Power Truck Hire (Pty) Ltd

T/A POWER TRUCK HIRE (PTY) LTD

REGISTRATION NUMBER: 1986/000900/07

SECURITY INCIDENT NOTIFICATION AND REPORTING POLICY

REGULATION 4

PROTECTION OF PERSONAL INFORMATION ACT 2013

1. Security Incidents

A Security Incident is defined as any action or event in contravention of the provisions of this Information Security Policy.

2. Notification of a Security Incident

Once a Security Incident is confirmed, the Information Officer should take the following steps as a matter of urgency:

a. The Information Officer should act immediately. Power Truck Hire (Pty) Ltd may disable accounts without notice, regardless of whether the account itself is suspected of having been misused.
b. If the Security Incident involves a possible breach of the Act, then the Information Officer will notify the Information Regulator and the Data Subject as soon as is practicable.
c. If another department of Power Truck Hire (Pty) Ltd is involved, then that department should be notified as soon as possible, preferably via the Information Officer.
d. If an organisation or person external to Power Truck Hire (Pty) Ltd is involved in any capacity, then the Information Regulator and the Data Subject need to be contacted.
e. If an organisation or person external to Power Truck Hire (Pty) Ltd is involved as a potential victim, then that organisation or person should be advised as soon as possible.

3. Reporting a Security Incident

A Report of the Security Incident should be prepared for the Information Officer. Once approved, the Report should be submitted to the relevant Information Officer outlining the following details (where possible):

- General nature of the Security Incident;
- General classification of people involved in the Security Incident (such as external client, privileged Staff Member);
- Computer systems involved in the Security Incident;
- Details of the Security Incident;
- Impact of the Security Incident;
- Possible courses of action to prevent a repetition of the Security Incident.

Where appropriate, the relevant Information Officer should undertake remedial action on the basis of this Report. Where a significant IT risk is identified the Information Officer is responsible for undertaking a risk assessment as part of Power Truck Hire (Pty) Ltd's Risk Management Plan.

4. Unauthorised Access Attempts

All unauthorised access attempts must be logged. The Audit Trail/System Access Log must be reviewed regularly, exception Reports generated and inspected by the System Administrator and appropriate action taken. A copy of the Report of unauthorised access attempts must be produced and kept for future reference.

5. Information Security Responsibilities

5.1 Information Officer

The Information Officer is responsible for:

- Providing appropriate security of Power Truck Hire (Pty) Ltd's central information technology facilities including ensuring relevant security standards and responsibilities are delegated, developed and implemented;
- Providing oversight of IT security across Power Truck Hire (Pty) Ltd;
- Providing specialist Information Security advice to the Officials of Power Truck Hire (Pty) Ltd;
- Receiving Reports of incidents, threats and malfunction that may have an impact on Power Truck Hire (Pty) Ltd's Information Systems;
- Ensuring remedial action is taken on all reported security breaches;
- Acting as Power Truck Hire (Pty) Ltd's representative on external bodies, including law enforcement agencies, on matters relating to IT security;
- Implementing disciplinary action for inappropriate use as delegated by the relevant Responsible Party Policies.

5.2 Manager: Cyber Security

The Manager: Cyber Security is responsible for managing Information Security Standards, Procedures and Controls intended to minimise the risk of loss, damage or misuse of Power Truck Hire (Pty) Ltd's information technology resources. More specifically, the Manager: Cyber Security's responsibilities include:

- Developing and maintaining Power Truck Hire (Pty) Ltd's Information Security Policy;
- Establishing and maintaining high-level standards and related Procedures for access to Power Truck Hire (Pty) Ltd's information and systems;
- Selecting, implementing and administering Controls and Procedures to manage information security risks;
- Distributing Security Report Information in a timely manner to the Information Officer and other appropriate Responsible Party administrators;
- Liaising with external security authorities; and
- Promoting security awareness within the broader Responsible Party community.

6. System Owners

System Owners have the authority to make decisions related to the development, maintenance, operation of and access to the application and Personal Information associated with that business activity. More specifically, the System Owner's responsibilities include:

- Interpreting relevant Laws and Responsible Party Policies to classify data and define its level of sensitivity;
- Defining required levels of security, including those for Personal Information transmission;
- Developing guidelines for requesting access;
- Reviewing and authorising access requests;
- Establishing measures to ensure Personal Information integrity for access to Personal Information;
- Reviewing access by users with critical roles particularly when segregation of duties cannot be implemented;
- Reviewing usage information;
- Defining criteria for archiving data, to satisfy retention requirements;
- Developing and testing business continuity plans.

7. System Administrators

A System Administrator must take reasonable action to assure the authorised use and security of Personal Information during storage, transmission and use. A System Administrator is responsible for:

- Developing, maintaining and documenting Operational Procedures to include Personal Information integrity, authentication, recovery, and continuity of operations;
- Ensuring that access to Personal Information and applications is secured as defined by the System Owner;
- Providing adequate Operational Controls to ensure Personal Information protection;
- Ensuring that access requests are authorised;
- Modifying access when Employees terminate or transfer;
- Communicating appropriate use and consequences of misuse to users who access the System;
- Protecting Confidential Files and Access Control Files from unauthorised activity;
- Performing day to day security administration;
- Taking remedial action in respect of all audit findings and reported security breaches;
- Maintaining access and audit records;
- Creating, distributing and following up on security violation reports;
- Developing and testing Disaster Recovery Plans.

System Administrators should be properly trained in all aspects of System Security.

8. Information Officer

An Information Officer is responsible for ensuring that the Security Policy is implemented within their area of responsibility. These duties may be delegated; however, it is the responsibility of the Information Officer (or equivalent) to:

- Ensure that Employees understand Security Policies, Procedures and responsibilities;
- Approve appropriate Personal Information access;
- Review, evaluate and respond to all security violations reported against staff and students and take appropriate action;
- Communicate to appropriate Responsible Party areas on Employee departures and changes affect computer access.

9. Responsible Party's Internal Audit Office

Assurance Services is responsible for providing an independent assessment on the adequacy of security procedures within the IT infrastructure and Information Systems.

Assurance Services is also responsible for evaluating the Information Security Policy and Procedures Compliance during regular operational audits of Power Truck Hire (Pty) Ltd's Information Systems.

10. Users

Users of Power Truck Hire (Pty) Ltd's Information Technology Resources are responsible for:

- Keeping their password secure and ensuring it is not shared with any other user;
- Ensuring the security of their workstation by logging off or locking it when it is left unattended;
- Ensuring the safe keeping of Personal Information within their own area of work within any systems they have been granted access to;
- Storing and labelling Personal Information appropriately;
- Reporting Security Incidents or problems as soon as possible to the IT Help Desk.

11. Compliance

Power Truck Hire (Pty) Ltd considers any Breach of Security to be a serious offence and reserves the Right to copy and examine files or information resident on or transmitted via Power Truck Hire (Pty) Ltd's information technology resources.

Information Strategy and Technology Services may confiscate computer equipment; temporarily remove material from websites or close any account that is endangering the running of the System or that is being reviewed for inappropriate or illegal use.

12. Awareness and Communication

It is essential that all aspects of Information Security, including confidentiality, privacy and procedures relating to System Access, are incorporated into formal staff induction procedures and conveyed to existing staff on a regular basis.

Each Employee, on commencement of employment, should be made aware that they must not divulge any Personal Information that they may have access to in the normal course of their employment. Staff must also be made aware that they should not seek access to Personal Information that is not required as part of their normal duties.

13. Changes to this Policy

Power Truck Hire (Pty) Ltd reserves the Right to amend, alter and terminate this Policy at any time.

INFORMATION OFFICER DETAILS

Name: Arnold Michael Friedman
Tel: (011) 769-1288
Cell:
Physical Address: 97 Albertina Sisulu Drive
Industria
Johannesburg
2093

Date: 18 October 2021
Email:
Website: www.powertruckhire.co.za
Postal Address: P.O. Box 2489
KRUGERSDORP
1740