INCIDENT RESPONSE AND DATA BREACH POLICY

DATED: 01 July 2021

DOCUMENT NUMBER: HRM_094

DEADLINE FOR NEXT REVIEW: 31 December 2021

T · +27 21 702 2884 26 Bell Close, Westlake Business Park
F · +27 86 555 0693 Westlake 7945, Cape Town
NCC Environmental Services (Pty) Ltd | Reg No: 2007/023691/07 | VAT No. 4450208915

THIS POLICY FORMS AN INTEGRAL PART OF THE OVERALL PRIVACY POLICY OF NCC ENVIRONMENTAL SERVICES (PTY) LTD.

1. PURPOSE OF THIS POLICY

The purpose of this policy is to set out the processes and procedures that **NCC Environmental Services (Pty) Ltd ("the Company")** must put in place to effectively report and respond to Incidents and Data Breaches.

This document applies to all employees of the Company, who must familiarise themselves with the content of this document.

Dean Ferreira is the Information Officer of the Company with the overall responsibility of ensuring day-to-day implementation and adherence to this policy, as well as other policies relating to the **Protection of Personal Information Act 4 of 2013, as amended from time to time ("POPIA").**

2. EFFECTIVE DATE

The effective date of this policy is 1 July 2021.

3. DEFINITIONS

3.1. **Data Breach:** A type of Incident where Personal Information is accidentally or unlawfully accessed, viewed and/or retrieved or otherwise processed as defined in POPIA, leading to it, among others, being destroyed, lost, stolen, or used by cyber attackers without authorisation.

3.2. **Data Subject:** The individual or juristic person whose personal information is being processed.

3.3. **Incident:** An incident is an event that takes place that compromises the Company's systems or data. It allows a person or persons to get unlawful and unauthorised access to Personal Information.

3.4. **Incident Response:** A coordinated approach to prepare for, identify, confirm, report, escalate, respond to, contain, evaluate, and recover from a Data Breach.

3.5. **Information Officer:** The person in a business who is responsible for compliance with POPIA, as defined in POPIA itself and the **Promotion of Access to Information Act 2 of 2000 ("PAIA")**, as amended from time to time.

3.6. **Information Regulator:** The juristic person responsible for, among others, enforcing compliance with POPIA and PAIA.

3.7. **Personal Information:** Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, and as more comprehensively defined in POPIA.

3.8. **Responsible Party:** 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.

4. PREPARING FOR AN INCIDENT OR DATA BREACH

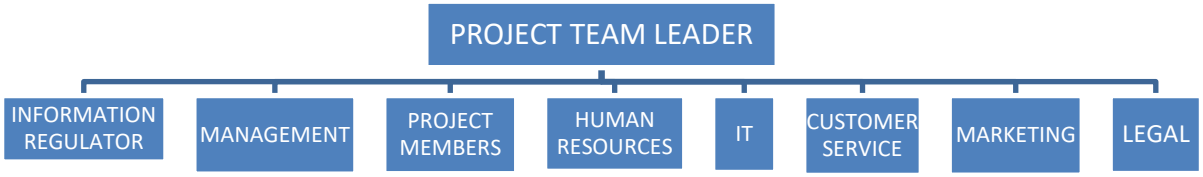
4.1. IDENTIFY THE DIFFERENT INCIDENTS MOST LIKELY TO AFFECT YOUR BUSINESS

Examples of Incidents:

- **Phishing:** A cybercrime where attackers attempt to obtain sensitive information or data, e.g.
  - **E-mail phishing**, usually sent to large groups, where attackers impersonate banks or other legitimate companies.
  - **Spear phishing**, usually targeted towards a specific person or business.
  - **Clone phishing,** where an e-mail is recreated and sent from an address nearly the same as that of the original sender.
  - **Whale phishing**, where CEO's or COO's are targeted.
  - **Pop-up phishing**, where attackers use pop-up adds to install malware in computers.
- **Malware:** Software that is specifically designed to disrupt, damage or gain unauthorized access to a computer system, e.g. viruses, worms, bots, trojan horses.

- **Insider threat:** Threats that come from someone within a business, or with legitimate access to IT systems, e.g. disgruntled or former employees, contractors, partners.
- **Hackers:** Attackers look for vulnerabilities in a business's infrastructure, such as open networks or outdated software.
- **Ransomware:** Attackers encrypt a business's data and demand a ransom to restore access to it.
- **Password guessing:** Attackers repeatedly guess passwords until they get access to the system. For this reason, strong passwords are always recommended. A strong password contains uppercase and lowercase letters, numbers, and special characters. It should not contain any personal information.

4.2. PUT A RESPONSE PROJECT TEAM IN PLACE



- **Project Team Leader:** Ideally, this should be the Information Officer, whose main responsibility is to oversee overall compliance with POPIA and to ensure that:
  - a compliance framework is developed, implemented, monitored and maintained.
  - a personal information impact assessment/gap analysis is done to ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of personal information.
  - a manual is developed, monitored, maintained, and made available as prescribed in sections 14 and 51 of PAIA.
  - internal measures are developed together with adequate systems to process requests for information or access thereto; and
  - internal awareness sessions are conducted regarding the provisions of POPIA, regulations made in terms of the POPIA, codes of conduct, or information obtained from the Information Regulator.

- Information Officers may only take up their duties in terms of POPIA after the Responsible Party has registered them with the Information Regulator.

- **The Project Team Leader works closely with:**
  - **Information Regulator:** To establish a relationship with the Information Regulator and prepare an efficient notification process in the event of a data breach.
    To work with the Regulator in relation to investigations conducted.
  - **Management:** To keep executive management, the board of directors and shareholders informed.
  - **Project Members:** To collaborate with different internal and external parties to ensure all tasks are completed on time.
  - **HR:** To develop awareness campaigns, internal communications, as well as employee training (in conjunction with the IT department) and to assist in the event of personal data breaches.
  - **IT:** To identify the security risks most likely to affect the business, to train employees (in conjunction with HR), to identify compromised data, to recover compromised data and to take all necessary steps to prevent further loss.
  - **Marketing :** To ensure there is a well-documented plan in place to develop and get approval for internal and external communication, to determine the best communication and notification strategies in the case of an Incident or Data Breach, e.g. through printed media, the company's existing website, a new website and/or social media, to respond to press coverage during and after a Data Breach, to ensure all relevant people are informed, i.e. affected Data Subjects, the Information Regulator, customers, employees, management, shareholders and business partners.
  - **External attorneys:** To build relationships with legal advisers and/or external attorneys for a better understanding of POPIA and its impact on the business, and to obtain sign-off on all material that will be distributed and to ensure the correct use of "private and confidential" on this material, to ensure relevant contracts are updated to include reference to POPIA.

4.3. INSURANCE POLICIES

Obtain insurance cover for data breaches. Use a broker that is an expert in the field of cyber insurance and data privacy.

4.4. INTERNATIONAL BREACHES

In the event of transborder information flows, comply with the relevant sections of POPIA.

5. RESPONDING TO AN INCIDENT AND REPORTING A DATA BREACH

5.1. DETECTING AN INCIDENT

- Speak to those involved with discovering the Incident and everyone else who may know about it to determine whether there is a potential breach:
    - Identity the person/s who discovered the Incident, as well as the date and time that it was discovered
    - The person who reported the Incident, if not the same as the person who discovered the incident
    - To whom they reported the Incident
    - Everyone who knows about the Incident
    - The type of Incident that occurred

- In the event of a Data Breach, determine and document the following:
    - The type of personal information affected, e.g. names, e-mail addresses, account information.
    - The number of records affected.
    - The type of breach, e.g. whether it was internal or external, and due to an accident or malicious intent.
    - When (date and time) the Response Project Team was informed of the breach.

5.2. INITIATING THE DATA BREACH RESPONSE PLAN

- Inform everyone in the Response Project Team.
- Inform the Information Regulator and the Data Subjects involved in the breach.
- Work with the IT Team to contain the Data Breach, to take the necessary precautions to secure the area where the Data Breach occurred, not to disturb or contaminate evidence, and to prevent any further data loss.
- Notify all the other relevant stakeholders (management, HR, Legal, Marketing) and provide a report including all the facts about the Data Breach (time of discovery, actions already taken, next actions, risks) and keep them informed and where necessary involved in the Data Breach Response Plan.
- Determine if the Data Breach will have any impact on upcoming projects and how to address any areas of concern.

5.3. EVALUATING THE DATA BREACH RESPONSE PLAN

Determine continuously how effective the process is being handled so that improvements can be made where necessary.

5.4. PREVENTING REPUTATIONAL RISK

- Marketing (brand marketing) is to formulate communication to the public to prevent any reputational risk to our brand. Communication must be open and clear and must include the steps that have been taken to prevent a future Data Breach.
- Immediately after a Data Breach was discovered and confirmed, the Information Regulator, as well as the Data Subjects involved in the Data Breach should be notified.
- Decide on the best channels to use for communication, e.g. to publish it on our website, to release a media statement, to make use of social media, or a combination of the different channels.
- Ensure all employees are aware of the communication protocol – this should form part of our training.

6. ESCALATING AN INCIDENT OR DATA BREACH

- The company should have internal and external escalation processes in place.
- For internal escalation, the Incident Investigation Form should be used where a possible Incident or Data Breach has been detected, the person reporting the incident should complete the form and alert the Information Officer, or head of IT, depending on the established protocol.
- For an external escalation, it is important to determine before a Data Breach when and how to escalate an Incident to external parties.

7. PRACTICING THE DATA BREACH RESPONSE PLAN

If possible, simulate a Data Breach and follow all the processes and procedures put in place in the event of a real Data Breach. This should be done regularly to ensure everyone in the company is comfortable and familiar with the process, but also to make updates and improvements to the Data Breach Response Plan.

REVIEWED AND APPROVED BY:

Dean Ferreira

Managing Director – NCC Environmental Services (Pty) Ltd