PRIVACY PROTECTION AND DATA SECURITY

Privacy protection and data security are highly regulated in South Africa, inter alia through the National Health Act, 61 of 2003, which mandates confidentiality and permits personal information disclosure only under specific circumstances. Dis-Chem also adheres to the requirements of the Protection of Personal Information Act, 4 of 2013 (POPIA).

To ensure compliance with legislative requirements and to protect customers' information as well as the Group's own, the CIS/SANS Top 18 Critical Security Controls Framework was adopted. A range of technical and organisational security measures are implemented, including:

- Firewalls and comprehensive enterprise email security gateways
- Network traffic analysis to detect anomalies
- Penetration testing, patching and vulnerability management
- User access control management and tracking based on the principle of least privilege with auditable records of access to data
- Real-time protection anti-virus, anti-malware and anti-spyware software
- Physical and environmentally secure server room facilities
- Encryption of portable devices, data in transit and personal data at rest
- Best practice data backup and disaster recovery facilities including offsite hosting at secure ISO27001-certified data centres
- Comprehensive security incident and breach procedures
- Compulsory independent annual IT general controls internal and external audits

The following processes and controls have been implemented for data governance:

- We classify existing third-party vendors as either high, medium or low risk in terms of data security
- High-risk vendors that access, process and store information have been selected for independent audits
- By December 2023, all high-risk vendors were assessed based on expected controls
- All Dis-Chem vendors undergo annual security assessments, irrespective of their classification
- A new data vendor onboarding process has been implemented (see below)
- The data governance framework policy and other third-party data-related policies were created (see below)
- A data governance implementation project is in progress with the pharmacy division completed and the rest of the Group scheduled for completion by January 2025

Ensuring a secure data interface with vendors

The Group has experienced third-party data risk first-hand. To mitigate this risk, a robust process is followed to contract and monitor data sharing with suppliers and other service providers.

Data security vendor onboarding summary

01 CONTRACTING

A data processing agreement is signed with each new vendor. A vendor account is then created on our third-party risk management platform.

02 RISK EVALUATION

Onboarding and inherent risk assessments are completed.

A vendor risk level is assigned.

03 APPROVAL

A core or lite security assessment is triggered thereafter and reviewed, approved or declined. Only when approved does the vendor become active and a service provider.

04 MONITORING

Annual security assessments are required and provided to vendors to assess any changes within the data environment.

Read more about how we handled a data breach in 2022 on page 21.

Our key performance indicators for privacy protection and data security are reported in the ESG data table on page 96.

5
DATA BREACHES RECORDED

66
CUSTOMERS AFFECTED BY DATA BREACHES

CASE STUDY

BOLSTERING OUR DIGITAL DEFENCES

Employees are key in protecting our assets, whether physical or digital. In October 2023, we hosted a cybersecurity awareness event to equip our employees with the necessary knowledge and tools to combat cyber crime.

Dis-Chem employees participated in interactive IT games, explored gadgets and engaged in educational sessions designed to enhance their understanding of cybersecurity threats and solutions. Various prizes rewarded employees who participated in competition quizzes and successfully completed cybersecurity training.

We believe that a well-informed and cyber-aware workforce is crucial in safeguarding our digital assets. We continuously educate employees and foster a culture of vigilance and preparedness in the face of cyber threats.

Employees also receive monthly cybersecurity awareness videos. After watching the videos, employees are tested to gauge the effectiveness of the training. These training statistics are tracked against every employee's profile to ensure compliance and improved security awareness.

OUR GOVERNANCE APPROACH TO PRIVACY PROTECTION AND DATA SECURITY

The Audit and Risk Committee provides oversight of privacy protection and data security, and considers the entire data lifecycle related to creating, accessing, storing and disposing of information. The Committee ensures that we have adequate systems to manage privacy protection and data security risks to avoid compliance gaps, reputational damage and financial loss.

We have a data governance department that focuses on setting standards and putting policies in place on how the data lifecycle works, and how information is stored, processed, and shared with third parties and internally within Dis-Chem. The department is responsible for data protection and limiting data breach risks to ensure that the Group's data is credible and accurate. It has the responsibility to ensure that systems that can access Group data have the required security controls to limit any possible data breaches. The department confirms that data is consistent and trustworthy and does not get misused.

Dis-Chem adopted COBIT 5 and the CIS/SANS Top 18 Critical Security Controls Framework. This ensures process focus and ownership, including Dis-Chem's fiduciary, quality and security needs. Our privacy and data security criteria include effectiveness, efficiency, availability, integrity, confidentiality, reliability, and compliance.

Dis-Chem policies related to this material sustainability matter include:

- Data protection policy
- Data management policy
- Data encryption policy
- Data leakage prevention policy
- Credit card handling policy
- Security management policy
- IT disaster recovery and business continuity plans (non-SAP systems)
- Information security policy
- Data privacy policy
- Data subject access request policy
- Data governance framework policy and RACI
- Third-party risk assessment policy
- POPIA policy

The policies are reviewed regularly and training is conducted to familiarise employees with data privacy requirements. Dis-Chem ensures its employees are legally bound to protect and maintain the confidentiality of any information they handle and/or process.

Read more about data sharing with suppliers in the supply chain chapter from page 82.

CASE STUDY

ENHANCEMENTS AFTER A DATA PRIVACY BREACH IN 2022

In May 2022, an unauthorised party gained access to a third-party Dis-Chem service provider's database. Using a brute force attack, the hacker was able to crack a password after continuously trying different combinations. We became aware of the incident through SMSs sent to some of our employees and notified the information regulator.

Approximately 3.6 million data subjects' records were accessed, including names and surnames, email addresses and cellphone numbers. As a result of the incident, the information regulator identified data protection weaknesses and required that we:

- Conduct a personal information impact assessment
- Implement an adequate incident response plan
- Maintain a vulnerability management programme
- Implement strong access control measures and maintain an information security policy
- Ensure written contracts are concluded with all operators who process personal information on our behalf

We reported on the implementation of all these actions to the regulator. We deployed additional safeguards and have invested significantly in systems, training and controls to mitigate this risk. The regulator has given Dis-Chem clearance and closed the matter. Read more about this material matter on page 18.

All data privacy incidents are formally reported quarterly to the Audit and Risk Committee; however there are instances where such incidents are reported as and when they occur.

DATA-SHARING PARTNERSHIPS ENABLE MORE EFFICIENT, SECURE AND ACCESSIBLE SERVICES TO PATIENTS WHO VISIT OUR CLINICS. WE USE AN ELECTRONIC PATIENT RECORD PLATFORM THAT ENABLES DIS-CHEM NURSES TO FACILITATE A VIDEO CONSULTATION WITH A NETWORK-APPROVED GENERAL PRACTITIONER WHEN REQUIRED. PATIENT RECORDS ARE SHARED, AND THE DOCTOR PARTICIPATES VIA A BIG SCREEN IN THE CLINIC WITH THE NURSE PERFORMING THE NECESSARY PHYSICAL EXAMINATIONS. THE DOCTOR RECOMMENDS TREATMENT AND WILL PROVIDE A SCRIPT THAT CAN BE FILLED AT THE DISPENSARY.