Information Governance

STANDARD OPERATING PROCEDURE

Title	Reporting information/data breach in terms of POPIA		
SOP no	2.2.4_1.1.12_breach	**Version no**	0.001
Date of approval	18 May 2022	**Revision date**	2023

1 COMPILATION AND AUTHORISATION

Action	Designated person
Compiled by:	Amanda van der Merwe
Checked by:	POPIA Task Team
1st line authorisation	Information Management Committee
Approved by:	University Management Committee

2 DISTRIBUTION

Department/Unit	Name	Date
All staff members	Intranet/Daily Comms	3 August 2022

3 DOCUMENT HISTORY

Date	Version no	Reason for revision
2022-05-01	0.001	Compile new SOP for the process

4 PURPOSE OF THE SOP

The purpose of this SOP is to provide a procedure for the reporting of information/data breaches in terms of the POPIA and the subsequent handling thereof.

5 ABBREVIATIONS AND/OR DEFINITIONS

Abbreviation/definition	Description
SOP	Standard Operating Procedure
NWU	North-West University
POPIA TT	Protection of Personal Information Task Team of the NWU
POPIA	The Protection of Personal Information Act, 4 of 2013
PI	Personal Information
POPIA Champion	Staff members as nominated by their relevant managers
UMC	University Management Committee

Abbreviation/definition	Description
IMC	Information Management Committee
IR	Information Regulator
CRM	Corporate Relations and Marketing
Information Regulator	An individual appointed in terms of the POPIA to serve as information regulator for a certain period of time.
DIO	Deputy Information Officer

6 RESPONSIBILITIES

6.1 Information Governance Coordinator Responsibilities

6.1.1 Compile the SOP for the process as determined.

6.1.2 Provide appropriate portal for the reporting of information/data breaches in terms of POPIA, section 22.

6.1.3 Daily monitoring of the portal.

6.1.4 Scheduling of meetings to discuss the reported breaches with the POPIA task team.

6.1.5 Leading the investigation into the data/information breach.

6.1.6 Preparing the report on the data/information breach investigation and getting the approval of the POPIA task team.

6.1.7 Preparing information/data breach communication feedback to the data subject in terms of section 22 (4) and (5) of POPIA.

6.1.8 Sounding the feedback with Legal Services before providing feedback to data subjects.

6.1.9 Providing feedback to the data subjects, as well as the mitigating steps to be taken by the NWU line manager and relevant POPIA champions where the breach occurred.

6.1.10 Conducting follow-ups to ensure the mitigating steps have been put in place.

6.1.11 Preparing the information/data breach notice to the IR for signature of the DIO.

6.1.12 Informing the IR of the data/information breach.

6.1.13 Discussing the possible reputational damage with CRM and resolving on possible external/internal communication.

6.1.14 Reporting to the IMC on information/data breaches of PI.

6.1.15 Keep a register of information breaches.

6.2 POPIA Task Team

6.2.1 Examine and discuss the reported information/data breach of PI.

6.2.2 Provide expert advice and guidance to the IGC on the investigation.

6.2.3 Approving the final data/information breach of PI report.

6.3 Legal Services

6.3.1 Providing legal advice in regard to the information/data breach of PI as part of the POPIA TT.

6.3.2 Ensuring the feedback to be provided to the data subjects is legally sound.

6.4 CRM

6.4.1 Providing expert advice on possible reputation damage caused by the information/data breach.

6.4.2 Providing suitable communication to limit the extent of the damage that might have been caused by the breach in order to ensure re-establishing data subject trust.

7 PROCEDURE

7.1 Data breach reporting by a staff member, member of student leadership, students and/or external stakeholder of the NWU

When a staff member or a member of the NWU student leadership becomes aware of a data breach. The individual must follow the undermentioned procedure.

7.1.1 Reporting the data breach to the NWU POPIA task team

The staff member/member of student leadership must immediately after becoming aware of any data breach, report the data breach to the POPIA task team of the NWU, by completing the forms (paper/electronic/webform) that will be made available for this purpose.

7.1.2 Receiving the report of a data breach (POPIA task team)

- As soon As the report as contemplated in 7.1.1 is received, the POPIA task team must acknowledge receipt to the individual reporting the data breach and inform the individual that the necessary investigation will be concluded.
- The POPIA Task team must also inform all data subjects that a data breach has been reported and that an investigation is being conducted into the matter.
- The POPIA task team must inform the Information Management Committee, the Deputy Information Officer(s) as well as the Information Officer that a data breach was reported, and that the breach is being investigated.

7.1.3 Investigating the data breach

- The POPIA task team must allocate staff members 2 a multidisciplinary task team/response team to investigate the data breach concerned. This team may include staff members/student leadership from the undermentioned:
  - POPIA task team
  - Legal Services
  - The office where the breach has originated
  - Information Technology
- A multidisciplinary task team/response team, must, as soon as possible investigate the data breach and provide a report including recommendations, solutions and the response to the data breach to the Deputy Information Officer(s) and Information Officer.
- This report must include the following:
  - Background and information of the data breach
  - Investigation and facts relating to the investigation
  - Findings of the investigation
  - Remedies and recommendations
  - Communication to be provided to all stakeholders
- The Deputy Information Officer(s) and Information Officer must consider the report from the multidisciplinary task team and recommend possible amendments to the response to the data breach. These officials must also approve the response and subsequent communication to the relevant stakeholders.

7.1.4 Feedback of the data breach

- Upon approval, the POPIA task team, mast, on behalf of the Deputy Information Officer(s) and Information Officer compile and finalise the response to the data breach to the individual who reported the data breach, all affected data subjects, as well as report the matter to the Information Management Committee for noting.
- After feedback the data breach must be reported to the Information Regulator as contemplated in paragraph 7.4

7.1.5 Records Management of records relating to the data breach

All records related to the reporting, investigation and feedback, must be retained in safe and secure storage by the POPIA task team for a period of five (5) years after the finalisation of the data breach, whereafter it must be destroyed by means of the approved destruction process of the NWU.

Minimal information may be kept for statistical purposes only.

8 REFERENCE DOCUMENTS

- NWU Information Security Policy
- NWU Information Governance Framework
- Protection of Personal Information Act, 4 of 2013
- NWU Personal Information Privacy Policy

9 Addenda

No	Document name

Original details: (11664754) P:\1. Governance\Standard Operating Procedure - Data breach.docm
1 August 2022

File reference: 2.2.4_1.1.12_breach