Data Governance and Security Policy

1. Purpose

The purpose of this policy is to establish a framework for managing and protecting Virtumed's data assets.

2. Oversight

Data governance at Virtumed is led by the Chief Executive Officer (CEO), supported by the IT Administrator, ensuring infrastructure and information governance decisions align with industry best practices, security standards, and regulatory compliance. The CEO's expertise in enterprise-level data oversight informs Virtumed's strategic approach.

3. Framework and Compliance

Virtumed adheres to the Protection of Personal Information Act (POPIA) and aligns with the General Data Protection Regulation (GDPR) where applicable. Key practices include:

- Collecting data for specific, defined purposes.
- Implementing role-based access controls across all systems.
- Conducting quarterly reviews of data access and usage by the IT Administrator.

Virtumed adopts client-provided POPIA-compliant operator clauses for data processing, ensuring personal information is handled strictly as instructed, utilizing AES-256 encryption, role-based access controls, and staff training on POPIA requirements.

4. Technology Infrastructure

Virtumed's core systems are hosted in Microsoft's Dataverse and SharePoint cloud environments, with accounting functions managed via Sage Cloud Accounting. These platforms comply with ISO 27001 and SOC 2 standards, undergoing regular vendor-managed security assessments.

No data is stored on-premises except for minimal paper records required by law. The network is protected by an enterprise-grade Ubiquiti firewall with automatic firmware updates applied within 7 days for critical issues and intrusion detection/logging enabled.

5. Classification and Risk Management

Virtumed maintains a data classification framework, categorizing data as:

- Public
- Internal Use
- Confidential
- Restricted

This framework enables risk-tiered security, retention, and backup procedures. Patient data (patient numbers, medical scheme details) in Sage Accounting and Dataverse is classified as Restricted, with access limited to the CEO, Chief Officers (COs), and invoicing staff via password-protected accounts and email-based authentication.

6. Backup and Redundancy

System backups are managed through Microsoft's automated services, with daily snapshots and redundancy across multiple regions. Sage Cloud Accounting backups comply with POPIA standards, including integrity verification.

7. Security Controls

- Network Security: Utilizes an Ubiquiti firewall with wired-only access, no Wi-Fi for operational systems, and remote access disabled.
- Endpoint Security: All devices are encrypted with screen-lock timeouts and two-factor authentication.
- Patch Management: Automatic updates for Sage Accounting, SharePoint, and Dataverse apply critical patches within 24-48 hours. Ubiquiti firmware updates are applied within 7 days.
- Vulnerability Management: Vendor-managed scans for Sage and Microsoft systems are supplemented by quarterly checks using Microsoft Defender for Cloud on Windows PCs. MacBooks utilize Apple's security updates.

8. Patient and Client Data

Virtumed stores patient data (Patient numbers, medical scheme details) in Sage accounting and Dataverse as invoices, accessible only by authorized staff. Bidder information is stored in SharePoint for evaluation, accessible by the IT administrator and CEO. No patient-identifiable clinical information is collected. All data handling complies with POPIA and client requirements.

9. Breach Monitoring and Incident Response

Virtumed maintains a robust incident response process, including:

- Immediate system lockdown.
- Notification to the CEO and IT Administrator.
- Engagement with affected parties within 48 hours.
- Root cause analysis and incident log updates.

If penetration testing identifies vulnerabilities, the IT Administrator produces a remediation plan within 30 days, with timelines: critical (7 days), high (14 days), medium (30 days), low (60 days).

Example:

- Vulnerability: Outdated firewall firmware.
- Action: Apply Ubiquiti firmware update via UniFi console.
- Responsible Party: IT Administrator.
- Timeline: 7 days.
- Verification: Confirm update and test functionality.

10. Data Retention and Deletion

Company information in SharePoint is deleted within 30 days upon request using Microsoft's secure deletion tools. Patient data in Sage Accounting and Dataverse is retained indefinitely for order fulfilment and legal compliance, with no deletion unless legally required. Retention practices align with POPIA.

11. Data Privacy Impact Assessment (DPIA)

Virtumed supports client DPIAs by providing detailed data flow descriptions for Sage Accounting and Dataverse, covering input from healthcare professionals, secure cloud storage, and restricted access. Vendor-provided diagrams from Sage and Microsoft are supplied when available, or custom diagrams are created upon client request.

12. Compliance Certification

An annual compliance certification, signed by the CEO, confirms adherence to this policy, reliance on Sage and Microsoft's ISO 27001/SOC 2 compliance, and Ubiquiti firewall security practices.

13. Continuous Improvement

Virtumed's data governance prioritizes secure, compliant, and streamlined systems with minimal complexity. Quarterly reviews and post-upgrade audits by the IT Administrator ensure ongoing alignment with POPIA, GDPR, and client requirements.