POPI Compliance
& Security Policy

Contents

Introduction & Overview

Section 1

This POPI Compliance and Security Policy describes how we handle your information when you use our software and services. This Policy was last revised on 11 May 2020 - date changes are implemented.

In compliance with POPI, we have two roles and responsibilities:

- We are the responsible party regarding the client's personal information: company details, staff / user details, such as email addresses, phone numbers, billing details, and other information used to do business.
- We are the service provider or operator regarding the personal information that the client uploads in the form of a database, distribution list, or the like.

1.1 Privacy Principles

As your service provider, stewardship of your data is critical to us and a responsibility that we embrace. We abide by the following principles when collecting, recording, storing, disseminating, and destroying personal information, and responding to government requests for our users' data:

- **Choice and consent:** We will not contact / solicit you unless you have given us your consent to do so.
- **Transparency:** We let you know up front that we will be processing your data in fulfilment of your request.
- **Accountability and security:** We take measures to ensure data is kept safe and prevent loss of, damage to, or unauthorised destruction of personal information, and unlawful access to or processing of personal information.
- **Access:** We will give you access to any of your personal information that you request, unless the request is unlawful.

Client data is always treated as confidential and for the sole purpose of rendering services to you.

1.2 Compliance

We are compliant with the following:
- Protection of Personal Information Act (POPI)
- CPA Section 11
- Electronic Communications Act of 2002 (ECT)

1.3 Information Request

By Existing Client: If your personally identifiable information changes (e.g. your email address or cell phone number), or if you no longer desire to use or access the service, we encourage you to correct, update, or remove the personal information that you provided. This can be done by contacting us directly.

By Data Subject: In the event that a data subject (i.e. a contact in your email or SMS list) would like access to their data, requests must be submitted to us in writing. Requests for personal information will be handled in accordance with the POPI Act as outlined in our Subject Access Request Policy.

In the unlikely event that there is a data breach (e.g personal information has been compromised in your data on the system): Notification will be sent to the responsible party. The response procedure for requests for customer data from regulatory authorities, courts, law enforcement authorities, and other third parties, is outlined in our Data Breach Response and Notification Procedure Policy.

For any requests outside of these two documents, we engage our lawyers for legal advice.

1.4 How to Contact Us

Contact Number:	
Email Address:	
Physical Address:	
Postal Address:	

1.5 Changes to this Policy

If we make any material changes, we will notify you by email or by providing the revised policy on our website. Your continued use of our services following the update means that you accept our updated POPI Compliance & Security Policy.

2.1 Server Setup

Our servers are set up for high performance and uptime. We use a fully redundant and load-balanced setup to run our application, ensuring high availability and data security. Our server setup includes the following:

Web servers

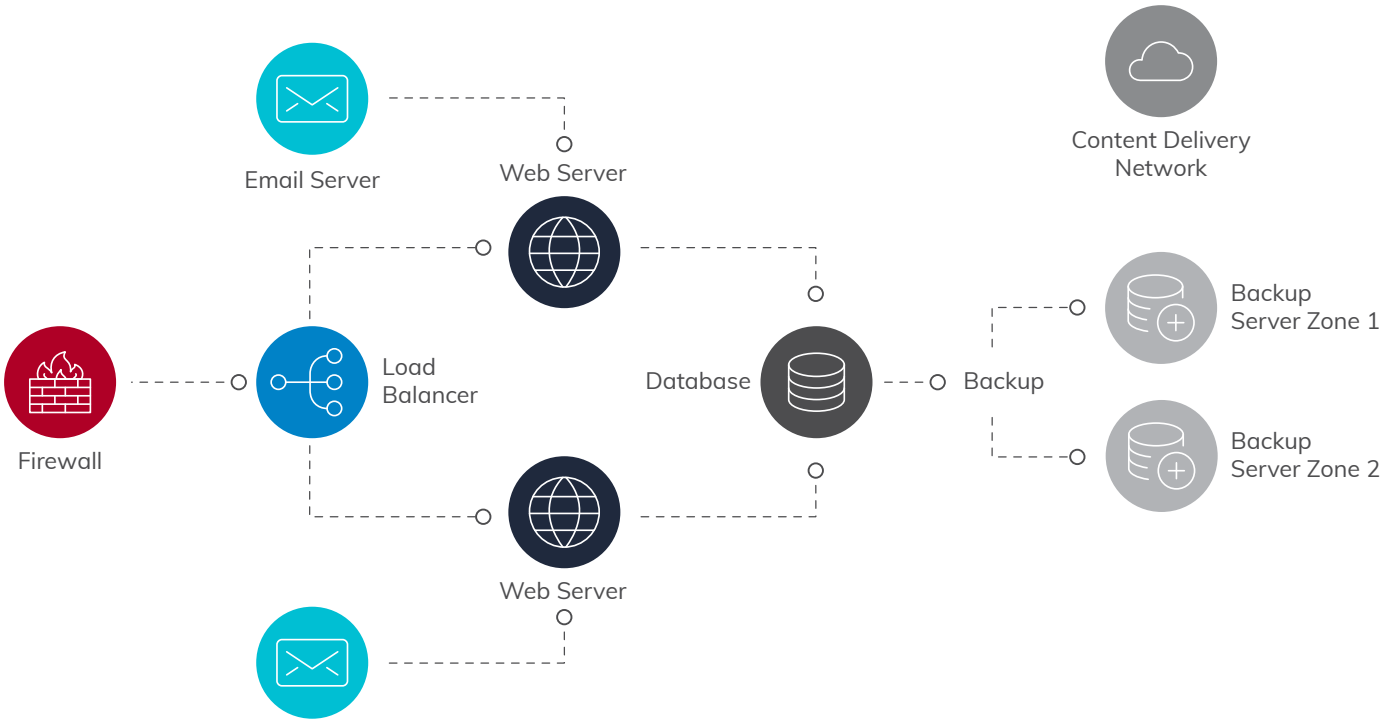
Database servers: Our data is hosted by Databank in the United States and Microsoft Azure in South Africa.

Mail Transfer Agents (MTA): The MTA is a software program that transfers messages from one computer to another. The major functions of the MTA are:

- Accepting messages originating from the user agent and forwarding them to their destination (other user agents).
- Receiving all messages that are transmitted from other user agents for further transmission.
- Keeping track of each and every activity, analysing, and storing the recipient list to perform future routing functions.
- Sending auto-responses about non-delivery when a message does not reach its intended destination.

Global Content Delivery Networks (CDN): A CDN is a network of servers that deliver webpages and email content to readers, depending on where they are in the world.

Backup Servers: In our network, the backup servers store all our data to prevent data loss.



Limited Script Execution

We do not allow scripts to be executed in any location that the application has access to.

Intrusion Prevention & Detection

- All requests that enter our intrusion prevention and detection systems (IPS / IDS) go through a deep packet inspection and are analysed for legitimacy.
- Databank's IPS / IDS systems monitor traffic in real-time at gigabit speeds, and block over 2 million attacks per day. Rules are updated routinely and include most zero-day exploits.
- On Azure servers, packets are inspected in real-time using our Web Application Firewall on the layer 7 network gateway, protecting our application from various web vulnerabilities and attacks.

Dedicated Firewalls

- Firewalls limit ingress and egress traffic, perform state-full packet inspections, and establish VPN connectivity to your offices and for remote users.
- Our international servers (Databank) use dedicated high-performance Cisco ASA firewalls to achieve complete isolation between each client's installations. Because each client's security needs are different, our firewall administrators work with you to tune your firewall's specific rules.
- Our Local Servers (Azure) use a high-performance, auto-scaled, layer-7 gateway with a WAF, combined with NSGs. Each application layer in Azure is divided and isolated on their own subnets with their own NSG rules.

2.2 Data Storage

Our data storage is handled in the following manner:

Data Hosting
- We use both local and international servers to host our data.
- The international servers are hosted by Databank in the United States and the local South African servers are hosted by Microsoft Azure.
- We are currently in the process of moving all our infrastructure to Microsoft Azure, where most of our data will be hosted locally with an additional option to host data at any Azure datacenter in the world.

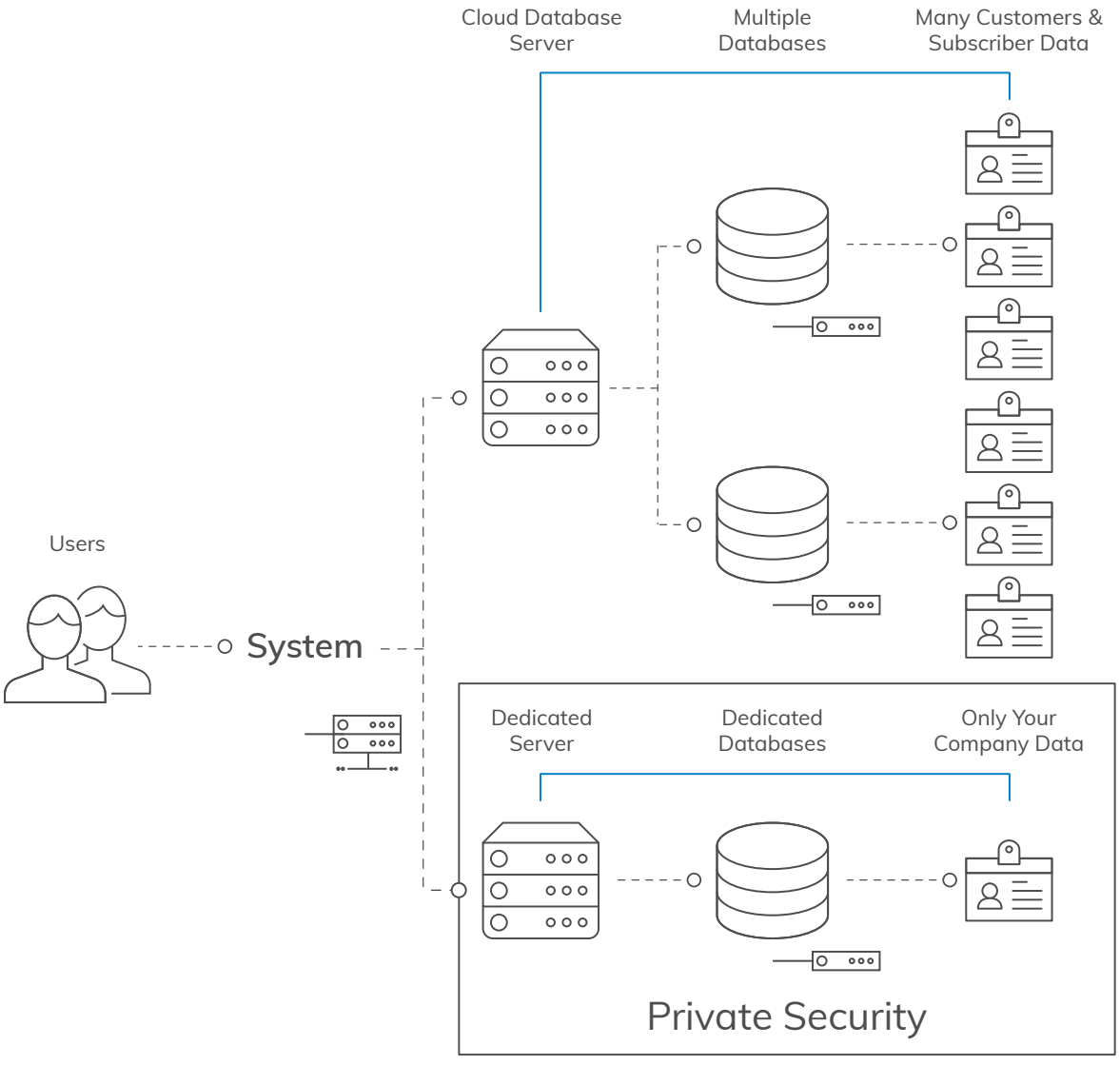
Logical Separation
Data is logically separated, but not physically. However, it is segregated inside the solution. Our database structure is a relational database and each contact record contains a relational customer key. Clients can only see their own contacts due to relational key restrictions.

Physical Separation
The client may request that data be stored in a separate physical database. There are various options for this, including each application being separated with separate URL logins and user credentials.

With our Private Security option, we have dedicated servers available too, hosted on the cloud.

The **Private Security offering** is a privately hosted extension of our Advanced service level agreement. It's designed for companies that require their data to be hosted on exclusive and dedicated servers where custom policies can be applied.

It has additional security measures like:
- A private / dedicated server for database hosting.
- Exclusive encryption keys used for data at rest and database backups.



2.3 Physical Security - Physical Access to Data Centre

Prior to Data Centre

- Restricted parking on the premises
- Restricted access to the facility
- Signs identifying the data centre facility
- Guard at entrance
- Photo identification required
- Business identification required (photo ID or business card)
- Sign-in / sign-out process

Data Centre Security & Facility Access Rights

- Restricted access to the data centre facility
- Keypad access
- Signs posted for restricted access to data center
- Unique access ID for each employee
- No generic IDs granted for vendors, maintenance, or others
- Process for granting / revoking data center access
- Escort required for visitors
- Escort required for vendor and maintenance workers
- Periodic reconciliation of staff with data centre access

Tracking

- Live monitoring of access
- Digital log of door access
- Written visitor log in restricted data centre area
- Camera placement at all door access points
- Camera placement at aisles / cages
- Digital and analogue, motion CCTV system
- One-day CCTV recording cycle
- Ninety-day CCTV storage beyond normal recording cycle

2.4 Application Security

The system has been developed with application security in mind from the very beginning. The product has been written to prevent and withstand attacks common to web-based applications. We use industry-standard safeguards to stand up to the following types of attacks:

SQL Injection Attacks
Data filtering and escape mechanisms prevent attack via SQL malware scripts. Additionally, all queries run on the database use bound parameters (a method of escaping input) or MySQL escaped strings to prevent SQL injections.

Cross-Site Scripting Attacks
All input is validated and type cast to ensure input data is valid. Output data from the database is also sanitised before displayed on the interface. Additionally, we include the X-XSS-Protection header in requests to enable and enforce the XSS filter built into web browsers.

File System Monitoring
Attackers commonly target the file system on an application server. To counter these attacks, we have mechanisms in place that monitor for any unauthorised file system changes. If any change is detected, the application is shut down and we are alerted to the problem so we can investigate the issue.

Session Management
We use PHP session management. It is a robust, trusted mechanism. Furthermore, we namespace and segregate all session data.

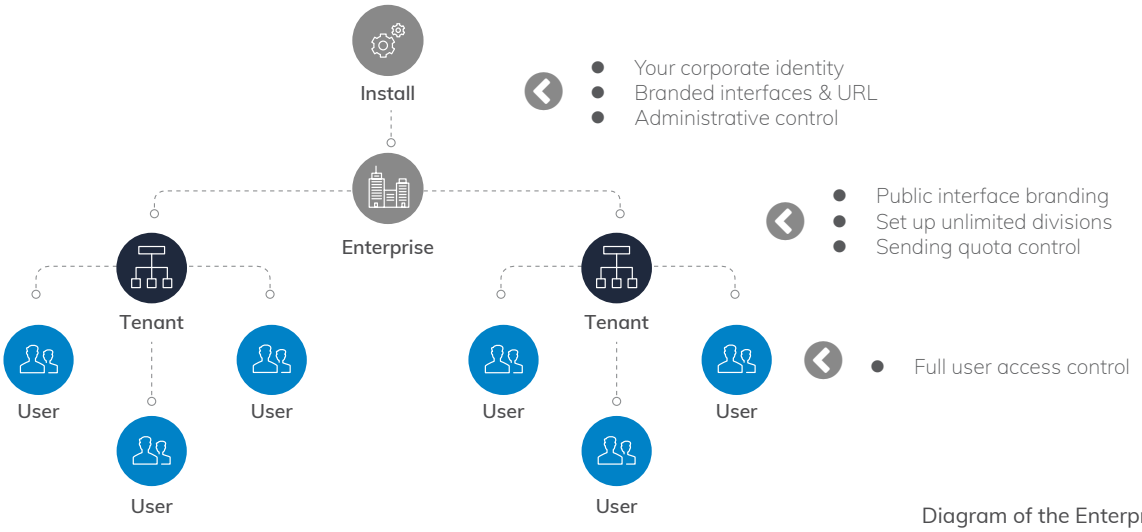


Diagram of the Enterprise Architecture

2.5 Data Backups

As we handle extremely sensitive data, we have taken every precaution to safeguard our clients' data.

Backups
All backups are treated as private and confidential. No data will be shared with a third party unless we are legally obligated to. All backups, both onsite and offsite, are stored in a secure private location, and backed-up files are encrypted at rest.
Daily Backups
We do daily snapshot backups for every account holder. All data is backed up, including contact data, messages, and reports. These daily backups are kept onsite for 30 days. We perform two types of backups: physical and logical. With physical backups, we backup the entire server and data on site and remotely. With logical backups, we backup the database exclusively, both locally and remotely.
Offsite Backups (Weekly)
Complete weekly backups are performed for every account. These backups are stored offsite for 90 days.
Encryption
Data is stored in a Relational Database, which is only accessible with username, password, and firewall access.

Although the data is not encrypted at rest, it is stored in the files of the database management system, MySQL Enterprise, and cannot be accessed from the database unless the necessary login details are correct. The database servers exist behind a secure firewall and root access to the servers is not possible.

- **Secure ISP:** Our internet service provider uses the highest security protocol.
- **SFTP:** We transfer files using a secure data stream.
- **HTTPS:** This secure layer encrypts and decrypts user page requests and pages returned by the server.
- **Secure MTA:** Our MTA uses strict security measures to make sure all messages are secure during transfer.

2.6 API Use & Security

We offer a full range of API methods to integrate external data sources and expose all the raw data produced by the platform. The range includes data submission and manipulation, campaign dispatch, and analytics for both email and SMS respectively.

To integrate with the system via our API platform, an API key and a URL are required. All API calls are authenticated via the unique API key.

- **API Key:** The API key is generated on the user profile. API keys are generated per user.
- **URL:** The URL used by each user to access their software. We validate all API commands to ensure that the values given are correct.

We monitor the use of the API to ensure no abuse of the API. Please refer to API use policy.

HTTPS
To keep things as simple as possible, we use Basic Authentication on all our endpoints. Here are some of the reasons why:

- **Security:** Because we enforce SSL, the basic authentication headers are encrypted in transit.
- **Speed:** Because of the increased security, requests using Basic Authentication can send the user's credentials in the initial requests, instead of having an extra request to negotiate the connection each time.
- **Simplicity:** Basic Authentication is simple and easy to implement. It's also widely supported by libraries, browsers, and frameworks.

2.7 Application Access Control

We use industry-standard procedures and protocols to ensure the highest levels of access control.

Secure Login
We take every possible precaution to ensure that only authorised parties can log into the system. Users have the option to enable multi-factor authentication as well.

IP Locking
As with browser-based access to the system, the API access can also be locked to your IP, so it is only available to users on your network.

Passwords
- For security reasons, we do not share the specifics of application password encryption. At a high level, our passwords are double encrypted, and only forward validation is possible.
- All passwords are encrypted, including those used for API integrations. The passwords are encrypted in such a way that they can't be decrypted.
- Users can change their password within the application using the 'forgot password' function. A user can only change his or her password this way.
- Furthermore, the "Remember Me" function has a rotating authentication key.
- Passwords are bound by length and complexity requirements.

Brute Force Attack Prevention
Our authentication system detects and limits the effectiveness of a brute force attack.

Failed Login Notifications
Administrators can set up notifications on failed login attempts on their account.

User Access Control
User access is managed at the application level. The client nominates an internal Enterprise Administrator who can define normal user access, user rights, and passwords. Access to subsets of features can be accommodated by creating users with access to silos of information, housed per department in the product hierarchy. IP restriction per enterprise is available on request.

Administrator
Admin users can change their passwords, access message reports, and create new messages. These users have additional rights:

- Enterprise users have access to all tenants through remote login.
- They can change another user's password, but not view it.
- Admin users can create additional tenants and users.
- They can also define user access rights.

Normal users can edit their user information and password.

User Access Rights can be set by the Administrator.

Properties | Settings | Access Rights

Contacts

	Allow all	Access	View	Add	Edit	Delete	Search	Report	Notification	Duplicates	Bounces
Contacts	☐	☑	☑	☑	☑	☑	☑	☑	☑		☑
Lists	☐	☑	☑	☑	☑	☑					
List groups	☐	☑	☑	☑	☑	☑					
Bulk update	☐	☑						☑			
Import	☐	☑							☑	☑	
Export	☐	☑									

Super Administrator
The Super Administrator is a special user that has full access to the system. Use of this account is restricted to specific staff. Each authorised staff member has their own super administrator login details for monitoring purposes. Staff are notified immediately if a super admin password is changed. Any unauthorised changes will result in the user immediately being disabled.

2.8 Application Monitoring

Access logs
We log each and every user access to the system and analyse these logs for exceptional behaviour.

Audit Logs
There are two levels of audit trails:

1. **User audit trails:** Related to login, message creation, contact imports, exports and deletion.
2. **Subscriber audit trails:** Subscriber activity with the system is logged and available for inspection via the interface.

Information Systems Acquisition, Incident, and Development Maintenance

- Data input validation is employed on applications to ensure that all data is validated and appropriate.
- We use key management to support our cryptographic techniques.
- We regularly obtain timely updates about possible technical vulnerabilities in our system.
- Whenever a vulnerability is discovered, we take immediate action to mitigate any associated risk.
- We have technology in place to protect against web application security threats, distributed denial of service attacks, and infrastructure-related threats.
- Formal information-security-event reporting procedures, incident response, and escalation procedures have been developed and implemented.

Business Continuity Management

- We identify events that cause interruption to business process, along with the probability and impact of such interruptions, and their consequence for information security.
- We develop plans to maintain and restore business operations, and ensure availability of information at the required level, within the required time frame following an interruption or failure of our business processes.

2.9 Disaster Recovery

Backups are scheduled to run after working hours and start at around midnight daily, weekly, and monthly. These backups are also automated, verified, and encrypted, and are stored in the data centre and remotely / off site. Incidents that cause major power / system outages and internet disconnections are of the highest priority, and we ensure that the Client's use of the Software, as well as the Client's data, is factored into the overall Disaster Recovery Plan.

There are three levels of disaster recovery planning:

1. Single Server Failure
If a single web server goes down, our load balancer automatically stops sending traffic to the failing server and diverts traffic to the healthy one. Such switchovers are automatic and take no longer than 32 seconds. For our database servers, no failover is available as yet as we are currently in the process of migrating to Microsoft Azure. However, we will rely on our two backups, specifically the full-server backup, should an incident occur.

2. Complete Component Failure
- In the very unlikely event of a complete component failing (like our web cluster), we have a 12-hour SLA with our ISP on repairing boxes. If it is impossible to restore the node of a cluster, a new node will be installed, and the data will be restored from a backup.
- We perform backups every 24 hours. Restore time for a complete component failure is 24 hours but, based on our distributed infrastructure, it's extremely unlikely that this will happen.

3. Site Failure
In the unlikely event of a nuclear bomb, or the complete destruction of our ISP, the entire product can be restored from offsite backups. Restore time for complete site failure is a maximum of 48 hours.

2.10 Tests and Audits

We conduct monthly vulnerability testing on our internal networks and servers, with additional testing after each upgrade. Additionally, we continually monitor our systems and alert security staff of any malicious activity.

Annual penetration tests are conducted by Vox. We also had an external service provider perform a penetration test, our recent test was done by Sensepost in 2018 and our next one is scheduled to be concluded before the end of this year.

2.11 Error Logs

We have exception handling at all layers of the product. Verbose errors are only logged to a secure and private location;they are never displayed to the public.

Overview of Controls & Internal Access to Client Data

Section 3

Access to client data from within our company is limited to essential staff who are required to access our systems for client service or maintenance purposes. This section outlines the measures that we have taken to ensure client data is kept safe, even within the office.

3.1 Physical Access to the Office

We employ the following physical safety measures within our office:

- Gated security
- Keycard entry
- Receptionist to identify / welcome anyone who does not have access
- Receptionist to ensure all visitors sign our visitor register
- CCTV

These access records and procedures are reviewed by management regularly.

3.2 Staff

In general, all support staff and assigned client relationship managers have access to client data to support clients. These employees are moderated by their employment contracts, and the gravity of their access rights is re-enforced during induction. Access is physically restricted to the office through IP restriction; only staff on our IP network can access client data. Furthermore, staff members can only access client data if they have permission to do so.

All staff and contractors attest to terms and conditions that specifically outline privacy, information security, and confidentiality. Staff are also trained yearly on the following:

- Compliancy
- General procedures
- Paper records
- Email and personal productivity software
- Electronic remote access
- Laptops / notebooks
- Mobile storage devices
- Data transfer
- Monitoring
- Breach management

3.3 Employee, Contractor & Service Provider Procedures

- Background checks (including criminal record checks) are conducted on all staff and contractors before they are hired.
- Personnel who retire, transfer from any internal department, resign etc. are removed immediately from mailing lists and access control lists. Relevant changes also occur when staff transfer to other internal assignments.
- New staff are carefully coached and trained before being allowed to access confidential or personal files.
- Contractors, consultants, and external service providers employed by us are subject to a strict formal contract in line with the provisions of the POPI Act. The terms of the contract, and undertakings given, are reviewed and audited to ensure compliance. External partners are never given permission to client data unless approved by the client in writing.
- We have an up-to-date Acceptable Usage Policy relating to the use of any office technology and software (e.g. telephone, mobile phone, fax, email, internet, intranet, and remote access, etc.) by its staff. This policy is understood and signed by each user of such technology.
- Staff ensure that callers to the office or other unauthorised persons are unable to view personal or sensitive information, whether held on paper documents or information displayed on PC monitors, etc.
- All staff ensure that PCs are logged off or 'locked' when left unattended. Where possible, staff are restricted from saving files to the local disk. Users are instructed to only save files to their allocated network drive.

3.4 Policies & Controls for Unauthorised Access to Client Information

Paper Records

- Paper records and files containing personal data are handled in such a way as to restrict access to only those persons with business reasons to access them.
- We shred all paper records that contain confidential information. Other secure disposal methods are in place and properly used for confidential material not on paper.
- Facsimile technology (fax machines) are not used for transmitting documents containing personal data.
- Papers with confidential data are locked away when not in use.

Email & Personal Productivity Software

- Standard unencrypted email is never used to transmit data of a personal or sensitive nature. Clients who wish to use email to transfer such data must ensure that personal or sensitive information is encrypted or password protected, either through file encryption or through the use of a secure email facility that encrypts the data (including attachments) being sent.
- We scan and flag outgoing emails and attachments for keywords that indicate the presence of sensitive data such as banking and credit card details.

Remote Access

When accessing this data remotely, it is done via a secure encrypted link via an SSL VPN tunnel with relevant access controls in place. Stringent security and access controls, such as strong passwords, are used for an additional layer of protection.

We use technologies that provide for the automatic deletion of temporary files that may be stored on remote machines by its operating system.

We ensure that only known machines (whether desktop PC, laptop, mobile phone, PDA, etc.) configured appropriately with up-to-date anti-virus and anti-spyware software can remotely access centrally held personal or sensitive data.

Laptops & Other Mobile Storage Devices
All portable devices are password-protected to prevent unauthorised use of the device and unauthorised access to information held on the device. Passwords used to access PCs, applications, databases, etc. are of sufficient strength to deter password cracking or guessing attacks. We instruct employees to create a password that includes numbers, symbols, and both upper and lowercase letters.

Personal, private, sensitive, or confidential data is not stored on portable devices. Laptops are physically secured if left in the office overnight. When out of the office, the device is kept secure at all times. When replacing or selling laptops, hard drives are formatted and sanitised with a hard drive degausser program.

Data Transmissions
Data transfers only take place via secure online channels where the data is encrypted rather than copying to media for transportation. In general, we do not employ manual data transfers using removable physical media (e.g. memory sticks, CDs, tapes, etc.). However, in the event it is absolutely necessary, any such encrypted media will be accompanied by a member of our staff delivered directly to, and be signed for, by the intended recipient.

Monitoring
We ensure that all systems are protected by appropriate firewall technologies, that this technology is kept up to date, and is sufficient to meet emerging threats.

Access to files containing personal data is monitored by supervisors on an ongoing basis. Staff is made aware that this is done. IT systems are in place to support this supervision.

We also take the below precautions:
- Privileges are allocated on a need-to-use basis, and only after a formal authorisation process.
- User access rights are reviewed at regular intervals.
- Users are advised on how to select and maintain secure passwords.
- Users and sub-contractors are made aware of the security requirements and procedures for protecting unattended equipment.
- Inactive sessions are shut down after a defined period of inactivity.

Reports & Incidents
We have a breach management plan to follow should an incident occur. There are five elements:

1. Identification and Classification
2. Containment and Recovery
3. Risk Assessment
4. Notification of Breach
5. Evaluation and Response

Identification and Classification
Though we do everything technologically to ensure data security, we have also put procedures in place that allow any staff member to report an information security incident. For instance, staff are aware they should report such an incident to the Information Officer within 72 hours of being made aware of the breach. This allows for early recognition of the incident so it can be dealt with appropriately. The report is then reviewed by the Information Officer to confirm if a breach has occurred.

Containment and Recovery
This step limits the scope and impact of the breach of data protection procedures. If a breach occurs, the Information Officer:
- Investigates the breach and ensures that the appropriate resources are made available for the investigation.
- Establishes who in the organisation needs to be made aware of the breach and begins the containment exercise.
- Establishes whether there is anything that can be done to recover losses and limits the damage the breach can cause.

Risk Assessment
In assessing the risk arising from a data security breach, the Information Officer will consider what the potential adverse consequences are for individuals (i.e. how likely it is that adverse consequences will materialise) and, in the event of them materialising, how serious or substantial are they likely to be.

Notification of Breaches
If inappropriate release / loss of personal data occurs, it is reported immediately internally, to the Data Protection Office, and, if appropriate in the circumstances, to the persons whose data it is. When notifying individuals, we use the most appropriate medium to do so.

Evaluation and Response
Subsequent to any information security breach, a thorough review of the incident occurs. This ensures that the steps taken during the incident were appropriate and identifies potential areas for improvement.