

	Petrobuild	POLICY
	DATA PROTECTION & POPIA POLICY	2026.01

1. Purpose

The purpose of this policy is to protect Petrobuild's information systems, data, and digital assets from unauthorized access, misuse, loss, or cyber threats, and to ensure the secure and responsible use of technology across the organisation.

2. Scope

This policy applies to:

- All employees, contractors, and third parties
- All IT systems, networks, devices, and data owned or used by Petrobuild
- All locations, including remote work environments

3. Objectives

- Safeguard company and client information
- Ensure business continuity
- Reduce cybersecurity risks
- Promote responsible use of IT resources
- Comply with legal and regulatory requirements (including POPIA)

4. Acceptable Use of IT Systems

Users must:

- Use company IT systems for legitimate business purposes only
- Not access, download, or distribute inappropriate or illegal content
- Not install unauthorized software or applications
- Use company email and internet responsibly

Limited personal use may be allowed if it does not interfere with work or security.

5. Access Control

- Access to systems will be granted based on job roles ("least privilege")
- Unique user IDs and strong passwords are required
- Passwords must not be shared
- Multi-factor authentication (MFA) should be used where possible
- Access rights will be reviewed regularly



+27 76 747 9075
+243 834 885 299



Info@petrobuild.co.za



147 Lavender Road, Johannesburg, RSA



Avenue NADIA WETU, Quartier Joli Site Cité du Park, Commune Annexe, Ville de Lubumbashi, Province du Haut Katanga DRC

	Petrobuild	POLICY
	DATA PROTECTION & POPIA POLICY	2026.01

6. Password Management

- Passwords must be strong (minimum length and complexity)
- Passwords must be changed periodically
- Default passwords must be changed immediately
- Passwords must never be written down or shared

7. Data Protection & Confidentiality

- Sensitive and personal data must be always protected
- Data must only be accessed by authorized individuals
- Confidential information must not be shared without approval
- Data handling must comply with the POPIA Policy

8. Email & Communication Security

- Users must be cautious of phishing emails and suspicious links
- Attachments from unknown sources must not be opened
- Company email must not be used for unauthorized purposes
- Sensitive information should be encrypted when shared electronically

9. Internet Usage

- Internet access must be used responsibly
- Accessing malicious or unsafe websites is prohibited
- Downloading unauthorized files or software is not allowed

10. Device Security

- All company devices must be secured with passwords or PINs
- Devices must not be left unattended in unsecured locations
- Anti-virus and security software must be installed and updated
- Lost or stolen devices must be reported immediately

11. Remote Work & BYOD (Bring Your Own Device)

Where personal devices are used:

- Devices must meet minimum security requirements



+27 76 747 9075
+243 834 885 299



Info@petrobuild.co.za



147 Lavender Road, Johannesburg, RSA



Avenue NADIA WETU, Quartier Joli Site Cité du Park, Commune Annexe, Ville de Lubumbashi, Province du Haut Katanga DRC

	Petrobuild	POLICY
	DATA PROTECTION & POPIA POLICY	2026.01

- Company data must be stored securely
- Public Wi-Fi must be used with caution (VPN recommended)
- Unauthorized sharing of company data is prohibited

12. Network Security

- Only authorized users may access company networks
- Wi-Fi networks must be secured with strong encryption
- Unauthorized access attempts will be monitored and investigated

13. Software & Updates

- Only approved software may be installed
- Systems and applications must be kept up to date
- Security patches must be applied promptly

14. Data Backup

- Critical data must be backed up regularly
- Backups must be stored securely
- Backup systems must be tested periodically

15. Incident Management

All employees must report:

- Cybersecurity incidents (e.g., hacking, malware, phishing)
- Suspicious activity
- Data breaches or loss

Petrobuild will:

- Investigate all incidents
- Take corrective action
- Notify affected parties if required

16. Monitoring & Compliance

- IT systems may be monitored to ensure compliance and security
- Unauthorized use may result in disciplinary action



+27 76 747 9075
+243 834 885 299



Info@petrobuild.co.za



147 Lavender Road, Johannesburg, RSA



Avenue NADIA WETU, Quartier Joli Site Cité
du Park, Commune Annexe, Ville de
Lubumbashi, Province du Haut Katanga DRC

	Petrobuild	POLICY
	DATA PROTECTION & POPIA POLICY	2026.01

17. Third-Party Access

- Third parties must comply with Petrobuild's security requirements
- Access must be limited and controlled
- Confidentiality agreements must be in place

18. Training & Awareness

Petrobuild will:

- Provide cybersecurity awareness training
- Educate employees on threats such as phishing and social engineering
- Promote best practices for data protection

19. Non-Compliance

Failure to comply with this policy may result in:

- Disciplinary action
- Termination of employment or contract
- Legal consequences where applicable

20. Review of Policy

This policy will be reviewed regularly to ensure it remains effective and aligned with:

- Technological changes
- Emerging cybersecurity threats
- Legal and regulatory requirements

Approved by: Bonita Botha

Position: Managing Director

Date: 1 March 2026



+27 76 747 9075
+243 834 885 299



Info@petrobuild.co.za



147 Lavender Road, Johannesburg, RSA



Avenue NADIA WETU, Quartier Joli Site Cité
du Park, Commune Annexe, Ville de
Lubumbashi, Province du Haut Katanga DRC