internal logs, commercial and open-source threat feeds, industry partnerships, and government agencies. This intelligence will be analysed using established frameworks (e.g., MITRE ATT&CK) and integrated into incident response, vulnerability management, and security and privacy awareness programs. NEC XON shall ensure secure sharing of intelligence internally

and externally, in compliance with ISO 27001, ISO 27032, ISO 27701, and relevant data protection laws (e.g., GDPR, POPIA). Designated teams, including security analysts and SOC personnel, will oversee intelligence collection, validation, and response. Threat intelligence processes shall be continuously improved through regular reviews, testing, and updates to security and privacy controls.

3.12 Business Continuity Management

NEC XON shall develop, maintain, and regularly test business continuity plans to ensure the continued availability of critical information processing facilities. Business impact analyses shall be conducted to identify critical business functions and their dependencies on information systems. Recovery time objectives (RTOs) and recovery point objectives (RPOs) shall be defined for all critical systems and processes. Regular backup procedures shall be implemented with periodic testing of backup restoration. Alternative processing facilities shall be identified and maintained to support business continuity requirements, with regular testing of failover procedures.

Section 4: Roles and Responsibilities

4.1 Board of Directors

The Board of Directors shall provide strategic oversight of NEC XON's information security and privacy program, and demonstrate organisational commitment to information security and privacy, as well as its successful implementation and operations.

4.2 Executive Management

Executive Management, including the CEO and executive leadership team, shall be responsible for:

- Establishing and maintaining a strong security and privacy culture throughout NEC XON
- Approving information security and privacy strategies, policies, and major initiatives
- Ensuring information security and privacy requirements are integrated into NEC XON's processes
- Allocating sufficient resources (financial, human, and technical) to maintain effective security and privacy controls
- Reviewing security and privacy performance metrics and risk indicators quarterly
- Supporting cross-functional coordination for security and privacy initiatives
- Ensuring security and privacy considerations are included in business planning and decision-making
- Annual review and approval of the Information Security and Privacy Policy and significant security initiatives
- Oversight of significant security and privacy risks and incidents through regular reporting
- Review of annual security and privacy program effectiveness metrics and assessments

- Approval of NEC XON's risk appetite and tolerance levels related to information security and privacy

4.3 Chief Information Security Officer (CISO) / Chief Information Officer (CIO)

The CISO and CIO shall have direct operational responsibility for the information security and privacy program and shall:

- Develop and maintain NEC XON's information security and privacy strategy and policies
- Oversee the implementation and operation of security and privacy controls across NEC XON
- Report security status, risks, and significant issues to executive management
- Manage the information security and privacy team and security and privacy operations
- Ensure compliance with security and privacy requirements and standards
- Coordinate security and privacy incident response activities
- Maintain relationships with external security and privacy partners and stakeholders
- Lead security and privacy awareness and training programs
- Provide security and privacy expertise and guidance to business units and departments
- Review and approve security architecture and designs

4.4 Information Security and Privacy Team

The Information Security and Privacy Team, under the direction of the CISO and CIO, shall:

- Implement and maintain security and privacy controls according to approved policies
- Monitor security and privacy events and respond to security and privacy incidents
- Conduct security and privacy assessments, audits, and testing
- Provide security and privacy consulting to business units and departments
- Manage security and privacy tools and technologies
- Develop security and privacy procedures and guidelines
- Deliver security and privacy awareness training
- Perform security and privacy risk assessments
- Support compliance activities and audits
- Investigate security and privacy incidents and violations

4.5 Department Managers and Business Unit Heads

Department Managers and Business Unit Heads shall be responsible for:

- Implementing security and privacy controls within their areas of responsibility
- Ensuring staff compliance with security and privacy policies and procedures
- Identifying and communicating security and privacy requirements for business processes
- Supporting security and privacy risk assessments and audits
- Reporting security and privacy incidents promptly
- Maintaining asset inventory for their department / Business Unit
- Reviewing access rights for their staff regularly
- Incorporating security and privacy requirements into project planning
- Supporting security and privacy awareness within their teams
- Ensuring security and privacy considerations in vendor relationships

4.6 System and Data Owners

System and Data Owners shall be accountable for:

- Defining classification levels for their information and privacy assets
- Approving access to systems and data under their ownership
- Reviewing access rights periodically
- Ensuring appropriate security and privacy controls are implemented
- Participating in risk assessments and security and privacy reviews
- Defining backup and recovery requirements
- Approving system changes that affect security and privacy
- Supporting security and privacy incident investigations
- Maintaining documentation of system security and privacy requirements
- Ensuring compliance with security and privacy policies for their assets

4.7 All Employees, Contractors, and Third Parties

All individuals who have access to organisational information assets shall:

- Comply with all information security and privacy policies and procedures
- Complete required security and privacy awareness training
- Protect information assets under their control
- Report security and privacy incidents and violations promptly
- Use information assets only for authorised purposes
- Maintain confidentiality of sensitive information
- Follow secure working practices
- Protect authentication credentials
- Ensure physical security of assets
- Support security and privacy assessments and audits, as required

Section 5: Compliance and Enforcement

5.1 Compliance Requirements

5.1.1 Policy Compliance

All employees, contractors, and third parties shall comply with this Information Security and Privacy Policy and all supporting policies, procedures, and standards. Compliance shall be monitored through:

- Regular security and privacy assessments and audits
- Automated compliance monitoring tools
- Security and privacy metrics and reporting
- Access reviews and activity logs
- Security and privacy awareness assessments
- Vendor security and privacy assessments
- Compliance validation processes

5.1.2 Regulatory Compliance

NEC XON shall maintain compliance with all applicable laws, regulations, and contractual obligations related to information security and privacy, including but not limited to:

- Industry-specific regulations
- Data protection and privacy laws
- Security breach notification requirements
- Electronic transaction regulations
- Records retention requirements
- Export control regulations
- Intellectual property protection

5.1.3 Compliance Monitoring

The Information Security and Privacy Team shall implement and maintain processes to monitor compliance with security and privacy requirements through:

- Automated security and privacy configuration monitoring
- Regular vulnerability assessments
- Security and privacy control testing
- Log monitoring and analysis
- Access control reviews
- Security and privacy metrics collection
- Compliance assessments
- Third-party security and privacy reviews

5.1.4 Audit Requirements

Internal and external security and privacy audits shall be conducted regularly to verify compliance with this policy and supporting requirements:

- Internal security and privacy audits shall be conducted at least annually
- External security and privacy audits shall be conducted annually
- Specialised audits shall be conducted as required by regulations
- Audit findings shall be tracked to resolution
- Audit reports shall be provided to appropriate management
- Remediation plans shall be developed for identified gaps

5.2 Policy Enforcement

5.2.1 Violations

Security and Privacy Policy violations shall be handled according to established procedures:

- All suspected violations shall be investigated promptly
- Investigations shall be conducted by authorised personnel
- Evidence shall be collected and preserved appropriately
- Confidentiality shall be maintained during investigations
- Results shall be documented and reported to management
- Appropriate corrective actions shall be implemented
- Forensic investigation capability is to be implemented to bolster non-repudiation

5.2.2 Disciplinary Actions

Violations of this policy may result in disciplinary action up to and including termination of employment or contract:

- Disciplinary actions shall be determined based on:
  - Severity of the violation
  - Intent of the violator
  - Impact on the organisation
  - History of previous violations
  - Cooperation with investigation
  - Risk of reoccurrence

- Disciplinary actions shall be:
  - Consistently applied
  - Properly documented
  - Reviewed by appropriate parties
  - Communicated as appropriate
  - Implemented promptly

5.2.3 Appeals Process

Individuals subject to disciplinary action shall have the right to appeal:

- Appeals must be submitted in writing within 3 business days
- Appeals shall be reviewed by designated authorities
- Additional information may be requested during review
- Appeal decisions shall be documented and communicated
- Appeal decisions shall be final

5.2.4 Legal Actions

The organisation reserves the right to pursue legal action for policy violations that:

- Result in significant harm or loss
- Violate applicable laws or regulations
- Breach contractual obligations
- Involve criminal activities
- Require regulatory reporting

5.3 Compliance Reporting

5.3.1 Internal Reporting

Regular compliance reporting shall be provided to management:

- Monthly security metrics and compliance indicators
- Quarterly compliance status reports to executive management
- Annual compliance assessment reports to the Board

- Ad-hoc reporting of significant compliance issues
- Trend analysis and recommendations

5.3.2 External Reporting

External compliance reporting shall be provided as required:

- Regulatory compliance reports
- Customer compliance attestations
- Audit reports for external parties
- Security and privacy incident notifications
- Breach reporting as required by law

5.3.3 Compliance Documentation

All compliance activities shall be documented and retained:

- Assessment and audit reports
- Compliance monitoring results
- Investigation records
- Disciplinary action records
- Remediation plans and status
- Training and awareness records

Section 6: Exceptions and Deviations

6.1 Exception Request Process

NEC XON recognises that legitimate business needs may occasionally require exceptions to this policy. All exceptions shall be managed through a formal process:

6.1.1 Exception Request Requirements

Exception requests must include:

- Detailed description of the requested exception

- Business justification and impact analysis
- Risk assessment and proposed compensating controls
- Implementation timeline and duration
- Technical specifications if applicable
- Cost-benefit analysis
- System and data owners' approval

6.1.2 Exception Review and Approval

All exception requests shall follow a structured review and approval process:

- Initial review by Chief Information Security Officer, Chief Information Officer and Executive Committee
- Risk assessment validation
- Technical review if required
- Approval by appropriate authority based on risk level:
  - Low risk: CISO approval
  - Medium risk: CISO and CIO approval
  - High and Critical risk: CISO, CIO and Executive Management approval

6.1.3 Exception Documentation

All approved exceptions shall be documented including:

- Unique exception identifier
- Scope and duration of exception
- Approved compensating controls
- Implementation requirements
- Monitoring and review requirements
- Approval signatures and dates

6.2 Exception Management

6.2.1 Exception Tracking

The Information Security and Privacy Team shall maintain an exception register containing:

- All current and historical exceptions
- Status of compensating controls
- Exception expiration dates
- Review and renewal dates
- Risk reassessment results
- Compliance implications

6.2.2 Exception Monitoring

Approved exceptions shall be monitored to ensure:

- Compensating controls remain effective
- Business justification remains valid
- Risk levels haven't changed
- Compliance requirements are met
- Exception duration isn't exceeded

6.2.3 Exception Review and Renewal

All exceptions shall be reviewed:

- At least quarterly for high and critical risk exceptions
- At least bi-annually for medium risk exceptions
- Annually for low-risk exceptions
- Prior to expiration date
- When significant changes occur

Section 7: Review and Maintenance

7.1 Policy Review Process

7.1.1 Regular Review

This policy shall be reviewed:

- At least annually
- When significant organisational changes occur

- After major security and/or privacy incidents
- When regulatory requirements change
- When technology changes impact security and privacy requirements

7.1.2 Review Participants

Policy reviews shall include participation from:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Legal and Compliance Department
- Information Technology Department
- Group Head: Sustainability, QHS and Lead ISO Auditor
- Business Unit Heads
- Department Heads
- External Subject Matter Experts (as needed)

7.1.3 Review Criteria

Policy reviews shall evaluate:

- Effectiveness of current controls
- Alignment with business objectives
- Compliance with regulations
- Relevance to current threats
- Implementation challenges
- Resource requirements
- User feedback
- Incident lessons learned

7.2 Policy Maintenance

7.2.1 Policy Updates

Updates to this policy shall:

- Follow change management procedures
- Be documented with version control
- Include summary of changes
- Be reviewed by stakeholders
- Receive appropriate approvals
- Be communicated effectively

7.2.2 Supporting Documentation

Related documents shall be maintained including

- Procedures and guidelines
- Technical standards
- Implementation guides
- Training materials
- Assessment tools
- Compliance checklists

7.2.3 Communication and Training

Policy changes shall be:

- Communicated to all affected parties
- Incorporated into training programs
- Posted in accessible locations
- Included in awareness campaigns
- Verified for understanding

7.2.4 Communication and Training

Policy changes shall be:

- Communicated to all affected parties
- Incorporated into training programs
- Posted in accessible locations
- Included in awareness campaigns
- Verified for understanding

Appendix A: Definitions

A.1 General Terms

- **Information Security**: The protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximize return on investments and business opportunities.
- **Information Security and Privacy Management System (ISPMS):** A systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organisation's information security and privacy.
- **Risk**: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.
- **Control**: Means of managing risk, including policies, procedures, guidelines, practices, or organisational structures, which can be of administrative, technical, management, or legal nature.
- **Third-Party:** For the purposes of the ISPMS, a Third-Party is any person that is not a direct employee, but acts on behalf of, or has direct access to NEC XON's data, assets or intellectual property.

A.2 Technical Terms

- **Authentication**: The process of verifying the claimed identity of a user, process, or device.
- **Authorization**: The process of granting or denying specific requests for obtaining and using information resources.
- **Encryption**: The process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key.
- **Incident**: A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operation

A.3 Classification Terms

- **Public Information**: Information that has been declared public knowledge and can be freely distributed.
- **Internal Information**: Information that is intended for use within the organisation and unauthorised disclosure would be against policy.
- **Confidential Information**: Information that requires special precautions to protect it from unauthorised disclosure.
- **Restricted Information**: The most sensitive business information, intended strictly for use within specific groups.

Appendix B: Related Documents

B.1 Policies

- Access Control Policy
- Asset Management Policy
- Business Continuity Policy
- Cryptography Policy
- Data Protection Policy
- Incident Management Policy
- Network Security Policy

- Physical Security Policy
- Remote Working Policy
- Supplier Security Policy

B.2 Procedures

- Access Management Procedures
- Backup and Recovery Procedures
- Change Management Procedures
- Incident Response Procedures
- System Development Procedures
- Vulnerability Management Procedures

B.3 Standards

- Configuration Standards
- Encryption Standards
- Network Security Standards
- Password Standards
- System Hardening Standards

B.4 Guidelines

- Data Classification Guidelines
- Risk Assessment Guidelines
- Secure Development Guidelines
- Security Testing Guidelines
- Third-Party Security Guidelines

Appendix C: References

C.1 International Standards

- ISO/IEC 27001:2022 – Information Security Management Systems Requirements
- ISO/IEC 27002:2022 - Code of Practice for Information Security Controls
- ISO/IEC 27005:2018 - Information Security Risk Management

C.2 Regulatory Requirements

Protection of Personal Information Act, no 4 of 2013, as amended ("POPIA").	POPIA sets out to promote the protection of personal information processed by public and private bodies, to introduce certain conditions so as to establish the minimum requirements for the processing of personal information, to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and in accordance with PAIA, to provide for the issuing of codes of conduct, to provide for the rights of persons regarding unsolicited electronic communication and automated decision making, to regulate the flow of personal information across the borders of the Republic and to provide for matters connected herewith.
The General Data Protection Regulation (GDPR) (EU) 2016/679.	Similar to POPIA, the GDPR establishes the general obligations of data controllers and of those processing personal data on their behalf. It is the strongest privacy and security law in the world. It places an obligation on organizations to implement appropriate security measures, according to the risk involved in the data processing operations they perform.
Promotion of Access to Information Act, 2 of 2000, as amended ("PAIA").	PAIA seeks to promote transparency, accountability and effective governance of all institutions by empowering people to understand their access to information rights, act on them and both scrutinize and engage with decision making that affects them.

The full register of laws and regulations that are being adhered to and tracked by NEC XON can be reviewed upon request. Said register is being maintained by the Legal and Compliance Department.

C.3 Best Practices

- NIST Cybersecurity Framework
- CIS Controls
- OWASP Security Guidelines
- Cloud Security Alliance Guidelines

Appendix D: Forms and Templates

D.1 Required Forms

- Exception Request Form
- Security Incident Report Form
- Access Request Form

- Risk Assessment Template
- Audit Checklist Template
- Policy Acknowledgment Attestation

D.2 Supporting Templates

- Security Design Review Template
- Vendor Security Assessment Template
- Business Impact Analysis Template
- Project Security Plan Template
- Security Metrics Scorecard Template

Information Security and Privacy Policy v5.0

Final Audit Report 2025-02-18

Created:	2025-02-14
By:	Durandt Eksteen (durandt@nec.xon.co.za)
Status:	Signed
Transaction ID:	CBJCHBCAABAAF9QwbtM8a1e2loc1nn407CHsANB33lpJ

"Information Security and Privacy Policy v5.0" History

Document created by Durandt Eksteen (durandt@nec.xon.co.za)
2025-02-14 - 16:19:33 GMT- IP address: 165.49.84.152

Document e-signed by Durandt Eksteen (durandt@nec.xon.co.za)
Signature Date: 2025-02-14 - 16:22:09 GMT - Time Source: server- IP address: 165.49.84.152

Document emailed to Jitesh Ramduth (jitesh.ramduth@nec.xon.co.za) for signature
2025-02-14 - 16:22:10 GMT

Email viewed by Jitesh Ramduth (jitesh.ramduth@nec.xon.co.za)
2025-02-15 - 18:20:23 GMT- IP address: 156.155.12.232

Document e-signed by Jitesh Ramduth (jitesh.ramduth@nec.xon.co.za)
Signature Date: 2025-02-15 - 18:22:04 GMT - Time Source: server- IP address: 156.155.12.232

Document emailed to thabiet.gabier@nec.xon.co.za for signature
2025-02-15 - 18:22:05 GMT

Email viewed by thabiet.gabier@nec.xon.co.za
2025-02-17 - 07:06:18 GMT- IP address: 104.47.18.126

Signer thabiet.gabier@nec.xon.co.za entered name at signing as Thabiet Gabier
2025-02-17 - 07:06:54 GMT- IP address: 105.242.70.33

Document e-signed by Thabiet Gabier (thabiet.gabier@nec.xon.co.za)
Signature Date: 2025-02-17 - 07:06:56 GMT - Time Source: server- IP address: 105.242.70.33

Document emailed to bart.vanbuynder@nec.xon.co.za for signature
2025-02-17 - 07:06:57 GMT

Email viewed by bart.vanbuynder@nec.xon.co.za
2025-02-18 - 08:21:24 GMT- IP address: 105.245.229.16

Signer bart.vanbuynder@nec.xon.co.za entered name at signing as Bart van Buynder

2025-02-18 - 08:22:02 GMT- IP address: 105.245.229.16

Document e-signed by Bart van Buynder (bart.vanbuynder@nec.xon.co.za)

Signature Date: 2025-02-18 - 08:22:04 GMT - Time Source: server- IP address: 105.245.229.16

Document emailed to carel.coetzee@nec.xon.co.za for signature

2025-02-18 - 08:22:05 GMT

Email viewed by carel.coetzee@nec.xon.co.za

2025-02-18 - 09:40:19 GMT- IP address: 41.13.21.66

Signer carel.coetzee@nec.xon.co.za entered name at signing as JC Coetzee

2025-02-18 - 09:41:59 GMT- IP address: 41.13.21.66

Document e-signed by JC Coetzee (carel.coetzee@nec.xon.co.za)

Signature Date: 2025-02-18 - 09:42:01 GMT - Time Source: server- IP address: 41.13.21.66

Agreement completed.

2025-02-18 - 09:42:01 GMT