Power Truck Hire (Pty) Ltd

T/A POWER TRUCK HIRE (PTY) LTD

REGISTRATION NUMBER: 1986/000900/07

INFORMATION SECURITY POLICY

(PERSONAL INFORMATION PROTECTION POLICY)

Last Updated:	
Date of Review:	

PURPOSE AND SCOPE

The purpose of this Policy is to ensure that Power Truck Hire (Pty) Ltd's Information Systems are recognised as a valuable asset and are managed accordingly to ensure their integrity, security and availability. This Policy applies to all users of Power Truck Hire (Pty) Ltd's Information Systems, including those who install, develop, maintain, and administer those Information Systems.

The Purpose of this Policy is to ensure:

- The provision of reliable and uninterrupted Information Systems;
- The integrity and validity of Personal Information contained in Information Systems;
- An ability to recover effectively and efficiently from disruption to Information Systems;
- The protection of Power Truck Hire (Pty) Ltd's IT assets including information, software and hardware.

Within this Policy, information assets (e.g. databases, files); software assets (e.g. applications and systems software and development tools); and hardware assets (e.g. computers, communications equipment and magnetic media) refer to those assets which taken together comprise Power Truck Hire (Pty) Ltd's Information Systems.

RISK ASSESSMENT

Power Truck Hire (Pty) Ltd will carry our regular risk assessments of its Information Systems using Power Truck Hire (Pty) Ltd's risk management procedures. These risk assessments will examine potential vulnerabilities and security measures and will lead to the development of controls consistent with reducing the identified risk to an acceptable level.

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

ACCESS MANAGEMENT

All users must be authorised to access Power Truck Hire (Pty) Ltd's Information Systems by the relevant System Owner. Access is controlled and monitored in accordance with Power Truck Hire (Pty) Ltd's Policy.

- **Authentication and Identification**
  - All Power Truck Hire (Pty) Ltd Information System users are granted a unique ID used for authentication into Power Truck Hire (Pty) Ltd Information System
  - To validate identity, each unique ID is secured with a password, pin, or equivalent mechanism to ensure authentication. Relevant approved security standards apply.
  - These unique IDs and security mechanisms are not to be shared
  - In special circumstances, temporary generic accounts may be approved by the Information Officer or delegate. These temporary accounts, should have an expiration date

- **Authorization and Account Management**
  - Access is granted by means of a computer account (see above), which also serves as identification
  - Only those users who have valid reasons (as determined by System Owners) for accessing Power Truck Hire (Pty) Ltd's Information Systems are granted access privileges appropriate to their requirements
  - Users who have access to multiple critical roles (where segregation is not enforced), should have their use regularly reviewed to ensure their use is appropriate. Particular focus should be given to the use of these roles in periods where that level of access may not be required.
  - All System Owners must regularly review their schedule of delegated authority, to determine who is authorised to use the system and their level of authorization
  - At a minimum, an annual review of all system access levels of users should be carried out.
  - System Owners should ensure any non-compliance as a result of this activity is addressed as a matter of priority. All records of non-compliance must be kept until all matters arising from non-compliance have been resolved.

- **Privileged Users**
  - System administrators have high-level access rights, enabling them to access any data stored on Power Truck Hire (Pty) Ltd's Information Systems.

- **Contractor and Third-Party access**
  - Contractor and Third-Party access are permitted only if agreed to by the System Owner. These parties must comply with the Power Truck Hire (Pty) Ltd Access Control Standards
  - If temporary accounts are issued, these should have an expiration date based on contract completion date.
- **Information Systems Operated by Third Parties**
  - Information Systems and resources operated by Third Parties must ensure they comply with the applicable Information Security and Acceptable Use Policies applying to those systems and resources, ensuring PoPI compliance.

ASSET SECURITY MANAGEMENT

All major Information Systems must have a nominated owner who is responsible for the implementation and management of this Policy in relation to those assets.

- **Servers and Systems Backup**
  - All critical Power Truck Hire (Pty) Ltd's information should be stored on appropriate storage media with an appropriate access and backup policy in place.
  - Frequency of backup is determined by the frequency with which the Personal Information changes and the effort required to recreate the Personal Information if lost. Standards apply to the backup of data from all Responsible Party systems.
  - All Personal Information must be stored with an appropriate level of encryption/security to prevent unauthorized access to the Personal Information. For example:
    - Full disk encryption (with appropriate authentication)
    - Container/folder encryption
    - Public/private key encryption
  - Any Personal Information stored outside of South Africa (E.g. Cloud storage solutions, like Dropbox or OneDrive, with servers outside of South Africa), required prior approval/permission from the Data Subject
  - If any Personal Information that is stored in other locations (eg. on other servers, desktops, laptops and other mobile devices outside of Power Truck Hire (Pty) Ltd) becomes the responsibility of the user to ensure it is stored securely and backed up on a regular basis.

- **Recovery**
  - System Administrators must document all restore procedures and test these on a regular basis, at least annually, to ensure recovery of data and Personal Information is possible.
  - Backup media must be retrievable within 24 hours, 365 days a year. Standards apply to the recovery of data from all Power Truck Hire (Pty) Ltd Systems.

- **Off-Site Storage (Backup Media)**
  - Off-site storage locations must provide evidence of adequate fire and theft protection and environmental controls.
    - Any Personal Information stored outside of South Africa (E.g. Cloud storage solutions, like Dropbox or OneDrive, with servers outside of South Africa), required prior approval/permission from the Data Subject.
  - A formal Service Level Agreement (SLA) must exist with the off-site storage provider
  - A site visit should be undertaken on an annual basis, if possible.

- **Personal Information Retention**
  - Owners of Power Truck Hire (Pty) Ltd's Personal Information are responsible for defining and documenting the length of time the Personal Information must be retained. The retention period, legal requirements, responsible parties, and source of legal requirement should be specified.
  - System Administrators are responsible for ensuring that these documented requirements are adhered to.

- **Business Continuity and Disaster Recovery**
  - As part of Power Truck Hire (Pty) Ltd's Risk Management Framework, Business Continuity and Disaster Recovery Plans should be prepared and tested for all of Power Truck Hire (Pty) Ltd's major Systems.
  - The testing strategy to be implemented will be influenced by the importance of the system to Power Truck Hire (Pty) Ltd's business operations and the ability to recover the system within agreed timeframes.

- **Physical Security**
  - Access to secure areas, including computer rooms, network equipment rooms and any associated service facilities, is restricted to authorised Responsible Party staff.

- **Network Security**
  - All wiring/cabinets/physical infrustructure must be secured and/or monitored to prevent any damage and to stop unauthorised attempts to connect to the network to obtain Personal Information or network resources.
  - All networks/network points (E.g. WiFi networks, WiFi access points, ethernet connections) should be adequately protected/secured to prevent unauthorized attempts at accessing Personal Information or network resources.
  - Adequate network defense/Firewall (hardware and/or software) should be in place to prevent/log/monitor unauthorized attempts at accessing Personal Information or network resources.

- **Information Classification**
  - Information assets are classified into four categories: Public, Internal, Confidential and Restricted. All major Information Assets must have a nominated owner who is responsible for establishing authentication and authorisation procedures commensurate with these categories noting that:
  - **Public information** can generally be made available or distributed to the general public. This is information which does not require protection and when used as intended would have little to no adverse effect on the operations, assets or reputation of Power Truck Hire (Pty) Ltd or Power Truck Hire (Pty) Ltd's obligations concerning information privacy.
    An Example of Public Information includes:
    - Power Truck Hire (Pty) Ltd marketing or promotional information
  - **Internal information** is for general internal Power Truck Hire (Pty) Ltd use only and not for external distribution (internal information may be accessed by authorised staff).
    Examples of Internal Information include:
    - Non-public Responsible Party Policies
    - De-identified Personal Information sets including for instance research methodologies
  - **Confidential Information** is for internal use only with access only by staff who require it in the course of performing their Power Truck Hire (Pty) Ltd responsibilities.
    Examples of Confidential Information include:
    - Procurement documentation
    - Commercial contracts
    - Financial and billing information
    - Intellectual property
    - Information and physical security logs
    - Personally identifiable sensitive information
    - Credit/debit card details
    - Disciplinary information
    - Individual salary information
    - Performance Management evaluations
    - Commercially sensitive research
    - Commercially sensitive audit reports.
    - Critical infrastructure information (physical plant detail, IT systems information, system passwords, information security plans, etc.)
    - Restricted information which is to be kept strictly confidential with access on a strictly "needs to know" basis. Examples include information affecting national interests and/or national security.
  - Staff should be aware of their legal and corporate responsibilities concerning inappropriate use, sharing or releasing of information to another party. Any Third Party receiving Confidential or Restricted Information must be authorised to do so and that individual or their organisation should have adopted Information Security Measures, which guarantee confidentiality and integrity of that Personal Information.

- **Information Labelling**
  - Wherever practicable information assets should be labelled as follows:

Classification	Labelling
Public	Non required
Internal	None required
Confidential	X-in-Confidence (where X = one of Security, Staff, Commercial, Medical, Legal, Council)
Restricted	Restricted

- **Handling and Distribution of Information Assets**
  - The following restrictions apply to the handling of Personal Information assets.

Public Information

- There are no specific restrictions on the distribution or handling of Public Information, although Power Truck Hire (Pty) Ltd Personnel must respect all Copyright, Trademark and Intellectual Property Rights of any Personal Information that they distribute.

Internal Information

- Internal Information is considered non-public and should be protected from unnecessary exposure to parties outside of Power Truck Hire (Pty) Ltd.
- **Access:** Responsible Party Employees, or Non-Employees with signed Non-Disclosure Agreements, who have a legitimate business or academic need to know.
- **Distribution within Power Truck Hire (Pty) Ltd:** Information can be shared via the web, but the user must provide Power Truck Hire (Pty) Ltd authentication.
- Electronic and hard copy information can be circulated on a need-to-know basis to Power Truck Hire (Pty) Ltd members subject to applicable laws (e.g. copyright) and Power Truck Hire (Pty) Ltd Policies.
- Internal Information may be accessed remotely and via disk-encrypted portable and mobile devices without further encryption
- **Distribution outside of Power Truck Hire (Pty) Ltd:** Information can be sent in unencrypted format via Power Truck Hire (Pty) Ltd email to external parties on a need to know basis. Information can be shared using Power Truck Hire (Pty) Ltd IT facilities e.g. OneDrive, SharePoint, shared file servers.
- Information can be circulated via Power Truck Hire (Pty) Ltd internal email system.
- **Storage:** Must be stored using Power Truck Hire (Pty) Ltd provided facilities.
- **Disposal/Destruction:** Electronic data should be securely and reliably erased or media physically destroyed.

- **Confidential Information**
  - Confidential Information should be protected to prevent unauthorised access or exposure.
  - **Access:** Power Truck Hire (Pty) Ltd Employees whose job function requires them to have and are approved by their supervisors and System Owners to have access, and Power Truck Hire (Pty) Ltd Vendors or Consultants who have executed Non-Disclosure Agreements with Power Truck Hire (Pty) Ltd.
  - **Distribution within Power Truck Hire (Pty) Ltd:** Access to Confidential Information must be strictly controlled by the System Owner who should conduct regular access reviews.
    - Confidential Information may be shared with authorised users via Power Truck Hire (Pty) Ltd IT facilities, including remote access, subject to Power Truck Hire (Pty) Ltd authentication. Encryption of data must be used for all web-based access to Confidential Information. Confidential Information must not be extracted from Responsible Party IT systems and stored on local IT systems without previous approval from System Owners.
    - If a portable device (e.g. a laptop, tablet or phone) is used to access Power Truck Hire (Pty) Ltd Confidential Information, the Personal Information must be encrypted and the device must have appropriate authentication in place (E.g. password or PIN to access the device).
  - **Distribution outside of Power Truck Hire (Pty) Ltd:** Electronic files must be encrypted (and optionally signed) using one of the following methods:
    - Public key encryption
    - Encrypted volumes/container
    - Secure authenticated web access
    - Password protected at the application level (i.e. signed PDF or Word document – Note: this is usually a weaker level of protection)
  - The encrypted/password-protected files can then be sent via email and/or secure electronic file transmission.
  - Third parties who are handling and/or storing Confidential Information must agree to abide by Power Truck Hire (Pty) Ltd's policies for safeguarding such information.
  - **Storage:** Information must be stored using Power Truck Hire (Pty) Ltd IT facilities.
    - Portable devices can have full disk encryption with appropriate authentication.
    - Portable devices can use appropriately secured encrypted volumes to store Personal Information
    - Encrypted removable media are not permitted without undertaking evaluation of other options by IT Support Staff.
    - Unencrypted removable media (e.g. USB sticks or drives) must not be used
    - Storage on personally owned (e.g. home) computer is NOT permitted without evaluation by IT Support Staff.
    - Storage on cloud servers or any server located outside of the Republic of South Africa is not permitted without prior approval/permission from the Data Subject
  - **Disposal/Destruction:** Electronic data should be expunged/cleared with a data scrubbing utility to ensure that portions of the original data cannot be reconstructed from the hard drive or other electronic storage medium.

- **Restricted Information or Special Personal Information**
  - Restricted Information or Special Personal Information has the highest level of sensitivity and represents the most risk to the Power Truck Hire (Pty) Ltd and individuals, should such Information be accessed by or exposed to unauthorised parties. Therefore, Power Truck Hire (Pty) Ltd Employees who handle Restricted Information or who use systems that store, transmit, or manipulate Restricted Information are required to maintain the confidentiality, integrity and availability of such Information at all times. The access, distribution, storage and disposal of Restricted information is subject to the prior authorisation from the Regulator and will require approval and review of the Information Officer.

- **Software Security**
  - Software for the purpose of this Policy document is defined as the programmes and other Operating Information used by, installed on, or stored on Power Truck Hire (Pty) Ltd owned computer systems or storage media. System Owners and System Administrators must ensure that software and other applicable materials are licensed (as required) in an appropriate manner.
    - Appropriate software updates/upgrades/patching policies should be in place to ensure security vulnerabilities are minimized
    - Control measures should also be in place for maintaining and accessing program and system source libraries.
    - All operational software should be maintained at current versions or at a level supported by the Supplier. In special circumstances, a non-current version of software for a legacy system may be retained for compliance purposes.
    - Security controls of audit trails and activity logs for the validation of data and internal processing are to be built into applications developed by Power Truck Hire (Pty) Ltd.

- **Internet and Email Security**
  - Computer devices connected to the Internet face significant risk of unauthorised access, or inappropriate use. A number of measures should be taken to mitigate this risk.
  - All Power Truck Hire (Pty) Ltd's devices require licensed anti-virus software with automatic definition updates to ensure that the device is protected from known malicious code.
  - Standards apply to all Internet capable devices requiring protection.

- **Power Truck Hire (Pty) Ltd Provided End-User Computing Device Security**
  - All Power Truck Hire (Pty) Ltd provided end-user computing devices including workstations, laptops, tablets and smart phones which connect to the Power Truck Hire (Pty) Ltd network will be configured, wherever possible to use:
    - Power Truck Hire (Pty) Ltd licensed anti-virus software with automatic definition update to ensure that the device is protected from known malicious code;
    - Automated patching process to ensure that operating systems and applications are kept up to date;
    - Device timeouts and password/PINs/biometric setting to minimise the risk of unauthorised access to the device.
  - By default, users will not have administrative access to their device but may be granted such access in special cases.
  - The installation of software and changes to the device’s configuration should be performed with the assistance of IT support staff.
  - Users must diligently protect mobile computing or storage devices from loss or disclosure of private information belonging to or maintained by Power Truck Hire (Pty) Ltd.
  - Confidential Information must not be downloaded to mobile or offsite computing devices, or storage devices unless approval has been obtained from the relevant Data Subject.
  - Mobile computing or storage devices that contain Power Truck Hire (Pty) Ltd’s Personal Information must use encryption or equally strong measures to protect the Personal Information while it is being stored.

- **Personally Owned Device Security**
  - This section applies to personally owned computing and storage devices which store any Internal or Confidential Information related to Power Truck Hire (Pty) Ltd such as Power Truck Hire (Pty) Ltd's e-mail, contacts and data in cloud storage.
  - Users must diligently protect mobile computing or storage devices from loss or disclosure of private information belonging to or maintained by Power Truck Hire (Pty) Ltd.
  - Users must not store Power Truck Hire (Pty) Ltd's Personal Information on personally owned devices or any other device not owned by Power Truck Hire (Pty) Ltd where such device can be used by another person, unless such devices are locked down to the Staff Member via password, pin or biometric access and the device locks itself after no more than 5 minutes of inactivity.
  - Confidential Information must not be downloaded to personally owned computing or storage devices unless approval has been obtained from the relevant Data Subject.
  - Personally owned computing or storage devices that contain the Power Truck Hire (Pty) Ltd's Personal Information must use encryption or equally strong measures to protect the Personal Information while it is being stored.
  - Restricted Information or Special Personal Information must not be stored on a personally owned device.

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