NEC XON HOLDINGS (Pty) Ltd and its subsidiaries

Protection of Personal Information (PII) Policy

File name	Protection of Personal Information (PII) Policy
File reference	DP_POL_001189
Last change	01-04-2025
Author of the last change	Durandt Eksteen
Contact	Durandt.Eksteen@nec.xon.co.za
Confidentiality Level	General
Status	Finalised
Version	5.0

Document Details

		Signatures with Date
Title	Protection of Personal Information (PII) Policy v5.0	
Version	5.0	
Classification	General	
Release Date	01/04/2025	
Description	The purpose of this policy is to make employees aware of how to process Personal Information (PII) and the actions set out in this Policy should be used as guidance when responding to a Personal Information (PII) Breach.	
Review Date	01/04/2026	
Author	Chief Information Officer	Durandt Eksteen
Approved By	Chief Executive Officer	
Owner	Head: Legal and Compliance	
Reviewed By	Information Security Officer	Jitesh Ramduth Jitesh Ramduth (Apr 4, 2025 08:37 GMT+2)
Reviewed By	Group Head: Sustainability, QHS & Lead ISO Auditor	TGabier TGabier (Apr 4, 2025 09:19 GMT+2)
Reviewed By	Chief Operating Officer	

Distribution List

Status
General

Version History

Version	*Revision Date*	*Reviewer/ Custodian Name*	*Approver Name*	*Brief Description of Amendments*
1.0	01/03/2018	Jurgen Grosse-Heitmeyer	Jurgen Grosse-Heitmeyer	Creation of Protection of Personal Information (PII) Policy
2.0	27/05/2021	Hardy van Wyk	Hardy van Wyk	Document Updated
3.0	21/07/2022	Thigerson Reddy	Thigerson Reddy	Document Updated
4.0	28/03/2024	Durandt Eksteen	Durandt Eksteen / Thigerson Reddy / Carel Coetzee	Alignment to ISO 27001:2022 certification requirements
5.0	01/04/2025	Durandt Eksteen	Carel Coetzee	Updating of document to align with ISO 27001:2022, ISO 27032:2023, ISO 27701:2019

Contents

1) Introduction

NEC XON and its subsidiaries ("NEC XON") recognises the importance of having effective protection-methods in place and is committed to compliance with applicable Personal Information (PII) protection laws, regulations, internal policies, and standards. These protections form the foundation of a trustworthy company, are necessary to maintain the confidence of customers and employees and ensure NEC XON's own compliance with such local laws.

This Protection of Personal Information Policy ("Policy") is based on globally accepted, basic principles on data protection and provides guidance on how to proceed to meet the rights of the data subjects regarding the processing by NEC XON of its Personal Information (PII) under the Protection of Personal Information Act ("POPIA") and it is implemented in conjunction with NEC XON's relevant Information Security and Privacy Management System (ISPMS) policies applicable to NEC XON's operations.

2) Scope

This Policy applies to all of NEC XON's indirect and direct employees, namely, contractors, consultants, temporary employees, trainees and any other third parties working for NEC XON whilst handling Personal Information (PII).

3) Purpose

The purpose of this policy is to make employees aware of how to process Personal Information (PII) and the actions set out in this Policy should be used as guidance when responding to a Personal Information (PII) Breach. It is intended that the steps set out here will be useful in ensuring that NEC XON's obligations under the Protection of Personal Information (PII) Act ("POPIA") are fulfilled.

4) Definitions

'PII'	Personal Identifiable Information
'Child'	any natural person under the age of 18 (eighteen) years;
'Data Breach'	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information (PII) under the control of or in the possession of NEC XON;
'Data Subjects'	means individuals or natural persons of whom a controller holds Personal Information (PII) and who can be identified, directly or indirectly, by reference to that Personal Information (PII);
'Chief Information Officer'	means in relation to, a – a) public body means an Information Officer or Deputy Information Officer as contemplated in terms of section 1 or 17 of POPIA; and

	b) private body means the head of a private body as contemplated in section 1 of POPIA.
'Employees'	means any employee of the NEC XON;
'Operator'	means a person who processes Personal Information (PII) for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;
'Processing'	means any operation or activity or any set of operations, whether by automatic means, concerning Personal Information (PII). This includes, amongst other things, the collection, recording, organisation, storage, modification, or transmission of Personal Information (PII);
'Person'	means a natural person or juristic person;
'Personal Information (PII)'	a. means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: b. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical, mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person; c. information relating to the education or the medical, financial, criminal or employment history of the person; d. any identifying number, symbol, personal e-mail address, physical address, telephone number, location information, online identifier, or other assignment to the person; e. the biometric information of the person; f. the personal opinions, views, or preferences of the person; g. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; h. the views or opinions of another individual about the person; and i. the name of the person if it appears with other Personal Information (PII) relating to the person or if the disclosure of the name itself would reveal information about the person.

'POPIA'	means the Protection of Personal Information (PII) Act No. 4 of 2013;
'Privacy Collaborator'	means the person in charge is responsible to ensure the implementation of POPIA in NEC XON.
'Responsible Party'	means a public or private body or any other person which alone or in conjunction with others, determines the purpose of and means for processing Personal Information (PII);
'Special Personal Information (PII)'	means Personal Information (PII) concerning a Data Subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life, biometric information, or criminal behaviour;
'NEC XON'	means NEC XON Holdings (Pty) Ltd and its subsidiaries ("NEC XON"); and
'Third Party'	means any independent contractor, agent, consultant, sub-contractor, or other representative of NEC XON.

5) Basic Principles

Fostering a data protection culture is essential for NEC XON to maintain its social credibility and sustain its business activities.

All NEC XON Personnel, irrespective of their function or geographic location, must understand their specific responsibilities related to data and user protection and actively work to manage risks associated with data and user protection. NEC XON aims to embed this data protection culture through various training courses and through rules and regulations. Where applicable (dependant on business area), Data and User Privacy laws or regulations applicable in other countries also need to be considered and implemented alongside the requirements of POPIA. Therefore, all relevant privacy-related laws and regulations also apply where only POPIA is listed below.

NEC XON applies the following basic principles to data protection globally:

Accountability

The responsible party must ensure compliance with all the conditions under POPIA and is responsible for implementing such conditions. This will include having to ensure that any third party or service providers (defined as 'operators' under POPIA) also comply with the provisions of POPIA.

Processing Limitation

Processing of Personal Information (PII) must be undertaken lawfully and done in a reasonable manner.

Purpose Specification

Personal Information (PII) must be collected for a specific, explicitly defined, and lawful purpose relating to the responsible party's business.

Further Processing

The further processing of Personal Information (PII) must be undertaken in accordance with, or be compatible with, the purpose for which the Personal Information (PII) was originally collected. It is important to note that further processing will be compatible with the original purpose if:

- the Data Subject gives consent;
- the information is in a public record or has been deliberately made public by the data subject;
- the further processing is necessary to avoid prejudice to the maintenance of the law by any public body, to comply with obligations imposed by the law or in the interests of national security; or
- the further processing is necessary to prevent or mitigate a threat to public health or safety or the life or health of the Data Subject or anyone else.

Information Quality

The responsible party will need to ensure that the Personal Information (PII) it processes about the data subjects is complete, accurate, not misleading and updated, when and where necessary.

Openness

This condition seeks to ensure transparency between the responsible party and data subject.

Security Safeguards

The responsible party must secure the integrity of Personal Information (PII) in its possession or under its control with appropriate and reasonable technical and organisational measures to prevent the loss of or damage to or unauthorised destruction of the Personal Information (PII), and any unlawful access to or processing of Personal Information (PII).

Data Subject Participation

A data subject, having provided adequate proof of identity, has the right to request the responsible party to confirm, free of charge, whether the responsible party holds Personal Information (PII) about that data subject. The Data Subject may then request a description of the Personal Information (PII), including information about third parties who have had access to the information, within a reasonable time and at a prescribed fee (if any). In addition, the information must be provided to the Data Subject in a reasonable manner and in a form that is generally understandable.

6) Process of Collecting Personal Information (PII)

Personal Information (PII) must be collected directly from the Data Subject as and when required for a defined purpose, unless an exception is applicable (such as, for example, where the Data Subject has made the Personal Information (PII) public, or the Personal Information (PII) is contained in or derived from a public record).

The exceptions to the collection of Personal Information (PII) are:

a. the information is contained in or derived from a public record or has deliberately been made public by the data subject;
b. the Data Subject or a competent person, where the Data Subject is a child, has consented to the collection of the information from another source;
c. collection of the information from another source would not prejudice a legitimate interest of the data subject;
d. collection of the information from another source is necessary —
    i. to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences;
    ii. to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);
    iii. for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
    iv. in the interests of national security; or
    v. to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied.
    vi. compliance would prejudice a lawful purpose of the collection; or
    vii. compliance is not reasonably practicable in the circumstances of the particular case.

NEC XON must always ensure that it protects the Data Subject's rights and will Process the Personal Information (PII) based on legitimate grounds in a manner that does not adversely affect the Data Subject in question.

If Personal Information (PII) is obtained from a Third Party, NEC XON shall ensure that the Third Party has collected the Personal Information (PII) in accordance with the applicable laws for sharing Personal Information (PII), however, NEC XON can't be held responsible.

An example of such Third Parties includes:

a) Recruitment agencies;

b) Other companies providing services to NEC XON; and

c) Where NEC XON makes use of publicly available sources of information (e.g., the Companies and Intellectual Property Commission (CIPC), an agency of the Department of Trade and Industry in South Africa etc).

7) Lawful Processing of Personal Information (PII)

The manner and reason for processing Personal Information (PII) must always be clear to the Data Subject. Where NEC XON is the Responsible Party, it must only Process a Data Subject's Personal Information (PII) (other than for Special Personal Information (PII)) where:

a) consent of the Data Subject (or a competent person, where the Data Subject is a Child) is obtained;

b) Processing is necessary to carry out the actions for conclusion of a contract to which a Data Subject is party;

c) Processing complies with an obligation imposed by law on NEC XON;

d) Processing protects a legitimate interest of the Data Subject; and/or

e) Processing is necessary for pursuing the legitimate interests of NEC XON or of a third party to whom the information is supplied.

7.1 Rights of the Data Subject

a) **Right to withdraw consent:** A Data Subject that has previously consented to the processing of his/her/its Personal Information (PII) has the right to withdraw such consent and must provide NEC XON with written notice. However, this will not affect the lawfulness of any processing carried out prior to the withdrawal of the consent or any processing justified by any other legal ground provided under POPIA.

If the consent is withdrawn or if there is otherwise a justified objection against the use or the processing of such Personal Information (PII), NEC XON must ensure that the Personal Information (PII) is no longer processed.

The Data Subject must provide sufficient identification to permit access to, or provide information regarding the existence, use or disclosure of the Data Subject's Personal Information (PII). Any such identifying information should only be used for the purpose of facilitating access to or information regarding the Personal Information (PII).

b) **a right of access:** a Data Subject having provided adequate proof of identity has the right to:

- request a Responsible Party to confirm whether any Personal Information (PII) is held about the Data Subject; and/or
- request from a Responsible Party, a description of the Personal Information (PII) held by the Responsible Party including information about Third Parties who have or have had access to the Personal Information (PII).

Such record or description is to be provided within a reasonable time and in a reasonable manner and in a format that is generally understandable.

c) **a right to request correction and/or deletion:** a Data Subject may also request NEC XON to –

- correct and/or update Personal Information (PII) about the Data Subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully; or
- destroy or delete a record of Personal Information (PII) about the Data Subject that NEC XON is no longer authorised to retain records in terms of POPIA's retention and restriction of records provisions.

  On receipt of such a request, NEC XON is required to, as soon as is reasonably practicable:

  - correct and / or update the information;
  - delete and / or destroy the information; and
  - provide the Data Subject with evidence in support of the information and keep a register of requests from data subjects.

The Data Subject can request in writing to review any Personal Information (PII) about the Data Subject that NEC XON holds including Personal Information (PII) that NEC XON has collected, utilised, or disclosed.

The Data Subject can challenge the accuracy or completeness of his/her/its Personal Information (PII) in NEC XON's records at any time.

7.2 Data Subject Requests

7.2.1 Personal Requester (Individual)

NEC XON will voluntarily provide the requested information or give access to any record about the Requester's Personal Information (PII), without the Requester having to pay an access fee except if the request is over burdensome in which case, this must be communicated with the requester. The prescribed fee for reproduction of the information requested will be charged as per the PAIA manual.

7.2.2 Other Requester (Legal Entity)

The Requester (other than a Personal Requester) is entitled to request access to information on third party or parties. However, NEC XON is not obliged to voluntarily grant access, and such a request may be denied. The Requester must fulfil the prerequisite requirements for access in terms of PAIA and POPIA, including identification and the payment of a request and access fee set out in the PAIA manual.

7.2.3 Third Parties

If the request pertains to a third party, the Chief Information Officer must take all reasonable steps to inform the third party of the request within 21 days of receipt of the request. The third party may within 21 days thereafter, either make representation as to why the request should be refused or grant written consent to disclosure. The third party must be advised of both the decision taken and of their right to appeal against the decision by way of application to court within 30 days after the notice.

7.2.4 Requirements for a Request

The following shall apply to all requests by any Data Subject regarding the processing by NEC XON of its Personal Information (PII):

a. Any request from the Data Subject is valid (e.g., over the telephone or face to face), if the identity of the Data Subject is not doubtful, and the request is further put in writing by the Data Subject;

b. If there is doubt about a Data Subject's identity, NEC XON may request further information or documentation to establish it;

c. NEC XON must answer the request without undue delay and within a maximum of 1 month from the receipt of the request. The response deadline may be extended for 2 additional months for complex or a high volume of requests, but the Data Subject must be informed of this within 1 month of request, together with the reasons for the delay;

d. Answers may be provided in writing, or electronically or by other means, if a request is made via electronic form, the response should be via electronic means, where possible, unless the Data Subject requests otherwise;

e. If it is decided that NEC XON must reject a request, it must inform the Data Subject without delay and at the latest within 1 month, stating the reason(s) and informing the Data Subject of its right to complain to the Chief Information Officer;

f. If a Data Subject successfully demonstrates that their Personal Information (PII) in NEC XON's records is inaccurate or incomplete, NEC XON must ensure that such Personal Information (PII) is corrected.

g. Responses to requests will be made free of charge, unless they are "manifestly unfounded or excessive", in which case NEC XON will either charge a reasonable fee or refuse to action the request; and;

h. Answers shall be provided to the Data Subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

7.2.5 Grounds for Refusal

NEC XON may in certain instances refuse access to records on the grounds set out in POPIA. The grounds, amongst others, include:

a. Mandatory protection of the privacy of a third party who is a natural person, which would involve the unreasonable disclosure of Personal Information (PII) of that natural person;

b. Mandatory protection of the commercial information of a third party;

c. Mandatory protection of confidential information of third parties if it is protected in terms of any agreement;

d. Mandatory protection of the safety of individuals and the protection of property;

e. Mandatory protection of records which would be regarded as privileged in legal proceedings;

f. The research information of NEC XON, its subsidiaries or a third party, if its disclosure would place the research at a serious disadvantage;

g. The commercial activities of NEC XON, which may include, without limitation:

- trade secrets of NEC XON
- the disclosure of financial, commercial, scientific, or technical information which could likely cause harm to the financial or commercial interests of NEC XON;
- information which, if disclosed could put NEC XON at a disadvantage in negotiations or commercial competition.

h. Requests for information that are clearly not legitimate, trivial, or nuisance, or which involve an unreasonable diversion of resources will be refused.

Employees have the responsibility to track and record requests that are processed by them to change, delete, or update Personal Information (PII). Such information must be recorded on a register and reported to NEC Corporation by the Chief Information Officer.

8) Special Personal Information (PII)

Special Personal Information (PII) as referred to in section 26 of POPIA, is sensitive Personal Information (PII) of a Data Subject and NEC XON must generally not Process Special Personal Information (PII) unless:

a) Processing is carried out in accordance with the Data Subject's consent;

b) Processing is necessary for the establishment, exercise, or defence of a right or obligation in law;

c) Processing is for historical, statistical or research purposes, subject to stipulated safeguards;

d) information has deliberately been made public by the Data Subject; or

e) specific authorisation applies in terms of POPIA.

NEC XON may not Process any Personal Information (PII) concerning a Child and will only do so where it has obtained the consent of the parent or guardian of that Child or where it is permitted to do so in accordance with applicable laws.

9) Purpose for Processing Personal Information (PII)

There should always be a legal basis for the processing of any Personal Information (PII). Processing must relate only to the purpose for and of which the Data Subject has been made aware (and where relevant, consented to) and not process any Personal Information (PII) for any other purpose(s).

Personal Information (PII) will naturally be used for the purposes required to operate and manage NEC XON's normal operations and these can include one or more of the following non-exhaustive purposes:

a) for the purposes of providing its products or services to customers and where relevant, for purposes of doing appropriate customer onboarding and credit vetting;

b) for purposes of onboarding suppliers or service providers as approved suppliers/service providers of NEC XON. For this purpose, NEC XON will also Process a service provider's/supplier's Personal Information (PII) for purposes of performing the necessary due diligence checks;

c) generally, for procurement and supply purposes;

d) for purposes of monitoring the use of NEC XON's electronic systems and online platforms by Data Subjects. NEC XON will, from time to time, engage third party service providers (who will Process the Data Subject's Personal Information (PII) on behalf of NEC XON) to facilitate this;

e) for purposes of preventing, discovering, and investigating violations of this Policy, the applicable law and other NEC XON policies;

f) in connection with the execution of payment processing functions, including payment of NEC XON's suppliers'/service providers' invoices;

g) for employment-related purposes such as recruiting staff, administering payroll, background checks, etc.;

h) in connection with internal audit purposes (i.e., ensuring that the appropriate internal controls are in place to mitigate the relevant risks, as well as to carry out any investigations where this is required);

i) for company secretarial related purposes. For this purpose, NEC XON will, from time to time, collect information relating to Data Subjects from third parties such as the Companies and Intellectual Property Commission, an agency of the Department of Trade and Industry in South Africa

j) for such other purposes to which the Data Subject may consent from time to time;

k) for such other purposes as authorised in terms of applicable law; and

l) to comply with any applicable law or any query from Government authorities, including any regulatory authority that has authority over NEC XON.

10) Keeping Personal Information (PII) Accurate

Personal Information (PII) must be kept as accurate, complete, and up to date as reasonably possible depending on the purpose for which Personal Information (PII) is collected or further processed.

11) Storage and Processing of Personal Information (PII) by NEC XON and Third Parties

Personal Information (PII) may be stored in hardcopy format and/or in electronic format using NEC XON's Information Technology infrastructure, locked cabinets, or other internally hosted technology, including Third Parties, e.g., cloud services or other technology systems, only if NEC XON has contracted with such Third Party, to support NEC XON's operations.

Such Third-Party service providers must process the Personal Information (PII) in accordance with the provisions of this Policy, all other relevant internal policies, and procedures and POPIA and employ at least the same level of security that NEC XON uses to protect the Data Subject's Personal Information (PII).

12) Retention of Personal Information (PII)

NEC XON must keep records of the Personal Information (PII), correspondence, or comments it has collected in an electronic and/or hardcopy file format.

In terms of POPIA, NEC XON must not retain Personal Information (PII) for a period longer than is necessary to achieve the purpose for which it was collected or processed and is required to delete, destroy (in such a way that it cannot be reconstructed) or de-identify the information as soon as is reasonably practicable once the purpose has been achieved. However, the maximum period for retention is 7 years. This prohibition will not apply in the following circumstances:

a) where the retention of the record is not required or authorised by law or by any Government authority;

b) NEC XON requires the record to fulfil its lawful functions or activities;

c) Retention of the record is required by a contract between the parties thereto;

d) the Data Subject (or competent person, where the Data Subject is a Child) has consented to such longer retention; or

e) the record is retained for historical, research, archival or statistical purposes provided safeguards are put in place to prevent use for any other purpose. Accordingly, NEC XON will, subject to the exceptions noted in this Policy, retain Personal Information (PII) for as long as necessary to fulfil the purposes for which that Personal Information (PII) was collected and/or as permitted or required by applicable law.

Where Personal Information (PII) is retained for longer periods for statistical, historical, legal, or research purposes, it must be archived with limited user access and appropriate safeguards that are put in place to ensure that all recorded Personal Information (PII) will continue to be processed in accordance with this Policy and applicable laws.

Once the purpose for which the Personal Information (PII) was initially collected and processed no longer applies or becomes obsolete, the Personal Information (PII) should be deleted, destroyed or de-identified sufficiently so that a person cannot re-identify such Personal Information (PII).

13) Personal Information (PII) Breach

This Policy also defines the reporting procedures which shall be taken when an incident has occurred within NEC XON that has resulted in or is believed to have resulted in a loss, alteration, or unauthorised access to, of Personal Information (PII) and to provide a framework within which NEC XON will ensure compliance with the legislative requirements of managing actual or suspected Personal Information (PII) Breach.

There is a duty upon all employees to report Personal Information (PII) Breach. All incidents affecting Personal Information (PII) that are likely to result in a risk of the rights and freedoms of data subjects must be reported to the Chief Information Officer without undue delay and as soon as reasonably possible of becoming aware of it.

13.1 Description of Personal Information (PII) Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information (PII) transmitted, stored, or otherwise processed, whether by accidental or deliberate causes.

Some examples of Personal Information (PII) Breaches can include the following:

- Access to Personal Information (PII) by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending Personal Information (PII) to an incorrect recipient.
- Information Technology equipment containing Personal Information (PII) being lost or stolen, that is believed to carry the risk of Personal Information (PII) exposure;
- Alteration of Personal Information (PII) without permission;
- Loss of availability of Personal Information (PII);
- Inappropriate access controls allowing unauthorised use, e.g., sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to Personal Information (PII) or information systems; and
- Insecure disposal of paperwork containing Personal Information (PII).

Practical examples of Personal Information (PII) Breaches that NEC XON employees should report to the Chief Information Officer include:

- I have lost a USB memory stick which I was using for my project, which holds Personal Information (PII).
- My Information Technology equipment has been stolen.
- I sent a data file to "Miss/Mrs XXXX" with Personal Information (PII) included, but it was the wrong recipient".
- I sent a letter including someone's bank details to an incorrect email address.
- I updated an employee's address and mobile number, but it was on the wrong profile.
- I printed a document which contained Personal Information (PII) and left it on my desk and now I cannot locate it.
- I lost a document which contained Personal Information (PII) in a publicly accessible location (Bus, Taxi etc.).

13.2 Reason for Reporting Personal Information (PII) Breaches

The longer a Personal Information (PII) Breach goes unreported, the harder it gets to resolve any vulnerabilities.

Impacted data subjects have a right to know that their data may have been compromised and that they could then take steps that could minimise an adverse impact on them. The incident can escalate or further incidents an occur.

Without timely reporting, NEC XON may not be able to fulfil its legal obligations.

Knowing that a Personal Information (PII) Breach has occurred and delaying reporting reduces the time available for the investigatory team to understand and assist with a response and still meet privacy compliance requirements.

Understanding the cause of Personal Information (PII) Breaches allows NEC XON to develop and implement systems and processes that are more robust to prevent future breaches and protect Personal Information (PII).

Personal Information (PII) Breaches and leakage of Personal Information (PII) can lead to severe financial penalties to NEC XON.

13.3 Procedure for Reporting a Personal Information (PII) Breach

The primary point of contact for reporting a Personal Information (PII) Breach incident is DataPrivacyIncident@nec.xon.co.za.

Responsibility for reporting a suspected or potential Personal Information (PII) Breach lies with the person who discovered the Personal Information (PII) Breach (Privacy Collaborator, nominee or any other party).

If any further information is required for investigation, the Chief Information Officer will ask you to complete the Data Breach Report form. This form should be sent via email.

The Chief Information Officer (or nominee) will investigate the suspected or potential Personal Information (PII) Breach and, where appropriate, notify the relevant person, complete the Decision Sheet for Notification Obligation, and make the decision as to whether the breach will result in a risk to a data subject's rights and freedoms.

13.4 Breach Reporting – to the Chief Information Officer

The Chief Information Officer (or nominee) must be notified of the Data Protection breach without undue delay. This can be logged by using the DataPrivacyIncident@nec.xon.co.za email address. When logging a suspected or actual breach, include as much detail as possible, such as, the time, date, and description.

All incidents must be reported to the Chief Information Officer as soon as reasonably possible, and without undue delay to individuals affected by the incident. It is vital that all employees or relevant external parties report actual or suspected Personal Information (PII) Breaches, however minor, as soon as possible after discovery, so that NEC XON can timeously establish what has happened, the size of the breach, how to resolve such a breach and whether it needs to be reported further.

Furthermore, the Chief Information Officer must and has the obligation to report all breaches to NEC Corporation.

13.5 Breach Notification

Where the Personal Information (PII) Breach, or suspected Personal Information (PII) breach, is likely to result in affecting the rights and freedoms of the;

- data subject; and
- Third party (if applicable).

The Chief Information Officer shall notify the affected data subjects, without undue delay and shall send a copy of the notification from the following email address DataPrivacyNotification@nec.xon.co.za.

13.6 Keeping the Records

The Chief Information Officer will keep documentation of all breaches including the decision sheet for notification obligation for record purposes. However, the documentation must not be retained longer than 7 years or longer than necessary for achieving the purpose for which the information was collected or subsequently processed.

14) Personal Information (PII) Impact Assessment ("PIA")

A Personal Information (PII) Impact Assessment under the POPIA regulation 4(b), describes a process designed to identify risks arising out of the processing of Personal Information (PII). It is an analysis of how personally identifiable information (PII) is collected, used, shared, and maintained and aims to minimise these risks as far and as early as possible. PIAs also support accountability by helping operators not only to comply with all the requirements, but also to demonstrate due diligence by taking appropriate actions to ensure full compliance on an ongoing basis.

PIA includes:

- describing the nature, scope, context, and purposes of the processing;
- assess necessity, proportionality, and compliance measures;
- identifies and assesses risks to data subjects; and
- identifies any additional measures to mitigate those risks.

Points to consider when undertaking a PIA assessment:

- Source of the Personal Information (PII);
- Who collected the Personal Information (PII), the method and purpose;
- Who is authorised to use the data;
- Format of the Personal Information (PII);
- Security controls during any Personal Information (PII) transfer;
- Location of the storage retention site; and
- The data disposal schedule.

To assess the level of risk, consideration should be given to both the likelihood and the severity of any impact on Data Subjects. High risk could result from either a high probability of harm, or a lower possibility of harm.

If a high risk is identified that cannot be mitigated, you must request prior authorisation from the Chief Information Officer before starting the processing.

The Chief Information Officer or the Head: Legal and Compliance must then give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, the Chief Information Officer may issue a formal warning not to process the information or ban the processing altogether.

Examples of processing	**Possible Relevant criteria**	**IS PIA likely to be required**
A company systematically monitoring its employees' activities, including the monitoring of the employees' workstation, internet activity, etc.	• Systematic monitoring. • Data concerning vulnerable data subjects.	Yes
The gathering of public social media data for generating profiles.	• Evaluation or scoring. • Data processed on a large scale. • Matching or combining of datasets.	Yes

	• Sensitive data or data of a highly personal nature.	
An institution creating a national level credit rating or fraud database.	Evaluation or scoring. • Automated decision making with legal or similar significant effect. • Prevents Data Subject from exercising a right or using a service or a contract. • Sensitive data or data of a highly personal nature.	Yes
Storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials.	• Sensitive data. • Data concerning vulnerable data subjects. • Prevents data subjects from exercising rights.	Yes
An online magazine using a mailing list to send a generic daily digest to its subscribers.	• Data processed on a large scale.	Yes
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website.	• Evaluation or scoring.	Yes

14.1 What about already processing operations?

A PIA is not needed for already processing operations that have been already checked by the Chief Information Officer and that does not present significant changes.

Conversely, this means that any data processing whose conditions of implementation (scope, purpose, Personal Information (PII) collected, identity of the operators or recipients, data retention period, technical and organisational measures, etc.) have changed since the prior checking performed by the Chief Information Officer or the Head: Legal and Compliance, and which are likely to result in a high risk should be subject to a PIA.

14.2 How to carry out a PIA

The PIA should be started prior to the processing of the Personal Information (PII) and as early as practicable in the design of the processing operation. It can also be necessary to repeat individual steps of the PIA as the development process progresses because the selection of certain technical or organisational measures may affect the risks posed by the processing.
The fact that the PIA may need to be updated once the processing has started is not a valid reason for postponing or not carrying out a PIA. In some cases, the PIA will be an on-going process, for example where a processing operation is dynamic and subject to ongoing change.

14.3 Who is obliged to carry out the PIA?

The Chief Information Officer is responsible for ensuring that the PIA is carried out only with regards to Personal Information (PII) processing under NEC XON's control (for example, employee data, clients or suppliers contact persons).

15) Cross Border Transfer

Section 72 of POPIA deals with transfers of Personal Information (PII) outside the Republic of South Africa or transborder information flows. Essentially, a responsible party may not transfer Personal Information (PII) about a Data Subject to a third party who is in a foreign country unless certain protections are in place, such as:

a. The foreign country has a law that provides adequate protection of Personal Information (PII);

b. There are binding corporate rules that provide adequate protection;

c. There is an agreement between the sender and the receiver that provides adequate protection;

d. The Data Subject consents; and

e. The transfer is necessary for the responsible party to perform in terms of a contract.

Employees should request confirmation from the Chief Information Officer and Head: Legal and Compliance prior to transferring Personal Information (PII) outside the Republic of South Africa.

16) Responsibilities

The Chief Information Officer is responsible for and will oversee the working of this Policy, which expresses NEC XON's commitment to protecting data and user privacy, the approach to data protection and its awareness of respecting the rights and freedoms of Data Subjects.
The Chief Information Officer and/or Head: Legal and Compliance, shall ensure that NEC XON complies with POPIA and other Data Protection Laws applicable including the implementation of this Policy and any other personal data protection policy(ies) within NEC XON and shall be the contact for all requests and enquiries relating to Personal Information (PII).

Business Unit and Department Heads shall undertake the responsibilities as set out in this Policy and shall

also be responsible to ensure that the personnel under their supervision follow this Policy and any other personal data protection policy(ies) as implemented by the Chief Information Officer and Head: Legal and Compliance. Such responsibilities may include, amongst others, the following:

a. Determining the purposes and methods of collection of Personal Information (PII);

b. Determining the contents of such notification to Data Subjects when collecting their Personal Information (PII) and the method of such notification;

c. Determining the collection or receipt of Personal Information (PII) from/to third parties, securing the contractual measure with the third parties to protect such information;

d. Determining the responses with the Chief Information Officer and/or Head: Legal and Compliance in the case of receiving inquiries or requests concerning disclosure, use or correction of Personal Information (PII) from Data Subjects and retention of related documents of the inquiries;

e. Establishment and maintenance of procedures that identify Personal Information (PII) in the possession of the Department or Business Unit;

f. Establishment, implementation maintenance and continuous improvement of the procedures for the protection and security of the Personal Information (PII) established in its Department/Business Unit, including the creation and maintenance of records to substantiate such procedures;

g. Reporting to the Chief Information Officer and/or Head: Legal and Compliance regarding the operation of the management of the protection of Personal Information (PII) established in its Department/Business Unit upon any request being made by the Chief Information Officer and/or Head: Legal and Compliance.

h. Assisting the Chief Information Officer and/or Head: Legal and Compliance, on Personal Information (PII) Breaches and in the implementation of educational training programs and activities for Personal Information (PII) protection for the personnel in its Department/Business Unit.

17) Non-Compliance and Reporting

Any Department or Business Unit, including individuals who are subject to this Policy and are found not to comply with the provisions as set out in this Policy or any amendment thereto, shall be subjected to appropriate disciplinary action.

If any person suspects non-compliance on or of any of the above-mentioned information, immediately consult with NEC XON's Legal and Compliance Department or the Chief Information Officer.

Protection of Personal Information (PII) Policy v5.0

Final Audit Report 2025-04-09

Created:	2025-04-04
By:	Durandt Eksteen (durandt@nec.xon.co.za)
Status:	Signed
Transaction ID:	CBJCHBCAABAAQ02sFINwM0_D2lP0LbsM_w2y0hvH7tGR

"Protection of Personal Information (PII) Policy v5.0" History

Document created by Durandt Eksteen (durandt@nec.xon.co.za)
2025-04-04 - 06:29:15 GMT- IP address: 165.49.84.152

Document e-signed by Durandt Eksteen (durandt@nec.xon.co.za)
Signature Date: 2025-04-04 - 06:32:23 GMT - Time Source: server- IP address: 165.49.84.152

Document emailed to Jitesh Ramduth (jitesh.ramduth@nec.xon.co.za) for signature
2025-04-04 - 06:32:24 GMT

Email viewed by Jitesh Ramduth (jitesh.ramduth@nec.xon.co.za)
2025-04-04 - 06:36:45 GMT- IP address: 104.47.18.126

Document e-signed by Jitesh Ramduth (jitesh.ramduth@nec.xon.co.za)
Signature Date: 2025-04-04 - 06:37:15 GMT - Time Source: server- IP address: 156.155.192.18

Document emailed to thabiet.gabier@nec.xon.co.za for signature
2025-04-04 - 06:37:17 GMT

Email viewed by thabiet.gabier@nec.xon.co.za
2025-04-04 - 07:09:18 GMT- IP address: 104.47.18.126

Signer thabiet.gabier@nec.xon.co.za entered name at signing as TGabier
2025-04-04 - 07:19:09 GMT- IP address: 105.242.70.33

Document e-signed by TGabier (thabiet.gabier@nec.xon.co.za)
Signature Date: 2025-04-04 - 07:19:11 GMT - Time Source: server- IP address: 105.242.70.33

Document emailed to Thigerson Reddy (thigerson.reddy@nec.xon.co.za) for signature
2025-04-04 - 07:19:13 GMT

Email viewed by Thigerson Reddy (thigerson.reddy@nec.xon.co.za)
2025-04-04 - 07:23:24 GMT- IP address: 196.223.192.2

Document e-signed by Thigerson Reddy (thigerson.reddy@nec.xon.co.za)
Signature Date: 2025-04-04 - 07:23:53 GMT - Time Source: server- IP address: 196.223.192.2

Document emailed to bart.vanbuynder@nec.xon.co.za for signature
2025-04-04 - 07:23:55 GMT

Email viewed by bart.vanbuynder@nec.xon.co.za
2025-04-09 - 07:25:09 GMT- IP address: 13.219.165.55

Signer bart.vanbuynder@nec.xon.co.za entered name at signing as Bart van Buynder
2025-04-09 - 07:31:25 GMT- IP address: 102.177.13.95

Document e-signed by Bart van Buynder (bart.vanbuynder@nec.xon.co.za)
Signature Date: 2025-04-09 - 07:31:27 GMT - Time Source: server- IP address: 102.177.13.95

Document emailed to carel.coetzee@nec.xon.co.za for signature
2025-04-09 - 07:31:29 GMT

Email viewed by carel.coetzee@nec.xon.co.za
2025-04-09 - 08:20:29 GMT- IP address: 41.193.225.149

Signer carel.coetzee@nec.xon.co.za entered name at signing as JC COETZEE
2025-04-09 - 08:21:17 GMT- IP address: 41.193.225.149

Document e-signed by JC COETZEE (carel.coetzee@nec.xon.co.za)
Signature Date: 2025-04-09 - 08:21:19 GMT - Time Source: server- IP address: 41.193.225.149

Agreement completed.
2025-04-09 - 08:21:19 GMT