Privacy Policy

Policy Objectives

- Protect the confidentiality, integrity, and availability of personal information.
- Ensure compliance with ISO/IEC 27001:2022 and applicable data protection legislation.
- Provide transparency on how TDC collects, uses, stores, shares, and disposes of personal data.
- Define responsibilities for safeguarding personal data.

Roles & Responsibilities

- Management – ultimate accountability for compliance.
- Information Security Officer (ISO) – responsible for oversight, monitoring controls, and reporting incidents.
- Data Protection Officer (DPO) – responsible for regulatory compliance, handling subject access requests, and liaison with authorities.
- Employees & Contractors – must comply with this policy and attend mandatory awareness training.
- Third-Party Suppliers – must adhere to contractual obligations regarding data protection.

Information Collection & Use

TDC may collect personal information including, but not limited to name, contact details, identification numbers, transaction records, and online identifiers. Personal information is collected for:

- Providing and improving services,
- Meeting contractual or legal obligations,
- Security monitoring and fraud prevention,
- Marketing and communications (with consent).

Data Subject Rights

Data subjects have the right to:

- Access their personal data,
- Request correction or deletion,
- Restrict or object to processing,
- Withdraw consent where processing is consent-based,
- Lodge a complaint with the Information Regulator.

Requests should be submitted to privacy@tdc.co.za and will be handled in accordance with regulatory requirements.

Legal & Regulatory Compliance

TDC complies with POPIA and all applicable international privacy regulations where services are delivered. Legal, regulatory, and contractual requirements are identified and reviewed regularly.

Security of Personal Information

TDC implements layered security controls including, but not limited to:

- Encryption of personal data in transit and at rest,
- Access control based on least privilege and role-based access,
- Security logging, monitoring, and vulnerability management,
- Incident response and breach notification procedures,
- Periodic risk assessments and penetration testing.

Retention & Disposal

- Personal data is retained only as long as necessary for business, regulatory, or contractual obligations.
- Retention schedules are documented and reviewed annually.
- Data will be securely disposed of via deletion, anonymisation, or certified destruction of physical media.

Third-Party Suppliers

- Suppliers processing personal data on behalf of TDC must sign data protection and confidentiality agreements.
- Supplier compliance will be reviewed periodically through audits, questionnaires, or certifications.
- Non-compliance may result in termination of contracts.

Cookies & Log Data (Website Use)

- TDC may use cookies and analytics tools for service improvement.
- Users may opt-out of non-essential cookies.
- Log data (IP addresses, browser type, pages visited) is collected for security and performance monitoring.

Incident Response

Any data breaches or security incidents involving personal information will be managed through the ISMS Incident Response Procedure. Where legally required, data subjects and regulators will be notified promptly.

Policy Review & Maintenance

- This policy will be reviewed at least annually and after significant changes in operations, regulations, or risks.
- Review outcomes will be included in Management Review meetings.
- The current version of this policy will be available on the internal ISMS repository.

Enforcement

Non-compliance with this policy may result in disciplinary action, contract termination, or legal proceedings, depending on severity.