Information Security Policy Handbook

NEC XON Holdings (Pty) Ltd

Document Number: IT_POL_000300

09/02/2024

t +27 11 237 4500 f 086 575 8405

www.nec.xon.co.za

1 Mints Street, Old Mint Park, Louwlardia, 0157, South Africa ▲ PO Box 6973, Halfway House 1685, South Africa

Document Details

		Signatures with Date
Title	NEC XON Holdings (Pty) Ltd Information Security Policy Handbook	
Version	1.1	
Classification	Public	
Release Date	21/04/2023	
Description	The Information Security Policy Handbook underpins the Information Security Policy for NEC XON Holdings (Pty) Ltd	
Review Date	09/02/2024	
Author	Durandt Eksteen	
Reviewer/ Custodian	Office of the CISO	
Approved By	Chief Executive Officer	
Owner	Chief Information Officer	

Distribution List

Name
Public

Version History

Version	*Revision Date*	*Reviewer/ Custodian Name*	*Approver Name*	*Brief Description of Amendments*
1.1	09/02/2024	Durandt Eksteen	Durandt Eksteen	Updates to align to ISO 27001:2022 requirements
1.2				
1.3				
1.4				
1.5				

Contents

1. Introduction 6
2. Purpose 6
3. Scope 6
4. Information Security Policy 7
5. Acceptable Use Policy 8
6. Disciplinary Action ..... **Error! Bookmark not defined.**
7. Protect Stored Data 9

It is prohibited to store: 10

8. Information Classification 10
9. Access to sensitive business, staff, or customer data 11
10. Physical Security 12
11. Protect Data in Transit 13
12. Disposal of Stored Data 13
13. Security Awareness and Procedures 14
14. Network Security 15
15. System and Password Policy 16
16. Anti-virus policy 17
17. Patch Management Policy 18
18. Remote Access Policy 19
19. Vulnerability Management Policy 19
20. Configuration Standards 20
21. Change Control Process 21
22. Audit and Log Review 23

23. Penetration Testing Methodology 26
24. Incident Response Plan 27
25. Roles and Responsibilities 28
26. Third Party Access to Business, Staff or Customer Data 29
27. User Access Management 29
28. Access Control Policy 30
29. Wireless Policy 32
Appendix A 33

1. Introduction

This policy handbook underpins the Information Security Policy and encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy handbook fully. This document will be reviewed and updated by management on an annual basis or when relevant to include newly developed security standards into the policy handbook and distribute it to all employees and contracts or contractors as applicable.

This Information Security Policy is NEC XON Holdings (Pty) Ltd's highest level information security policy and along with this Information Security Policy Handbook, sets out the governance requirements to manage information security throughout NEC XON Holdings (Pty) Ltd, to ensure that our information assets are protected against a variety of information security threats, whether internal or external, deliberate, or accidental.

2. Purpose

The purpose of this policy handbook is to describe NEC XON Holdings (Pty) Ltd's commitment, and the commitment of its management, to preserving the confidentiality, integrity, authenticity, and reliability of business, staff and customer-related information, as well as personal information, in the possession or control of the company and/or any of its employees, contractors, subsidiaries, or affiliates, through the establishment of a comprehensive information security management system (ISMS). This commitment includes meeting requirements as set forth by ISO 9001, ISO 27001, Protection of Personal Information Act of South Africa (POPIA), and the General Data Protection Regulation (GDPR).

3. Scope

This policy applies to:

- Employees, contractors, consultants, volunteers, temporary and other workers at NEC XON Holdings (Pty) Ltd, and all personnel affiliated with company subsidiaries or third parties.
- All equipment that is owned or leased by, or otherwise in the custody or control of, NEC XON Holdings (PTY) Ltd.

- The use of all information, electronic and computing devices, and network resources used by NEC XON Holdings (PTY) Ltd. to conduct business or interact with internal networks and business systems, whether owned or leased by, or otherwise in the custody or control of NEC XON Holdings (PTY) Ltd, the employee, a company subsidiary, or a third party.

4. Information Security Policy Handbook

NEC XON Holdings (Pty) Ltd handles sensitive information daily. Sensitive Information must have adequate safeguards in place to protect it, to protect privacy, to ensure compliance with various regulations and to guard the future of the organisation.

NEC XON Holdings (Pty) Ltd commits to respecting the privacy of all its staff and customers and to protecting any data about staff and customers from outside parties. To this end, management are committed to maintaining a secure environment in which to process information so that the organisation can meet these promises.

Employees overseeing Sensitive data should:

- Handling of organisational and customer information in a manner that fits with its sensitivity.
- Limit personal use of NEC XON Holdings (Pty) Ltd information and telecommunication systems and ensure it does not interfere with job performance.
- NEC XON Holdings (Pty) Ltd reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems, and network traffic in the event of non-conformance or suspected unsolicited activities.
- Do not use email, internet, or any other organisational resources to engage in any action that is counter-productive, offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing, or illegal.
- Do not disclose personnel's personal information unless authorised by the data owner (Chief Information Officer) or the NEC XON Holdings (Pty) Ltd Legal and Compliance Department.
- Protect sensitive business, staff, and customer information.
- Keep passwords and accounts secure.
- Request approval from the Chief Information Officer prior to procuring, installing and/or establishing any new software or hardware, third-party connections, etc.
- Do not uninstall authorised software or hardware, including applications, operating systems, modems, and wireless access unless you have explicit approval from the Chief Information Officer.
- Always leave desks clear of sensitive data and lock computer screens when unattended.

- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.
- You are required to review and follow all policies, processes, and procedures as shared and stipulated by the Organisation. Non-Compliance can lead to disciplinary action and/or dismissal.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies, procedures or processes detailed herein or distributed via other methods such as the company intranet (Information Central) or email, you should seek advice and guidance from your line manager or Human Resources.

5. Acceptable Use Policy

Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to NEC XON Holdings (PTY) Ltd.'s established culture of openness, trust, and integrity. Management is committed to protecting the employees, partners, and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly. NEC XON Holdings (PTY) Ltd. will maintain an approved list of technologies and devices and personnel with access to such devices.

- Employees are responsible for exercising good judgment and utmost care regarding the reasonableness of personal use, pertinent to data, software, and hardware.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorised access to confidential/restricted data, including business, staff, and customer data.
- Employees should ensure that technologies should be used and set up in acceptable network locations.
- Keep passwords secure and do not share accounts.
- Authorised users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with an automatic activation feature.
- Because the information contained on portable computers is especially vulnerable, particular care should be exercised in terms of data and device security and safety.
- Postings by employees from a Company email address to newsgroups, or other public forums should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of NEC XON Holdings (PTY) Ltd. unless posting is during or due to business duties.

- Employees must use extreme caution when opening email attachments or completing information against emails received from known or unknown senders, which may contain viruses, ransomware, malware etc. Due attention should be given to each email to avert any loss of data or impact on business due to social engineering tactics, phishing, or spear-phishing risks.

6. Non-Compliance

Violation of the standards, policies, processes, and procedures presented in this document or via any other organisational communications method/s, by an employee may result in disciplinary action. This policy will be managed and guided in accordance with the organisation's disciplinary code. Non-Compliance may lead to warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment cannot be used as excuses for Non-Compliance.

7. Protect Stored Data

- All sensitive business, staff or customer data stored and overseen by NEC XON Holdings (Pty) Ltd, and its employees must always be securely protected against unauthorised use and data loss. Any sensitive business, staff or customer data that is no longer required by NEC XON Holdings (Pty) Ltd for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see certain business, staff or customer data or information, it must be masked when displayed.
- Business, staff, or customer data which is not protected as stated above should not be sent outside the organisational network via end-user messaging technologies like email, chats, messenger services or applications etc.
- Business data shall be stored on the organisationally supplied Microsoft OneDrive cloud-based storage solution, which each user is issued with at the inception of their employment with the organisation. No other storage method, whether a cloud-based 3rd party or local storage based (SSD/HDD) method is allowed to be used for storage of business data. Data loss due to data stored in other locations such as PCs, notebooks, mobile devices etc. may lead to organisational and reputational damage, as well as disciplinary or legal repercussions.

It is prohibited to:

1. Store the contents of business, staff or customer information or data on any media whatsoever, if not encrypted.
2. Store personal information or data such as photos, music, videos, or other materials on organisational information systems and/or hardware. This includes Microsoft OneDrive, Microsoft SharePoint, Microsoft Teams, Microsoft Outlook etc.
3. Business, staff or customer data on personal services or applications such as WhatsApp or other personal communication methods, social media services, and personal storage services unless authorised by the Chief Information Officer and required by the organisation.

8. Information Classification

Data and media containing data must always be labelled to indicate the sensitivity level.

Confidential - This is information for which unauthorised disclosure (even within the organisation) would cause serious damage to the interests of NEC XON Holdings (Pty) Ltd and should only be available to specific individuals and specific interested parties. Access to this information for specific interested parties will be governed by a Non-Disclosure Agreement (NDA). Unauthorised access to confidential information could inflict harm by virtue of serious financial loss, severe loss of profitability or opportunity, grave embarrassment, or loss of reputation. This information might include, but is not limited to:

- Prior details before major acquisitions, divestments, and mergers
- High-level business and competition strategy
- Extremely sensitive customer, supplier, partnership, or competitor assessments
- Intellectual property information
- Unreleased organisational performance data

Restricted - This is information for which unauthorised disclosure (even within the organisation) would cause significant harm to the interests of NEC XON Holdings (Pty) Ltd and should only be available to a specific group of employees and authorised third parties (governed by a signed Non-Disclosure Agreement (NDA)). Unauthorised access to this information could inflict harm by virtue of financial loss, loss of profitability or opportunity, embarrassment, or loss of reputation. This information might include, but not limited to:

- Minutes of meetings
- Customer information
- Supplier information
- Personnel's personal information

Internal Use - This information may be disclosed to employees and/or trusted third parties, if so, required by NEC XON Holdings (Pty) Ltd's business objectives. This information might include, but is not limited to:

- Organisational charts
- Certain organisational policies and procedures
- Product or services information in the form of proof of concept, final design and project related documents.

Public - This information may circulate freely to the public and therefore does not require any special protection. This information should not harm the organisation in any way. This information might include, but not is limited to:

- Published marketing material.
- Organisational public statements or announcements
- Published organisational performance information.

9. Access to sensitive business, staff, or customer data

All access to sensitive (confidential and restricted) business, staff or customer data should be controlled and authorised. Any Job functions that require access to business, staff, or customer data should be clearly defined.

- Access rights to privileged user IDs should be restricted to the least privilege necessary to perform job responsibilities.
- Privileges should be assigned to individuals based on job classification and function (Role-based access control)
- Access to sensitive business, staff or customer information or data is restricted to employees that have a legitimate need to view such information. No other employees should have access to confidential data unless they have a genuine business need.
- If business, staff, or customer data is shared with a service provider (third party) then a list of such Service Providers will be maintained.
- NEC XON Holdings (Pty) Ltd will ensure a written agreement that includes an acknowledgement is in place that a service provider will be responsible for the business, staff, or customer data that the service provider possesses.
- NEC XON Holdings (Pty) Ltd will ensure that there is an established process, including that proper due diligence is in place before engaging with a service provider.
- NEC XON Holdings (Pty) Ltd will have a process in place to monitor the ISO 27001 compliance statuses of the Service providers.
- Access will not be allowed if MFA (Multi-Factor Authentication) is not enforced.

10. Physical Security

Access to sensitive information in both hard and soft media formats must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorised access to confidential data, including business, staff, and customer data.
- Employees should ensure that technologies should be used and set up in acceptable network locations.
- Personnel using organisational ICT devices should verify the identity of any third-party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using ICT devices should be trained to report suspicious behaviour and indications of tampering with the devices to the appropriate personnel.
- A "visitor" is defined as a trusted vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, received faxes, external disks, USB storage devices, computer drives, etc.
- Media containing sensitive business, staff or customer information must be encrypted, overseen, and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive business, staff, or customer information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where business, staff or customer data is accessible. "employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "residents" on NEC XON Holdings (Pty) Ltd sites. A "visitor" is defined as a trusted vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Network ports located in public and areas accessible to visitors must be disabled and enabled when network access is explicitly authorised.
- All ICT devices should be appropriately protected and secured so they cannot be tampered with, stolen,

or altered. This includes mobile data-carrying devices such as notebooks, tablets, phablets, and smartphones. It is expected that staff will do their utmost to always protect and secure hardware and data.

- Strict control is maintained over the external or internal distribution of any media containing business, staff or customer data and must be approved by management.
- Strict control is to be maintained over the storage and accessibility of media.

11. Protect Data in Transit

All sensitive business, staff or customer data must be protected securely if it is to be transported physically or electronically.

- Sensitive business, user or customer data must never be sent over the internet via email, instant chat, or any other end-user technologies unless explicitly approved by management.
- If there is a business justification to send sensitive business, staff, or customer data via email or via the internet or any other modes then it should be done after authorisation is obtained and by using a strong encryption mechanism.
- The transportation of media containing sensitive business, staff or customer data to another location must be authorised by management, logged, and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.
- Each employee should be cognisant of and maintain strict control over the email communication they initiate to ensure that the correct file is attached and/or the correct link is supplied, and that the audience of the email has been verified before the email is sent.

12. Disposal of Stored Data

- All data must be securely disposed of when no longer required by NEC XON Holdings (Pty) Ltd, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of business, staff and customer data must be manually destroyed as and when no longer required for valid and justified business reasons. A quarterly process must be in place to

confirm that all non-electronic business, staff, and customer data has been appropriately disposed of in a timely manner.

- NEC XON Holdings (Pty) Ltd will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials be crosscut, shredded, incinerated, or pulped so they cannot be reconstructed.
- NEC XON Holdings (Pty) Ltd will have documented procedures for the destruction of electronic media. These will require:
    - All business, staff or customer data on electronic media must be rendered unrecoverable when deleted e.g., through degaussing or electronically wiping using military-grade secure deletion processes or the physical destruction of the media.
    - If secure wipe programs are used, the process must define the industry-accepted standards followed for secure deletion.

13. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain an elevated level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day-to-day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form.
- All employees that oversee sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the organisation.
- All third parties with access to sensitive business, staff or customer data are contractually obligated to comply with the ISO 27001 standard/framework.
- Company security policies must be reviewed annually and updated as needed.

14. Network Security

- Firewalls must be implemented at each internet connection point, any demilitarised zone and the internal company network.
- A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the business, staff, or customer data-containing production environment.
- Stateful Firewall technology must be implemented where the Internet enters NEC XON Holdings (Pty) Ltd's network to mitigate known and ongoing threats. Firewalls must also be implemented to protect local network segments and the ICT resources that attach to those segments such as the business network, and open network.
- All inbound and outbound traffic must be restricted to that which is required for the business, staff, and customer data-containing environment.
- All inbound network traffic is blocked by default unless explicitly allowed and the restrictions must be documented.
- All outbound traffic must be authorised by management (i.e., what are the allowed categories of sites that can be visited by the employees), and the restrictions must be documented.
- NEC XON Holdings (Pty) Ltd will have firewalls between any wireless networks and the business, staff and customer data-holding environment.
- NEC XON Holdings (Pty) Ltd will quarantine wireless users into a Demilitarised Zone (DMZ), where they will be authenticated and firewalled as if they were coming in from the Internet.
- Disclosure of private IP addresses to external entities must be authorised.
- A topology of the firewall environment must be documented and must be updated in accordance with the changes in the network.
- The firewall rules will be reviewed on a six-month basis to ensure validity and the firewall must have a clean-up rule at the bottom of the rule base.
- No direct connections from the Internet to the business, staff and customer data-containing environment will be permitted. All traffic must traverse through a firewall.

15. System and Password Policy

All users, including contractors and vendors with access to NEC XON Holdings (Pty) Ltd's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- A system configuration standard must be developed along industry acceptable hardening standards (SANS, NIST, ISO)
- System configurations should be updated as issues are identified (as defined in ISO 27001)
- System configurations must include common security parameter settings.
- The systems configuration standard should be applied to any new systems configured.
- All vendor default accounts and passwords for the systems must be changed at the time of provisioning the system/device into the NEC XON Holdings (Pty) Ltd network and all unnecessary services and user/system accounts must be disabled.
- All unnecessary default accounts must be removed or disabled before installing a system on the network.
- Security parameter settings must be set appropriately on system components.
- All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed.
- All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system.
- Any insecure protocols, daemons, services in use must be documented and justified.
- All users with access to business, staff or customer data must have a unique user ID.
- All users must use Mult-Factor Authentication (MFA) to access the company network or any other electronic resources.
- All user IDs for terminated users must be deactivated or removed immediately.
- The user ID will be locked out if there are more than five unsuccessful attempts. This locked account can only be enabled by an ICT system administrator. Locked-out user accounts will be disabled for a minimum period of 30 minutes or until the ICT systems administrator enables the account.
- All system and user-level passwords must be changed on at least a quarterly basis.
- A minimum password history of twelve months must be implemented.
- A unique password must be set up for users and the users are to be prompted to change the password on the first login.
- Group shared or generic user accounts or passwords or other authentication methods must not be used to administer any system components.
- Where SNMP is used, the community strings must be defined as something other than the Standard defaults of "public," "private" and "system" must be different from the passwords used to log

in interactively.

- All non-console ICT system administrative access will use appropriate technologies like ssh, vpn etc. or strong encryption is invoked before the ICT system administrator password is requested.
- System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands.
- ICT system administrator access to web-based management interfaces is encrypted using strong cryptography.
- The responsibility of selecting a password that is hard to guess falls to users. A strong password must:

a) Be as long as possible (never shorter than ten (14) characters).
b) Include mixed-case letters, if possible.
c) Include digits and punctuation marks, if possible.
d) Not to be based on any personal information.
e) Not to be based on any dictionary word, in any language.

- If an operating system without security features is used (such as DOS, Windows or MacOS), then an intruder only needs temporary physical access to the console to insert a keyboard monitor program. If the workstation is not physically secured, then an intruder can reboot even a secure operating system, restart the workstation from his own media, and insert the offending program.
- To protect against network analysis attacks, both workstations and servers should be cryptographically secured. Examples of strong protocols are the encrypted Netware login and Kerberos.

16. Anti-virus policy

- All machines must be configured to run the latest anti-virus software as approved by NEC XON Holdings (Pty) Ltd.
- The preferred application to use is Microsoft Defender for Endpoint (Plan 1), which must be configured to retrieve the latest updates to the antiviral program automatically daily. The antivirus should have periodic scanning enabled for all the systems.
- The Anti-Virus software in use should be capable of detecting all known types of malicious software (viruses, trojans, adware, ransomware, malware, spyware, worms, and rootkits).
- All removable media (for example USB memory sticks, external storage (HDD and SSD) and others) should be scanned for viruses before being used.

- All the logs generated from the antivirus solutions must be retained as per legal/regulatory/contractual requirements or at a minimum of ISO 27001 requirements.
- Master Installations of the Anti-Virus software should be set up for automatic updates and periodic scans.
- End users must not modify or alter the Anti-Virus software.
- Emails with attachments coming from suspicious or unknown sources should not be opened. All such emails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any email, which they suspect may contain a virus or may be malevolent in any way.

17. Patch Management Policy

- All Workstations, servers, software, system components, applications etc. owned by NEC XON Holdings (Pty) Ltd must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
- Wherever possible all systems and software must have automatic updates enabled for system patches released from their respective vendors. Security patches must be installed within one month of release from the respective vendor and must follow the process in accordance with the change control process.
- Any exceptions to this process must be documented.
- The onus rests with the user where a manual reboot of equipment is required to finalise patch installation. If a security event occurs from an unpatched device (due to a user not having assured patch installation), the user in question could be held liable and may face disciplinary action.

18. Remote Access policy

- It is the responsibility of NEC XON Holdings (Pty) Ltd's employees, contractors, vendors, and agents with remote access privileges to the organisation's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the organisation.
- Secure remote access must be strictly controlled. Control will be enforced by multi-factor authentication (MFA) via a one-time password authentication or public/private keys with strong passphrases.
- Vendor accounts with access to NEC XON Holdings (Pty) Ltd's network will only be enabled during the time-period the access is required and will be disabled or removed once access is no longer required.
- All hosts that are connected to NEC XON Holdings (Pty) Ltd's internal networks via remote access technologies will be monitored on a regular basis.
- All remote access accounts used by vendors, or third parties will be reconciled at regular intervals and the accounts will be revoked if there is no further business justification.
- Vendor accounts with access to NEC XON Holdings (Pty) Ltd's network will only be enabled during the time the access is required and will be disabled or removed once access is no longer required.

19. Vulnerability Management Policy

- All the vulnerabilities would be assigned a risk ranking such as High, Medium, and Low based on industry best practices.
- As part of the ISO 27001 Compliance requirements, NEC XON Holdings (Pty) Ltd will run internal and external network vulnerability scans at least quarterly and after any notable change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- Quarterly internal vulnerability scans must be performed by NEC XON Holdings (Pty) Ltd, by internal staff, or a third-party vendor and the scan process must include that rescans will be done until passing results are obtained, or all High vulnerabilities are resolved.
- Bi-annual external vulnerability scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes may be performed by the organisation's internal staff. The scan process should include re-scans until passing results are obtained.

20. Configuration Standards

- Information systems that process transmit, or store business, staff or customer data must be configured in accordance with the applicable standard for that class of device or system. Standards must be maintained by the team responsible for the management of the system/s in conjunction with the Information Technology Department.
- All network device configurations must adhere to NEC XON Holdings (Pty) Ltd's required standards before being placed on the network as specified in the organisation's configuration guide. Using this guide, a standard configuration has been created that will be applied to all network devices before being placed on the network.
- Before being deployed into production, a system must be certified to meet the applicable configuration standard.
- Updates must be applied within the time frame identified by the Information Technology Department.
- Administrators of network devices that do not adhere to NEC XON Holdings (Pty) Ltd's standards (as identified via a previous exception) must document and follow a review process of announced vendor updates to the operating system and/or configuration settings. This process must include a review schedule, risk analysis method and update method.
- All network device configurations must be checked annually against the configuration standard to ensure the configuration continues to meet required standards.
- Where possible, network configuration management software will be used to automate the process of confirming adherence to the standard configuration.
- For other devices, an audit will be performed quarterly to compare the standard configuration to the configuration currently in place.
- All discrepancies will be evaluated and remediated by the network administration processes and/or staff.
- A hardware asset, (once configured by the Information Technology Department) may not be amended in terms of software installation or removal, unless approval has been obtained from the Chief Information Officer.

21. Change Control Process

- Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, evaluated, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.
- The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.
- All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented. A documented audit trail, containing relevant information shall be maintained. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.
- A risk assessment shall be performed for all changes and dependent on the outcome, an impact assessment should be performed.
- The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable, consider compliance with legislative requirements and standards.
- All change requests shall be prioritised in terms of benefits, urgency, the effort required and potential impact on operations.
- Changes shall be evaluated in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

- Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.
- All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e., the change request was made by an authorised user, the impact assessment was performed and proposed changes were evaluated.
- All users significantly affected by a change shall be notified of the change. The user representative shall sign off on the change. Users shall be required to make submissions and comments prior to the acceptance of the change.
- Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to the effort required to develop and implement said changes.
- Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fallback procedures will be in place to ensure systems can revert to what they were prior to the implementation of changes.
- Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.
- Specific procedures to ensure proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as emergency changes.
- All changes will be monitored once they have been rolled out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

22. Audit and Log Review

- This procedure covers all logs generated for systems within the business, staff, and customer data-accessible environment, based on the flow of data over the NEC XON Holdings (Pty) Ltd's network, including the following components:
    - Operating System Logs (Event Logs and su logs).
    - Database Audit Logs.
    - Firewalls & Network Switch Logs.
    - Antivirus Logs.
    - CCTV Video recordings.
    - File integrity monitoring system logs.

- Audit Logs must be maintained for a minimum of 3 months online (available for immediate analysis) and 12 months offline.
- Review of logs is to be conducted by means of NEC XON Holdings (Pty) Ltd's network monitoring system, which is controlled from the organisational console. The console is installed on a server/s, located within NEC XON Holdings (Pty) Ltd.'s Head Office based Data Center environment, as well as in the cloud within Microsoft Sentinel.
- The following personnel are the only people permitted to access log files (ICT System Administrators).
- The network monitoring system/s software is configured to alert NEC XON Holdings (Pty) Ltd's Information Technology Department to any conditions deemed to be potentially suspicious, for further investigation.

  Alerts are configured to:
- A dashboard browser-based interface, monitored by the Organisation's Information Technology Department.
- Email / SMS alerts to NEC XON Holdings (Pty) Ltd's Information Technology Department's monitoring mailbox with a summary of the incident.
- The following Operating System Events are configured for logging, and are monitored by the Information Technology Department:

  a) Any additions, modifications, or deletions of user accounts.

b) Any failed or unauthorised attempt at user login.
c) Any modification to system files.
d) Any access to the server, or application running on the server, including files that hold business, staff, or customer data.
e) Actions taken by any individual with root or administrative privileges.
f) Any user access to audit trails.
g) Any creation/deletion of system-level objects installed by Windows. (All system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)
h) Any installation or removal of software on organisationally owned ICT infrastructure / assets.

- The following Database System Events are configured for logging, and are monitored by the network monitoring system:

a) Any failed user access attempts to log in to the Microsoft SQL databases.
b) Any login that has been added or removed as a database user to a database.
c) Any login that has been added or removed from a role.
d) Any database role that has been added or removed from a database.
e) Any password that has been changed for an application role.
f) Any database that has been created, altered, or dropped.
g) Any database object, such as a schema, which has been connected to.
h) Actions that are taken by any individual with DBA privileges.

- The following Firewall Events are configured for logging, and are monitored by the network monitoring system:

a) ACL violations.
b) Invalid user authentication attempts.
c) Logon and actions taken by any individual using privileged accounts.
d) Configuration changes made to the firewall (e.g., policies disabled, added, deleted, or modified).

- The following Switch Events are to be configured for logging and monitored by the network monitoring system:

a) Invalid user authentication attempts.
b) Logon and actions that were taken by any individual using privileged accounts.

c) Configuration changes made to the switch/es (e.g., configuration disabled, added, deleted, or modified).

- The following Intrusion Detection Events are to be configured for logging, and are monitored by the network monitoring system:

a) Any vulnerability listed in the Common Vulnerability Entry (CVE) database.
b) Any generic attack(s) not listed in CVE.
c) Any known denial of service attack(s).
d) Any traffic patterns that indicated pre-attack reconnaissance occurred.
e) Any attempts to exploit security-related configuration errors.
f) Any authentication failure(s) that might indicate an attack.
g) Any traffic to or from a back-door program.
h) Any traffic typical of known stealth attacks.

- The following File Integrity Events are to be configured for logging and monitored by the network monitoring system:

a) Any modification to system files.
b) Actions taken by any individual with administrative privileges.
c) Any user access to audit trails.
d) Any Creation / Deletion of system-level objects installed by Windows. (All system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

- For any suspicious event confirmed, the following must be recorded on a Log Review Form, and NEC XON Holdings (Pty) Ltd's Chief Information Officer informed:

a) User Identification.
b) Event Type.
c) Date & Time.
d) Success or Failure indication.
e) Event Origination (e.g., IP address).
f) Reference to the data, system component or resource affected.

23. Penetration Testing Methodology

- In this section should be listed the risks inherent in conducting penetration testing over the information systems of NEC XON Holdings (Pty) Ltd. Additionally, should be noted for each of the mitigation measures that will be taken. Examples might be:

Example one#

Risk: Denial of Service in systems or network devices because of the network scans.

Mitigation measure 1: network scans must be performed in a controlled manner. The start and end of the scan must be notified to responsible personnel to allow monitoring during testing. For any sign of trouble will abort the scan in progress.

Mitigation measure 2: scanning tools must be configured to guarantee that the volume of sent packets or sessions established per minute does not cause a problem for network elements. In this sense, we must perform the first scans in a very controlled way and use the minimum configuration that may be expanded when is evident that the configuration is not dangerous for network devices or servers in the organization.

- Key staff involved in the project by the organization will be listed:

Technical Project Manager:
Chief Information Security Officer:
Chief Information Officer:
Head of Communications:
Responsible for website http://www.nec.xon.co.za :

- External intrusion tests will be performed remotely from the supplier's premises. Internal intrusion tests will be conducted in the office of the organisation. The audit team must have access to the organisation's network. It must manage access permissions to the building early enough to ensure that the audit team can access it without problems during the planning period.
- All the tests will be conducted from the equipment owned by the audit team so no equipment for the execution of the tests is required. The only requirement in this regard will be to have an active

network connection for each member of the audit team. Those connections must provide access to the target network segment in every case.

- If an incident occurs during the execution of the tests that have an impact on the systems or services of the organisation, the incident should be brought immediately to the attention of those responsible for incident management.
- Findings or vulnerabilities identified during the tests conducted will be generated and documented with sufficient evidence to prove the existence of the same. The format of the evidence can be variable in each case, screen capture, raw output of security tools, photographs, paper documents, etc.
- As a result of tests performed should generate a document containing at least the following sections:

Introduction
Executive Summary
Methodology
Identified vulnerabilities.
Recommendations for correcting vulnerabilities
Conclusions
Evidence

24. Incident Response Plan

'Security incident' means any incident (accidental, intentional, or deliberate) relating to communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage the organisation.
The Incident response plan must be evaluated once annually. Copies of this incident response plan are to be made available to all relevant staff members and steps are to be taken to ensure that they understand it and what is expected of them.

Employees of the company will be expected to report to the Chief Information Officer, for any security-related issues.

NEC XON Holdings (Pty) Ltd's Security Incident Response Team:

Chief Information Officer
Marketing Manager
Head of Legal and Compliance
Office of the CISO
Cyber Security Business Unit
IT Operations Manager
Information Technology Department

25. Roles and Responsibilities

- The Office of the CISO and the Chief Information Officer is responsible for overseeing all aspects of information security, including but not limited to:
- Creating and distributing security policies, processes, and procedures.
- Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel.
- Creating and distributing security incident response and escalation procedures that include:
- Maintaining a formal security awareness program for all employees that provide multiple methods of communicating awareness and educating employees (for example – emails, posters, letters, and meetings).
- The Information Technology Department shall maintain daily administrative and technical operational security procedures that are consistent with ISO 27001 (for example, user account maintenance procedures, and log review procedures).
- System and Application Administrators shall:
- Monitor and analyse security alerts and information and distribute them to appropriate personnel.
- Administer user accounts and manage authentication.
- Monitor and control all access to data.
- Maintain a list of service providers.
- Ensure there is a process for engaging service providers including proper due diligence prior to engagement.
- The Human Resources Department and Legal and Compliance Department are responsible for tracking employee participation in the security awareness program, including:
- Facilitating participation upon hire and at least annually.
- Ensuring that employees acknowledge in writing at least annually that they have read and understand the Company's information security policy and other mandatory training.

- Written contracts require adherence to the ISO 27001 standard by the service provider/s.
- Written contracts include acknowledgement or responsibility for the security of business, staff, or customer data by the service provider/s.
- Cybersecurity and Information Technology staff have the right to terminate any user ID, workstation, and network communication identified pertinent to suspicious activity or a possible Cybersecurity breach (that could have negative consequences to NEC XON Holdings (Pty) Ltd)
- Cybersecurity and Information Technology staff have the right to forensically investigate any user's, equipment, emails, or any other form of digital interaction, in the event of a suspected Cybersecurity or Information Security breach or if any form of illicit activity is suspected.

26. Third Party Access to Business, Staff or Customer Data

- All third-party companies providing critical services to NEC XON Holdings (Pty) Ltd must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with the Company's Physical Security and Access Control Policy, as well as the Information Security Policy.
- All third-party companies which have access to business, staff or customer information must:

1. Adhere to the ISO 27001 standard and organisational security requirements.
2. Acknowledge their responsibility for securing the business, staff, or customer-related data.
3. Acknowledge that the business, staff, or customer data must only be used for assisting in the completion of a valid business requirement, providing a service or for uses specifically required by law.
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster, or failure.

27. User Access Management

- Access to NEC XON Holdings (Pty) Ltd is controlled through a formal user registration process beginning with a formal notification from the Human Resources Department.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work conducted.
- There is a standard level of access; other services can be accessed when specifically authorised.

- The job function of the user decides the level of access the employee has to business, staff, or customer data.
- Access to all NEC XON Holdings (Pty) Ltd systems is provided by the Information Technology Department and can only be started after proper procedures are completed.
- As soon as an individual leaves the organisation's employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process the Human Resources Department will inform the Information Technology Department of all leavers and their date of departure.

28. Access Control Policy

- Access Control systems are in place to protect the interests of all users of NEC XON Holdings (Pty) Ltd's computer systems by providing a safe, secure, and readily accessible environment in which to work.
- NEC XON Holdings (Pty) Ltd will provide all employees and other users with the information they need to fulfil their responsibilities in as effective and efficient a manner as possible.
- Generic or group IDs shall not normally be permitted but may be granted under exceptional circumstances if sufficient other controls pertinent to access are in place.
- The allocation of privileged rights (e.g., local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorisation provided jointly by the system owner and the Chief Information Officer. Technical teams shall guard against issuing privileged rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification, and/or is approved by the Chief Information Officer.
- Users are obligated to report instances of non-compliance to NEC XON Holdings (Pty) Ltd's Chief Information Officer or, the Human Resources Department.

- Access to The organisation's Information Technology resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any of the organisation's Information Technology resources and services will be provided without prior authentication and authorisation of a user's NEC XON Holdings (Pty) Ltd, Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Active Directory Group Policy Objects or Microsoft Intune.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed, or revoked must be made in writing and via a logged ticket.
- Users are expected to become familiar with and abide by all of NEC XON Holdings (Pty) Ltd's policies, Procedures, Processes, Standards and/or guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorisation by the Information Technology Department and will be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is vigorously and appropriately controlled according to the data classification levels described in the Information Security Policy Handbook.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, Microsoft SharePoint Online intranet authentication rights, SQL database rights, isolated networks, and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with the Information Technology Department to review users' access rights. The review shall be logged, and the Information Technology Department shall sign off on the review to give authority for users' continued access rights.

29. Wireless Policy

- Installation or use of any unapproved wireless device or wireless network located within any physical location in use by NEC XON Holdings (Pty) Ltd is prohibited.
- Installation or use of any wireless device or wireless network intended to be used to connect to any of the NEC XON Holdings (Pty) Ltd networks is prohibited.
- A quarterly test should be run to discover any wireless access points connected to the company network.
- Usage of appropriate testing using tools like net stumbler, kismet etc. must be performed on a quarterly basis to ensure that:
- Any devices which support wireless communication remain disabled or decommissioned.
- If any violation of the Wireless Policy is discovered because of the normal audit processes, the Chief Information Officer or anyone with a similar authority has the authorisation to stop, cease, shut down, and remove the offending device immediately.

If the need arises to use wireless technology, it should be approved by the Chief Information Officer and the following wireless standards must be adhered to:

1. Default SNMP community strings and passwords, passphrases, Encryption keys/security-related vendor defaults (if applicable) should be changed immediately after the installation of the device.
2. The firmware on the wireless devices must be updated accordingly as per the vendor's release schedule.
3. The firmware on wireless devices must support strong encryption for authentication and transmission over wireless networks.
4. Any other security-related wireless vendor defaults should be changed if applicable.
5. Wireless networks must implement industry best practices and strong encryption for authentication and transmission of business, staff, or customer data.
6. An Inventory of authorised access points along with a business justification must be maintained.

Appendix A – Agreement to Comply Form – Agreement to Comply with Information Security Policy and Information Security Policy Handbook

_____

Employee Name (printed)

_____

Department

In signing off below, I agree that I fully understand and commit to meeting the requirements set out in this document. I agree to take all reasonable precautions to assure that organisational, internal information, or information that has been entrusted to the organisation by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the organisation, I agree to return all information to which I have had access because of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Chief Information Officer, who is the designated information owner.

I have access to a copy of the Information Security Policy and its underpinning Handbook (this document), and I understand how it impacts my job. As a condition of continued employment, I agree to abide by this and all other relevant policies and procedures. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security requirements to the Chief Information Officer or the Human Resources Department.

_____

Employee Signature