# Contents

# 1. Introduction & Overview

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 March 2016.

In compliance with POPI, Everlytic has two roles and responsibilities:

- We are the responsible party regarding the client's personal information, such as email addresses, phone numbers, billing details, and other information used to do business with clients.
- We are the service provider, or operator regarding the personal information that the client provides 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'll 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. If you cancel your services with Everlytic we will delete your personal information, except for statistics which we store in a de-identified and aggregated manner.
- **Accountability and Security:** We take measures to ensure data is kept safe and prevent loss of, damage to, or unauthorized destruction of personal information, and unlawful access to or processing of personal information.
- **Access:** We'll give you access to any of your personal information that you request, unless the request is unlawful.

The client's required NDAs are generally accepted without issue. Client data is always treated as confidential and for the sole purpose of rendering services to you.

## 1.2 Compliance

Everlytic is compliant with the following:

- **Protection of Personal Information Act (POPI)**
- **CPA Section 11**
- **Electronic Communications Act of 2002 (ECT)**

## 1.3 Information Request

- 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, Everlytic encourages you to correct, update, or remove the personal information that you provided. This can be done by contacting us.
- In the unlikely event that a data subject (i.e. a contact in your email 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

## 1.4 How to Contact Us

Our Information Officer is: **Walter Penfold**, *Managing Director*

Please relay any questions you may have pertaining to our above stated policies to our Support Department by emailing us at **privacy@everlytic.com**

Other means of contact:

Everlytic Privacy Department;

Address: P.O. Box 1653, Parklands, 2121, South Africa;

Tel: +27 (0)11 447 6147

## 1.5 Changes to This Policy

If we make any material changes, we will notify you by email or by providing the revised privacy policy in your account within Everlytic. Your continued use of our services following the update means that you accept Everlytic's updated POPI Compliance & Security Policy.

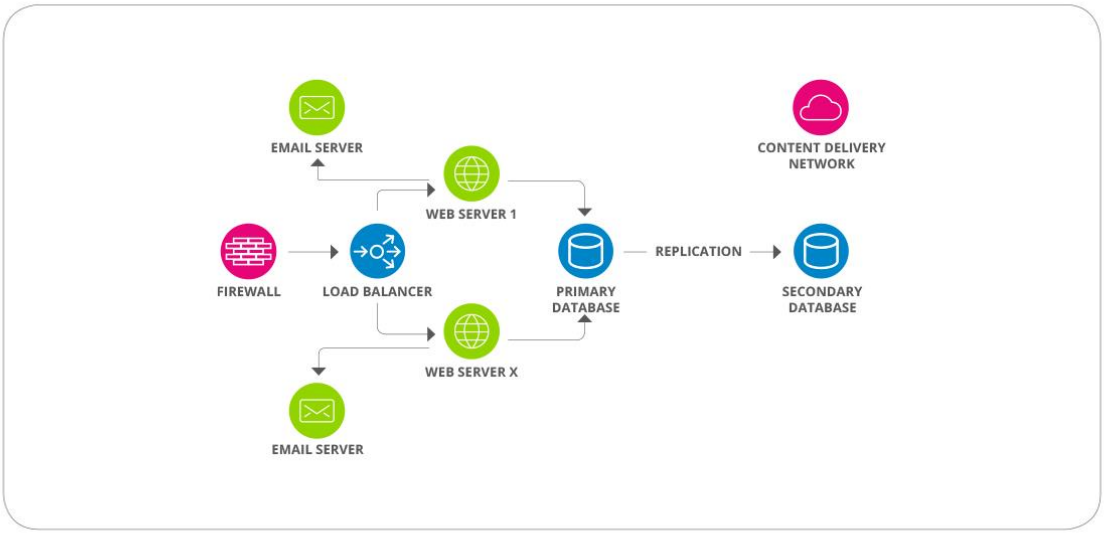
# 2. Server and Application Security

## 2.1 Server Setup

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

- Web servers.
- Database servers.
    - Our data is hosted by Edge in the United States and Internet Solutions 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 which enter our intrusion prevention and detection systems (IPS/IDS) go through a deep packet inspection, and are analysed for legitimacy.

Edge'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 the Internet Solutions servers, packets are inspected in real time using a Redundant Layer 7 Firewall Appliance and rules are dynamically created dependent on kinds of attacks to the system.

### Dedicated Firewalls

Firewalls limit ingress and egress traffic, perform state full packet inspections, and establish VPN connectivity to your offices and for remote users.

Edge uses 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.

IS uses dedicated high-performance Cloud Core Mikrotik firewalls. Unique client VLANs achieve complete isolation between environments.

## 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 client may choose to host locally or internationally.

The Edge data centres are hosted in the United States. Choosing the international hosting option offers highest speeds, and cost benefits.

For local hosting, we use Internet Solutions. South African hosting comes at a small premium, but ensures that you will comply with legal restrictions on data housing location.

### Logical Separation

Data is logically separated but not physically. Data is clearly segregated inside the solution however. Our database structure is a relational database and each contact record contains a relational customer key. Customers 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.

## 2.3 Physical Security - Physical Access to Data Center

### Prior to Data Center

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

### Data Centre Security and Facility Access Rights

- Restricted access to the data center 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 center access.

### Tracking

- Live monitoring of accesses.
- Digital log of door accesses.
- Written visitor log in restricted data center 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

Everlytic 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.

#### Cross-site Scripting Attacks

All input is validated and type cast to ensure input data is valid. Additionally, all queries run on the database use bound parameters (a method of escaping input) or MySQL escaped strings to prevent SQL injections.

#### 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 that 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.

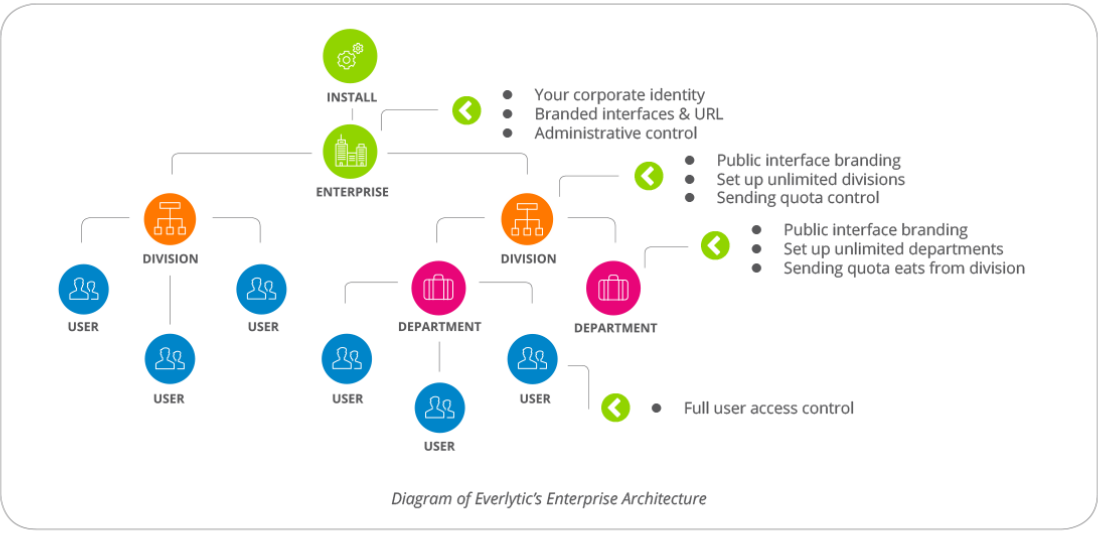



*Diagram of Everlytic's Enterprise Architecture*

## 2.5 Data Replication and Backup

As we handle extremely sensitive data, we have taken every precaution to safeguard our client's 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 backups files are encrypted at rest.

### Replication (Daily)

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.


**SQL Dump**

In addition to live replication we do a daily SQL dump of the databases.

**Offsite Backups (Weekly)**

Complete weekly backups are performed for every account. These backups are stored offsite for 180 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:** Everlytic transfers 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 and Security

Everlytic offers 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.

In order to integrate with Everlytic 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 Everlytic software.

Everlytic validates all API commands to ensure that the values given are correct.

Everlytic monitors 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 HTTP Authentication on all of our endpoints. Here are some of the reasons why:

- **Security:** Basic Authentication uses bcrypt encryption, which is more secure than the md5 encryption used by Digest Authentication
- **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.

### IP Locking

As with browser-based access to Everlytic, the API access can also be locked to your IP so that 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. No other user's details can be changed.

Furthermore, the "Remember Me" function has a rotating authentication key.

### 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.

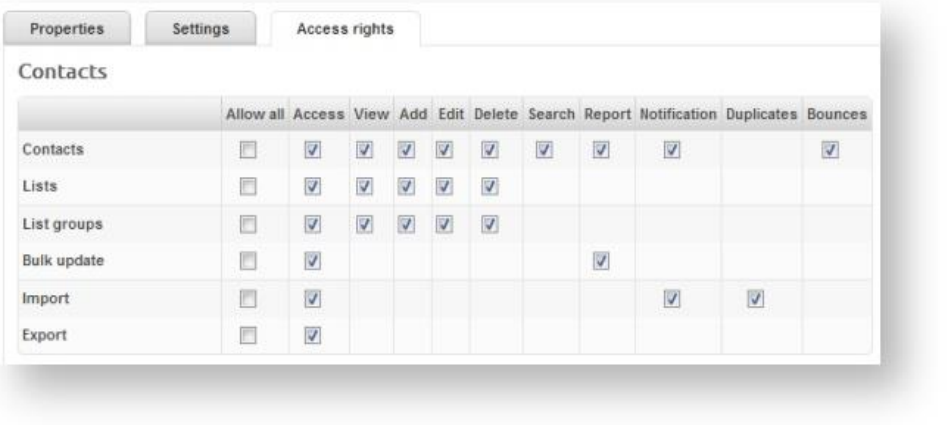
### User Access Control

User access is managed at the application level. The client nominates an internal Enterprise Administrator who has the ability to define normal user's access, user rights, and passwords. Access to subsets of data 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 departments through remote login.
- They can change another user's password, but not view it.
- Admin users can create additional departments and users
- They can also define other user access and rights




Normal users can edit their user information and password. These users can access and send emails/SMSes, and modify the imported data of the department they have access to.

**Super Administrator**

The super administrator is a special user that has full access to Everlytic. Use of this account is restricted to specific staff at Everlytic.

Everlytic staff is 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:

- **User audit trails**: Related to login, message creation, contact imports, and contact exports.
- **Subscriber audit trails**: All subscriber activity with Everlytic 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 correct 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.
- We have a formal information security event reporting procedure, incident response, and escalation procedures 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.
- We plan and consider the identification and agreement of responsibilities, and acceptable loss. We implement and document recovery and restoration procedures, and perform regular testing of all procedures mentioned in this section.

## 2.9 Disaster Recovery

Everlytic has three levels of disaster recovery planning:

**Single Server Failure**

If a single server from any one of our components goes down (including web, database, or mail transfer agent), our load balancer will automatically stop sending traffic to the failing server, and will divert traffic to the healthy server. Such switchovers are automatic and take no longer than 32 seconds. We have a 12 hour SLA with our ISP on replacing hardware in our servers and once the faulty server is repaired and tested the load balancer will automatically deliver traffic to both servers.

**Complete Component Failure**

In the very unlikely event of a complete component failing (like our entire database cluster or 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 which are then replicated off site. Restore time for a complete component failure is 24 hours but, based on our distributed infrastructure, it's extremely unlikely that this will happen.

**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 weekly penetration 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.

Our **external** servers have been audited by Microsoft South Africa, and we passed all requirements.

External verifications are not currently conducted. However, the company is open to them.

## 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.

# 3. Overview of Controls and Internal Access to Client Data

Access to client data from within our company is limited to essential staff that are required to access our systems for client service or maintenance purposes. This section outlines the measures that Everlytic has taken to ensure client data is kept safe even within the walls of Everlytic offices.

## 3.1 Physical Access to Everlytic Office

We employ the following physical safety measures within our office:

- Gated security
- Keypad entry
- Receptionist to identify/welcome anyone who does not have access
- CCTV

These access records and procedures are reviewed by management regularly.

## 3.2 Everlytic Staff

In general, the client is assigned a senior account manager and they will have access to client data in order to support their 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 Everlytic 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 Everlytic staff and contractors attest to terms and conditions that specifically outline privacy, information security, and confidentiality.

Everlytic staff are also trained yearly on the following:

- 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, and Service Provider Procedures

- Background checks that include a criminal record and credit check 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 transfers 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 Everlytic are subject to strict a 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

- Everlytic has an up-to-date Acceptable Usage Policy in relation 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 at Everlytic

- Staff ensures 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 ensures that PCs are logged off or 'locked' when left unattended for any period of time. Where possible, staff is restricted from saving files to the local disk. Users are instructed to only save files to their allocated network drive.

-

## 3.4 Everlytic Policies and Controls for Unauthorized 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.

Everlytic shreds 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 and Personal Productivity Software**

Standard unencrypted email is never used to transmit any data of a personal or sensitive nature. Clients that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted, either through file encryption or through the use of a secure email facility which will encrypt the data (including any attachments) being sent.

Where personal or sensitive data is held on applications and databases with relevant security and access controls in place, additional controls prevent such data from being copied to personal productivity software (i.e., Dropbox, Drive etc.).

Everlytic scans outgoing emails and attachments for keywords that would indicate the presence of personal data and, if appropriate, prevent its transmission.

**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.

Everlytic utilises technologies that will provide for the automatic deletion of temporary files which may be stored on remote machines by its operating system

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

**Laptops and 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, upper and lowercase letters. Passwords are changed every 90 days.

Personal, private, sensitive, or confidential data are 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.

Staff-owned devices, such as portable media players (e.g. iPods, etc.), digital cameras, USB sticks, etc., are technologically restricted from connecting to Everlytic-owned computers. Everlytic implements procedures that will ensure that personal data held on mobile storage devices is fully deleted when the data is no longer required.

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 on-line 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 Everlytic staff delivered directly to, and be signed for by the intended recipient.

**Monitoring**

Everlytic ensures that all systems are protected by appropriate firewall technologies and that this technology is kept up-to-date and is sufficient to meet emerging threats.

Audit trails are used where technically possible, to capture instances of inappropriate access (whether internal or external), addition, deletion, or editing of data.

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

Everlytic also takes 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:

- Identification and Classification
- Containment and Recovery
- Risk Assessment
- Notification of Breach
- Evaluation and Response

## Identification and Classification

Though Everlytic does everything technologically to ensure data security, we have also put in place procedures that will allow any staff member to report an information security incident. Staff are aware they should report such an incident to the Information Officer. This allows for early recognition of the incident so that it can be dealt with in the most appropriate manner. The report is then reviewed by the Information Officer to confirm if a breach has actually 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 would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of 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, both internally and to the Data Protection Office and, if appropriate in the circumstances, to the persons whose data it is. When notifying individuals, Everlytic will consider using the most appropriate medium to do so.

## Evaluation and Response

Subsequent to any information security breach a thorough review of the incident will occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.