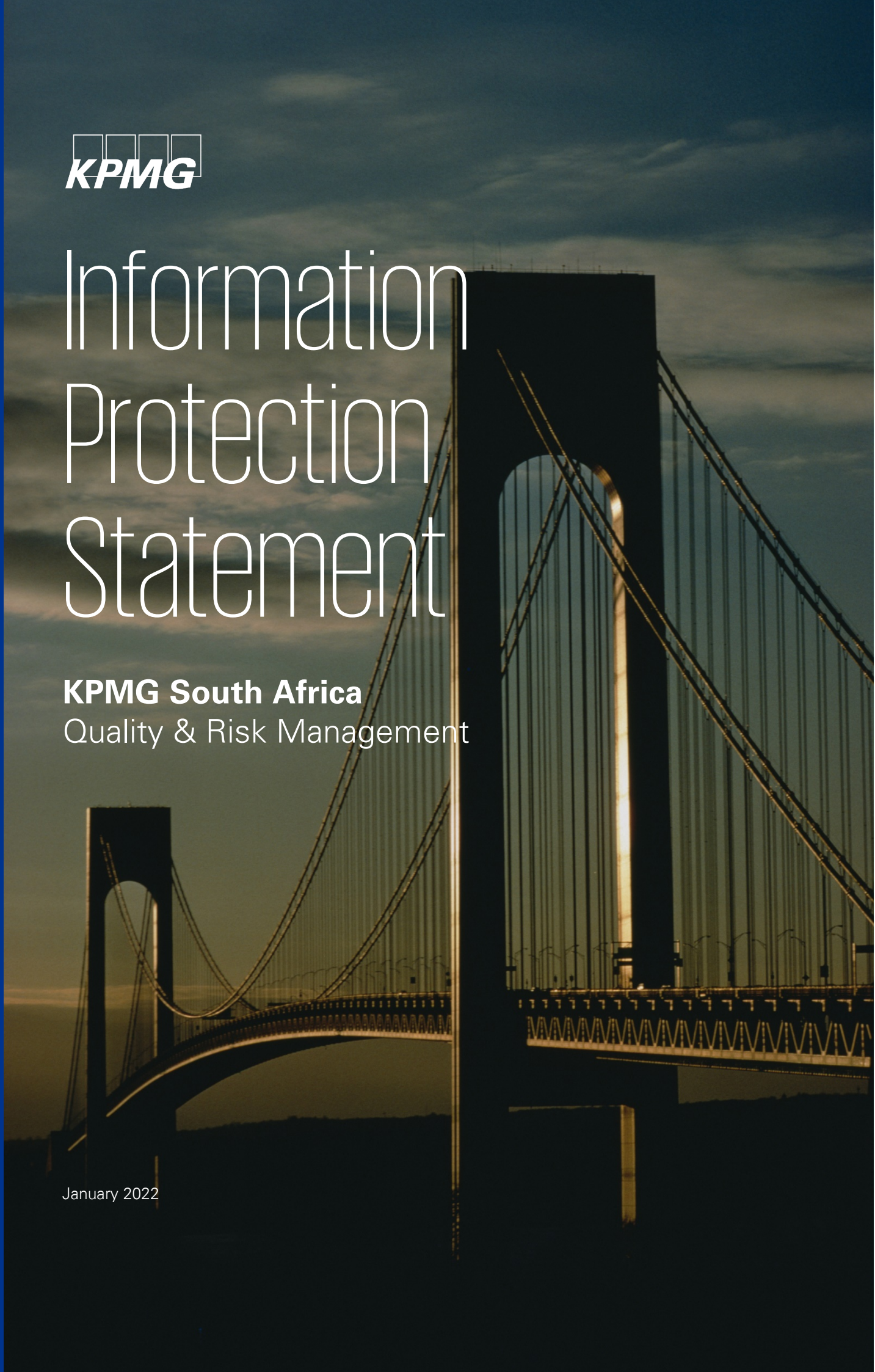

Information Protection Statement

KPMG South Africa
Quality & Risk Management

January 2022

Contents

1 Introduction

This document provides an overview of KPMG South Africa's information and data protection practices

KPMG is committed to providing a secure and safe environment for the personal data and confidential information we hold, as well as protecting the privacy of our clients, service providers and other third parties.

KPMG regards this information and our associated information systems as valuable and fundamentally important to our business operations. With dedicated resources that are focused on improving information protection practices throughout KPMG, we strive to identify risks to our information assets and to guard against any unauthorised access, loss, or misuse. As part of managing such risks, KPMG uses a variety of access controls, security devices, and monitoring tools to analyse our systems and network.

KPMG's security requirements are set out in the Global Information Security Policies and Standards published by KPMG International ('KPMGi' or 'Global').

We believe that everyone has a role to play in protecting client and confidential information. Policies and practices are communicated to all employees and, as appropriate, reinforced through guidance, awareness and training. Our employees are required to comply with our Acceptable Use Policy, this policy encourages effective and appropriate use of KPMG information technology resources, and highlights the protection requirements of all employee, KPMG, and client confidential information. Data privacy policies are also in place governing the handling of personal information.

The importance of maintaining client confidentiality is emphasised through a variety of mechanisms, including through regular communications on the topic, the Code of Conduct, training, and the annual independence/confirmation process, which all of our professionals are required to complete.

In addition, all KPMG employees are contractually bound to comply with KPMG's information protection and security policies.

2 Governance

At the Global level, information risk and security is overseen by the Information Protection Group (IPG). The group's information protection activities are headed by the Global Chief Information Security Officer, and its data privacy activities are headed by the Global Chief Privacy Officer.

Each member firm is required to appoint an individual to serve as its primary contact for information protection and to coordinate with other aspects of the business including physical security, legal, risk management, the privacy function and others as needed. These individuals are the principal contact points between KPMGi and the member firms for information protection matters.

The firm's dedicated Information Security function, including key people within our Quality & Risk Management (Q&RM) and supported through the firm's IT Services (ITS) function, are responsible for developing and promoting KPMG's information protection policies, driving our awareness and education activities, assisting with development of appropriate standards, conducting IT security reviews and risk assessments.

The firm's National Risk Management Partner is accountable for Information Risk for the firm, and ultimately signs off any information protection policies. The firm's Chief Information Security Officer or knows as the NITSO the KPMG context is the person with overall responsibility for establishing and operating an IT security organisation that complies with KPMG's Global IT standards and requirements.

By working closely with other business and central functions, these dedicated resources set appropriate standards designed to maintain the security of our information and that of our clients. Through these activities, the team also assist our staff with understanding our responsibilities for the security and protection of client information.

Information protection: key activities

Establish policies and guidance for the use of KPMG's Information Technology (IT) assets, equipment, network and systems. Develop strategies, standards, and design security controls to help protect client and other information within KPMG systems.

Establish policies and guidance on the labelling and handling of information. Developing strategies, standards and controls for data and information management. Advise on appropriate risk mitigating measures.

Monitor IT security controls and compliance with standards and specifically in relation to KPMG International requirements including:

— Conduct information protection reviews and risk assessments.

— Facilitate Internal Audit reviews of Information Technology Services and KPMG premises.

— Understand the impact of new laws and regulations on IT environment.

Undertake a programme of awareness and education activities to ensure that our people understand their responsibilities in relation to the protection of client, personal and KPMG information.

3 Information Protection Programme

KPMG's information protection programme is built on a comprehensive framework of policies, standards, and processes. Our framework is based on ISO 27001:2013 (Information Security Management Systems – requirements), and our security policies, standards and procedures are aligned to this and to KPMG International requirements. The framework includes the following elements:

- Governance and Security Organisation
- Security Policies
- HR Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Business Continuity Management
- Compliance

3.1 POLICIES

KPMG International issues global policies and requirements, and each member firm is responsible for local implementation and ongoing compliance with the policies and requirements, as well as any applicable local laws or regulations. KPMGi, the member firms and employees are required to comply with policies regarding acceptable use of IT resources, information protection, data protection and client confidentiality as outlined below. These policies are reviewed periodically and may be modified as needed. The three core policies in relation to information protection are:

- Global Acceptable Use Policy (G_AUP)
- Global Information Security Policies (GISP)
- Global Data Privacy Policy
- Data Protection & Privacy Policy
- Records Retention Policy

All KPMG employees are made aware of our policies and any changes to policy through a number of channels including:

— For new joiners, through the induction programme and mandatory Quality & Risk Management training.

— Annual mandatory Quality & Risk Management Information Protection Fundamentals and Privacy training, which includes covers areas such as IT security, data privacy and confidentiality.

— Regular updates and alerts using newsletters and email alerts.

3.2 CLIENT CONFIDENTIALITY AND DATA PROTECTION

KPMG employees are subject to policies governing the use and disclosure of client information.

These policies address the confidentiality principles established by the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA) and in the South African Institute of Chartered Accountants (SAICA) and the firm's regulator, the Independent Regulatory Board of Auditors (IRBA).

KPMG also complies with applicable legal and regulatory requirements and professional standards to protect the confidentiality of our clients' information and personal data.

KPMG employees are subject to our confidentiality policies, as detailed in our Code of Conduct and Quality & Risk Management Manual, with regard to the use and disclosure of our clients' information.

In addition, KPMG's policies on Data Protection and Privacy establishes minimum principles to be applied when handling personal information.

In instances where KPMG allows third parties to process confidential or personal information on our behalf, we address in our agreements with those third parties the obligation to maintain the privacy and confidentiality of such information, according to KPMG's confidentiality policies and practices or as otherwise appropriate. KPMG may also disclose client information where required by a mandatory provision of law, statute, rule or regulation, including any summons or other similar process.

4 Controls

This section provides an overview of KPMG's Information Security Management Policies and Controls.

4.1 HUMAN RESOURCE SECURITY

All KPMG employees and Partners must acknowledge that they understand and will comply with the firm's Code of Conduct, the Information Security, Acceptable Use, Data Protection & Privacy and Records Retention Policies & Practices. This is achieved through the Ethics and Independence confirmation as part of the on-boarding process and annually thereafter.

HR is responsible for conducting and approving pre-employment screening checks for KPMG employees and Partners. Pre-employment screening checks are applied to contractors under the guidance of Quality & Risk Management who establish requirements for service suppliers to perform pre-employment checks.

KPMG adopts a risk-based approach to pre-employment screening. Prospective employees undergo checks on:

- Employment references
- Relevant academic and professional qualifications
- Credit checks
- Criminal background

4.1.1 Information Protection awareness, education and training

KPMG has a comprehensive security awareness programme that includes email communications, security alerts and advisories and awareness emails.

All KPMG employees are made aware of their personal requirements in relation to information protection through several channels:

- For new joiners, through the induction programme and mandatory Quality & Risk Management training;
- Mandatory annual Quality & Risk Management training which includes section on IT security, data privacy and confidentiality.
- Regular updates and alerts through the IT Security Team.

4.1.2 Termination of employment

KPMG has an established joiner, mover and leaver process in place. The HR support team will initiate the leaver process for all departing employees. IT Services ensures that all leaver accounts are disabled within one business day of the termination date. All KPMG employees shall return all KPMG and client information and IT assets before their departure from KPMG. KPMG employees shall acknowledge in writing that they have returned all such materials before the termination procedures are completed.

4.2 ASSET MANAGEMENT

4.2.1 Inventory of assets

An inventory of hardware and software is maintained for all system in the firm's data centres and supplemented by detailed documentation regarding the purpose of each type of software or hardware asset. The named owner of hardware and software is held in the inventory.

4.2.2 Information handling

KPMG firms must adhere to a global information classification policy. The firm has four levels of classification: Public, Confidential and Highly Confidential. By default, all information created in KPMG or received into KPMG is considered to be 'KPMG Confidential' regardless of whether or not it is formally labelled as such. All KPMG employees must handle KPMG and client information in line with the provisions of these policies, or as explicitly directed by the client.

4.2.3 Retention

The retention of working papers is in compliance with statutory laws and regulations and KPMG's retention policies. If no period is defined, the KPMG working papers should be retained for six years (or eight year for SEC Clients) from the end of the engagement.

4.2.4 Media handling

KPMG uses a centrally managed software solution to manage and control removable media. Only KPMG approved corporate removable media, with enforced encryption and password protection, may be used to store KPMG or client information. Removable media may only be used for the short-term storage or transfer of information. Once no longer required, information must be securely removed from the device.

'End of life' KPMG PCs and hard drives are erased using industry standard erasure software. All server disks that are 'end of life' are degaussed and destroyed through certified destruction via a reputable third-party supplier.

4.3 ACCESS CONTROL

Access control requirements are defined on the basis of least privilege and are approved by the business owner and/or other authorised parties and documented. Business owners communicate their access requirements to IT Services in a form that enables effective implementation. 'Single Sign On' using Active Directory authorisation is used wherever possible.

KPMG employees with access to KPMG's information resources use a User ID that has been specifically assigned to them for business purposes only. All user IDs are associated with a password that adheres to the KPMG Password Policy as defined in the KPMG Acceptable Use Policy. User IDs are not to be used by anyone except the individual to whom the IDs have been issued. Users are responsible for all activity performed with their personal User IDs. Group or shared IDs are not permitted (other than for training purposes on machines dedicated for the purpose), unless permission has been explicitly granted by the NITSO and/or Quality & Risk Management.

4.3.1 Password management

A formalised password management process is in place, which includes a secure method for delivering initial and temporary passwords, and these must be changed at first login. Requests for

password resets include positive verification of identity and accounts.

Passwords are changed every 60 days and should be a minimum of eight (8) characters for standard users, guidance is given on password complexity.

4.3.2 Privileged accounts

The creation and use of privileged accounts are kept to a minimum. Individuals with a business need for such access are explicitly identified and all such assignment (and revocation) formally documented.

For systems processing information that is regarded as sensitive by the business owner or where required by contractual obligation, user access privileges are reviewed to determine if access rights are commensurate with the user's responsibilities. All user accounts assigned a higher level of privilege, are regularly reviewed both for account activity and for ongoing appropriateness. Evidence of account and privilege reviews (documenting when, who, and what action, if any, was taken) must be maintained for a period of twelve months.

4.3.3 Remote Access

KPMG employees who work in off-site locations can access KPMG's network and resources only via our virtual private network (VPN), using strong (dual factor) user authentication. KPMG employees are informed of their responsibilities for maintaining security via regular awareness communications.

4.4 CRYPTOGRAPHY

All laptops have full disk encryption through FIPS-140-2 compliant commercial products. Mobile devices like smartphones are managed through Mobile Device Management (MDM) with enforced policy, and authenticated through the use of device certificates for connection to the network.

Non-public information is encrypted during transport over the Internet, either by the use of a Virtual Private Network (VPN), or by using HTTPS encryption in the case of most Web-based applications. Transport Layer Security (TLS) encryption is enabled on demand on the Internet mail gateways, and a number of layered anti-malware controls are used to guard against inbound malicious content, defensive filtering, and content management.

4.5 PHYSICAL AND ENVIRONMENTAL SECURITY

KPMG is committed to ensuring the safety and security of its people, third-party suppliers, visitors, premises and the assets they contain. To ensure our people, authorised visitors and third-party suppliers are provided with a safe and secure environment in which to work, KPMG recognises that security must be afforded the same priority as its other business objectives.

Security perimeters (barriers such as walls, electronic access-controlled entry gates, turnstile and manned reception desks) are used to protect areas that contain information and information processing facilities.

A summary of the physical security controls implemented at KPMG offices is provided below:

- All KPMG offices are equipped with electronic access control, digital CCTV and intruder alarms linked to our 24-hour security control.
- The CCTV systems consist of colour day/night monochrome cameras strategically positioned both internally and externally.
- All KPMG employees are allocated photographic access control passes, which allow subject access to KPMG offices/buildings, and restricted/confidential zones according to their individual status/need. Access control passes must be displayed at all times, and are strictly non-transferable.
- A centrally monitored and controlled card-based electronic access system controls all physical access and stores detailed access logs that include name, date and time of activity.
- All visitors to KPMG offices are registered on an visitor management system, and are required to be signed in by a KPMG member of employee and be escorted at all times whilst on the premises.
- KPMG operates a Clear Desk Policy requiring all confidential papers, laptops and data holding devices to be stored securely out of office hours.
- Timeout for inactivity on laptops is set to five minutes with a password protected screensaver.
- Hard copy waste which is identified as confidential is disposed of in sealed confidential bins within KPMG offices, a third-party supplier destroys such data on a monthly basis.
- To minimise the threat of interception or damage, all cable and line facilities for voice, data and video are secured. Adequate protection is provided (e.g. use of shielding, conduit, burial and routing away from uncontrolled areas), and regularly maintained to meet this requirement.

4.6 Data Centres

4.6.1 KPMG South Africa Data Centres

KPMG South Africa's Data Centres utilise strict access control procedures. All attempts at unauthorised access are logged, Access is restricted to authorised individuals who go through an approval process that is based upon a person's need to access the related area/equipment. The Data Centres are monitored by on-site security officers 24/7/365.

The KPMG Data Centres contain:

- Air conditioning with heat and humidity sensors, which are managed by an environment management system
- Fire suppressant system
- Flood detection systems
- CCTV Monitoring

4.6.2 KPMG International Data Centres

The firm utilises certain cloud solutions such as Office 365 and Microsoft Teams, these services are delivered to the firm through a Microsoft Azure instance manged by KPMGi. Services consumed by the firm are mainly delivered through data centres located in the Netherlands and Ireland. These data centres are ISO27001 certified, and certain services also maintain a current SOC 2 Type 2 reports.

4.7 OPERATIONS SECURITY

4.7.1 Change management

KPMG IT services utilises a formal change and release management procedure. All changes follow a

predefined approval process with significant infrastructure changes requiring approval from the CIO.

4.7.2 Protection from malware

All KPMG workstations have automated virus and malware scanning. Systems check on a regular basis for updates to antivirus signatures. Web content and emails are virus-scanned by separate systems that utilise different antivirus vendors.

For Microsoft-based systems, the firm uses Microsoft Endpoint Protection Anti-virus, with Microsoft Defender Endpoint activated on all workstations. The firm utilised Next-Generation Firewall with advanced Threat Protection. The email system utilises a third-party spam filter service and three layers of multi-vendor antivirus scanning.

Windows servers operate the centrally managed and updated Symantec Endpoint Protection client, providing anti-malware protection. Alerts from the servers are sent to a central management server, where events logs are reviewed and any necessary remedial actions taken.

4.7.3 Data backup

Backups are run to a 31-day rolling cycle with additional backups taken as specified by the business.

IT Services maintain a business recovery plan, which forms part of the wider KPMG Business Continuity Plan. In the event of an emergency any essential information can be restored.

Backup tapes for core KPMG systems are retained within the tape library located at the failover data centre (i.e. these tapes are 'off-site' with respect to the Live data centre). For certain systems, data is mirrored between the data centres over private network links. All physical backup tapes are encrypted.

Backup tape recovery is tested when the disaster recovery testing plan or the business owner requires it, there is no fixed testing period. Systems with a resilient DR instance are maintained by our ITS Operations teams following operations procedures and run books.

Scripts are run that report when the last backup occurred, and when next backup is due to ensure that backup operations are timed correctly and complete as expected. The firm's Backup system highlight backup exceptions and errors, alerts are emailed to the Backup team. The Backup team constantly checks for issues.

4.7.4 Logging and monitoring

KPMG's dedicated in-house Global Security Operations Centre (GSOC), located in India, monitors KPMG's enterprise level infrastructure for threats and possible security incidents. Security logs are monitored 24/7 by the GSOC to detect potential security incidents and where appropriate these escalated through the firm security incident management process for the necessary action and remediation.

Audit logs, where appropriate, are maintained for 180 days as designated by the Log Management policy. Such logs are designated as KPMG Confidential, and are be protected accordingly. Care is taken to ensure that turning on any system auditing logging feature does not materially impair the performance of that system.

IT resources are regularly monitored to ensure secure, stable and available operation. Network and system activities that need to be monitored include, for

example, internet firewalls, the use of resources, remote access, security control mechanisms, capacity, overloads, outbound communications and periods of system unavailability.

Faults reported by KPMG employees regarding technical problems with information resources are logged and reported to the appropriate ITS Operational teams. These teams are responsible for addressing all technical problems that have been identified relating to the information resources under their control.

Only parties authorised by the CISO have the authority to access, retain and delete logging records. All administrative and operator activities shall occur through the use of unique personally assigned user accounts and not through generic system accounts where ever possible. System administrator and operator activities are logged. The logs are protected against unauthorised or inadvertent modification or erasure. Logs are automatically correlated for security conditions and retained to assist in access monitoring and future investigations.

4.7.5 Internet access

The Acceptable Use Policy determines access to sites that are deemed appropriate.

The firm filters employee Internet access from the office network. Access to personal web-based email is limited, as are on-line backup, storage, and collaborative sites, where categorised as such by the filtering system.

Other sites including adult, offensive and malicious sites are also blocked. KPMG outbound email is not filtered for content other than for viruses and other malware. Exceptions to these blocking rules are permitted in the presence of a strong business case, and require approval by Quality & Risk Management.

The KPMG office network utilises technology which only permits allowed HTTP and HTTPS connections, all other protocols are blocked unless an exception is approved. This, in conjunction with the enforced web filtering and the restriction of administrator rights on workstation prevents the use of peer-to-peer and other restricted software.

4.8 COMMUNICATIONS SECURITY

4.8.1 Network security

KPMG protects its internal network systems through the use of a multi-layered high availability firewall design, the firm also utilises network based threat protection. The type and configuration is confidential and this cannot be shared.

KPMG's internet-facing and internal systems are vulnerability scanned on a bi-weekly basis. All new web-based Internet facing systems are reviewed before the systems are promoted to the live environment. Non-standard devices deployed internally are also reviewed where required to assess any risks they pose to the internal network. The status of the KPMG Internet firewalls is monitored by the Network team for any anomalies.

Logs are sent to a central location and correlated for suspicious events and alerting.

4.8.2 Wireless networking

KPMG operates secure wireless access to the internal KPMG network. This wireless service is

only available to KPMG employees and is secured through the use of certificate (user and device) based authentication with Active Directory, as well as using AES encryption to secure the communications. Only KPMG trusted devices are allowed to connect to the wireless network.

Visitor wireless access is available in some KPMG offices, but is separate from the KPMG internal network.

4.8.3 Electronic messaging

Business as usual email is sent via opportunistic TLS as it passes over the internet. Policy enforced TLS email can be employed on demand, and other specific client requirements for encryption can be considered. A secure e-room (GlobalScape) is available for securely transferring files externally.

The e-rooms are hosted on KPMG data centres in the UK.

4.9 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

KPMG has robust processes in place for assessing the risks associated with new systems and applications. In relation to IT projects, the firms IT Security team is involved in appropriate stages of the project lifecycle, in order to provide relevant security evaluation and approvals.

4.10 SUPPLIER RELATIONSHIPS

All suppliers of IT or data related services are required to meet KPMG's information protection requirements as defined in the standard contract schedules. Detailed assessments are performed on suppliers as part of the selection process.

The KPMG business owner of each third-party service is responsible for monitoring their third-party contracts/agreements to ensure that the services are being delivered as expected and on time. Processes are put in place to monitor performance against committed service levels and the right to audits is included in the firm's standard contract wording.

4.11 INCIDENT MANAGEMENT

KPMG has procedures in place to manage security incidents including, for example, data loss/breach and physical security incidents:

- Escalation for a data-related incident would be through the firm's Privacy Liaison.
- Escalation for an IT security incident would be through the Chief Information Security Officer.
- Escalation for a physical security incident would be through Facilities.
- Escalation via KPMG's Global Security Incident Management when appropriate and when events that may impact our enterprise level network or other member firms.

Any incident involving client data would be escalated to the Client Lead Partner, Risk Management Partner, Chief Information Security Officer and Privacy Liaison.

This procedure is reviewed annually.

4.12 BUSINESS CONTINUITY

KPMG has contingency plans to handle disruptions to our operations and

services. These plans include provisions for disruptions that may impact local offices as well as our essential back-office applications hosted in our data processing facilities. In the event of an unforeseen disaster or emergency, KPMG has processes in place to minimise the impact of a disaster so we can continue to service our clients and recover our operations. Additionally, a comprehensive Crisis Management plan responds to any emergency that should threaten or affect KPMG employees, facilities, and operations, including data and processes. The Business Continuity Plan is reviewed annually.

5 Compliance

All KPMG firms are required to comply with KPMGi policies, standards and guidelines and other requirements. Compliance is monitored by a global compliance programme developed to ensure continued compliance to key policies focusing on key elements of information protection.

This programme includes annual information protection and privacy audits, with the local audit results and audit process reviewed by the KPMGi Compliance Team. Progress on associated remediation plans are tracked monthly by both the local Information Security Team and the Global Compliance Team.

5.1 COMPLIANCE WITH IT STANDARDS

Compliance with IT standards and appropriate maintenance of the software installed on all KPMG computers is a policy driven requirement within KPMG. IT standards, software versions and vendor patches are monitored and reviewed regularly by IT Services to ensure that they remain current and are updated or superseded as appropriate. Products and software that are part of our standard configurations are updated and deployed to all platforms as part of firm-wide deployments.

Contact us

Heinrich Vermeulen
Chief Information Security Officer
T +27 (0)79 223 5265
E heinrich.vermeulen@kpmg.co.za