ROKWIL GROUP
www.rokwil.com
+27 (0)31 003 0896
9 Old Main Road, Kloof, 3610

BREACH OF PERSONAL DATA

INCIDENT RESPONSE PLAN

ROKWIL (PTY) LTD

CONTENTS

1. INTRODUCTION

Organisations of all sizes and across all industry sectors are becoming targets of cyber criminals. Attacks are becoming more frequent, more sophisticated and with dire consequences to the company's finances and reputation.

A data breach, whether from a cyber intrusion or the loss of a device, can be a challenge for any organisation.

2. INCIDENT RESPONSE PLAN

The Incident Response Plan (the Plan) identifies and describes the roles and responsibilities of the Incident Response Team (the Team) and the quick and effective actions to be taken to identify and mitigate a breach of personal and/or confidential data.

3. INCIDENT RESPONSE TEAM

The roles and responsibilities of the Incident Response Team (the Team) are as follows:

3.1 Data Security Officer (internal)

- Provide relevant training to departmental/site administrators
- Determine the nature and extent of the incident
- Note date and time of detection of incident
- Contact the IT Support representative for advice as needed
- Inform members of the Team and other relevant parties about the incident
- Determine which member/s of the Team must investigate the incident
- Identify if any other individuals need be involved
- Co-ordinate and monitor progress of the investigation
- Keep the Information Officer updated on the nature of the incident any subsequent action taken
- Prepare a written report of the incident and corrective action taken
- Conduct a de-brief of relevant parties if deemed appropriate

3.2 IT Support (external)

- Provide relevant IT advice and assistance to the Team
- Secure the area where data breach has occurred
- Stop additional data loss by de-activating network
- Thoroughly investigate the incident
- Take necessary steps to mitigate the incident
- Checks for signs of a firewall breach
- Take action necessary to block traffic from suspected intruder/hacker
- Identify steps to be put in place to prevent a recurrence of the incident
- Submit a comprehensive report of the incident to the Team

3.3 HR Representative (internal)

- Contact with affected data subjects
- Provide ongoing support and reassurance to affected data subject/s
- Assist other members of the Team where appropriate
- Review and update privacy policy and procedures

3.4 Information Officer (internal)

- Keep CEO updated on incident
- Notify law enforcement if necessary
- Notify the Information Regulator of the incident
- Address all media queries

4. CATEGORISATION OF BREACHES OF PRIVACY

Types of breaches of personal data include, but are not limited to, the following:

4.1 Breach of Personal Information

Personal information includes any information that can be linked to, or identify, an individual, eg ID documents, bank details, medical records, etc. A full list of the types of personal information can be found in the Company's PAIA Manual on the website.

Personal information may only be accessed by the company for business purposes and all personal information and documents must be securely stored, either electronically or archived, at all times.

4.2 Firewall Breach

The company's policy on

4.3 Virus Outbreak

Info

5. PROCEDURE TO MANAGE A BREACH OF PRIVACY

5.1 Detection and Identification

- Determine the nature and extent of the incident (Data Security Officer)
- Note date and time of detection of incident (Data Security Officer)
- Inform members of the Team and other relevant parties about the incident (Data Security Officer)
- Determine which member/s of the Team must investigate the incident (Response Team)
- Identify if any other individuals need be involved (Response Team)
- Contact the IT Support representative for advice as needed (Data Security Officer)
- Secure the area where data breach has occurred (Data Security Officer / IT Support)
- Stop additional data loss by de-activating network (IT Support)
- Checks for signs of a firewall breach (IT Support)

- Take action necessary to block traffic from suspected intruder/hacker
- Take all necessary steps to mitigate the incident

5.2 Investigation

- Relevant individuals undertake thorough investigation (Data Security Officer *et al*)
- Identify and question any witnesses (Investigation Team)
- Contact affected data subjects and provide ongoing support and reassurance (HR Officer)
- Co-ordinate and monitor progress of the investigation (Data Security Officer)
- Keep the Information Officer updated on the nature of the incident any subsequent action taken (Data Security Officer)
- Notify CEO and Management of the incident (Information Officer)

5.3 Corrective Action

- Identify steps to be put in place to prevent a recurrence of the incident
- Conduct a de-brief of relevant parties if deemed appropriate

5.4 Post-Incident Feedback

- Compile a comprehensive report of the incident (Data Security Officer / IT Support)
- Submit report of the incident and corrective action taken to the Team (Data Security Officer)
- Update CEO and Management of the incident (Information Officer)
- Notify law enforcement if necessary (Information Officer)
- Address all media queries (Information Officer)
- Review and update privacy policy and procedures (HR Officer)

This Incident Response Plan will be reviewed and updated on a regular basis.