Data Protection Compliance & Security Policy

Amazon Web Services (AWS)

Index

Section 1 - Introduction & Overview

Section 2 - Server & Application Security

Section 3 - Overview of Controls & Internal Access to Client Data

Introduction & Overview

Section 1

This Data Protection Compliance and Security Policy describes how we handle your and your subscribers' information when you use our software and services. This Policy was last revised on 14 March 2021 - date changes are implemented.

In compliance with the relevant data protection legislation, Everlytic has two distinct roles and responsibilities:

- We are the Responsible Party / Controller 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 Operator / Processor regarding the Personal Information that the client uploads in the form of a database, distribution list, or the like, as we process Personal Information on your behalf.

For simplicity, the following terms shall have the meaning ascribed to them below:

- **"Responsible Party"** means a public or private body, or any other person who, alone or in conjunction with any other party determines the purpose of and means for processing Personal Information;
- **"Operator"** means a person who processes Personal Information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party;
- **"Personal Information"** means any Personal Information relating to an identifiable, living, natural person and where it is applicable, an identifiable, existing juristic person.

1.1 Privacy Principles

As your service provider, stewardship of your data is critical to us and it's a responsibility that we embrace. We abide by the following internal principles when collecting, recording, storing, disseminating, and destroying Personal Information, and when responding to official 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, in accordance with the requirements of Section 20 and 21 of POPIA and Art. 28 and 29 of the EU-GDPR and UK-GDPR.

1.2 Compliance

Everlytic is compliant with the following legislation:

- The EU-General Data Protection Regulation 2016/679 (EU-GDPR);
- The UK-General Data Protection Regulation (UK-GDPR);
- The Protection of Personal Information Act, 4 of 2013 (POPIA);
- The Consumer Protection Act, 68 of 2008 (CPA);
- Electronic Communications and Transactions Act 25 of 2002 (ECTA).

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, Everlytic encourages 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 Everlytic): Notification will be sent to the Responsible Party. Everlytic's 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, which is construed strictly in accordance with both Section 22 of POPIA and Art. 33(2) of the UK-GDPR and UK-GDPR.

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

1.4 How to Contact Us

If you would like to access, correct, amend, or delete any Personal Information we have about you, register a complaint, or simply want more information, contact our compliance department, compliance@everlytic.com, your client relationship manager, support@everlytic.com, or by post to Everlytic.

Physical Address: Block B2, Rutherford Estate, 1 Scott Street, Waverley, 2090
Postal Address: PO Box 522106, Rosebank, 2196, South Africa

Please relay any questions you have pertaining to our above-stated policies to our Compliance or Support Department by emailing us at compliance@everlytic.com or support@everlytic.com or call our office on +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 policy on our website. Your continued use of our services following the update means that you accept Everlytic's updated Data Protection Compliance & Security Policy.

Server & Application Security

Section 2

2.1 Server Setup

Our servers are set up in AWS and are architectured using a container orchestration system, ensuring high availability, scalability, and data security. Our server setup includes the following:

Cloudflare WAF Layer: All requests pass through Cloudflare's Web Application firewall.

We use Cloudflare's Web Application Firewall for all incoming http requests, which filters out traffic based on sets of rules. This offers the following security defenses:

- Protection from zero-day vulnerabilities
- Core OWASP rules to block the top 10 attack techniques
- Sensitive data detection alerts
- DDOS Protection

AWS Shield

AWS Shield's always-on detection and mitigation systems automatically scrub bad traffic at Layer 3 and 4 to protect our application from infrastructure layer attacks, such as SYN floods, UDP floods, etc.

- **Public Layer:** This layer consists of our network load balancers and is the only layer that interfaces with the public on specific open ports.
- **Application Layer:** This is a private layer that contains our cluster management nodes, as well as our containerised application instances.
- **Database Layer:** This is a private layer where the data is stored on managed RDS instances.

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 every activity and 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.

MTAs are hosted with Vox Telecommunications ("Vox") on the Teraco infrastructure.

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.

Vault

Application runtime secrets and credentials are securely stored in a Secrets Management System. At rest, all secrets and credentials are encrypted using a secure AWS Key Management Service key. When in use, the secrets are decrypted and stored in a protected memory region within the Secrets Management System. At runtime, secrets are securely transmitted to an application instance and stored in an in-memory filesystem. At no point are secrets stored unencrypted on disk.

Containerisation

Application instances are deployed using industry-standard Linux container isolation. Each application instance is isolated from other instances. The root filesystem of the container is configured to be read-only, preventing unauthorised filesystem changes. Container images utilise a minimal base operating system with a focus on security, Alpine Linux. Automated scanning of application container images is used to detect vulnerabilities in system-level dependencies before deployment.

Principle of Least Privilege

All our servers are set up using the principle of least privilege as a security measure. Our application nodes run in containers with read-only permissions sets.

Compliance Certification

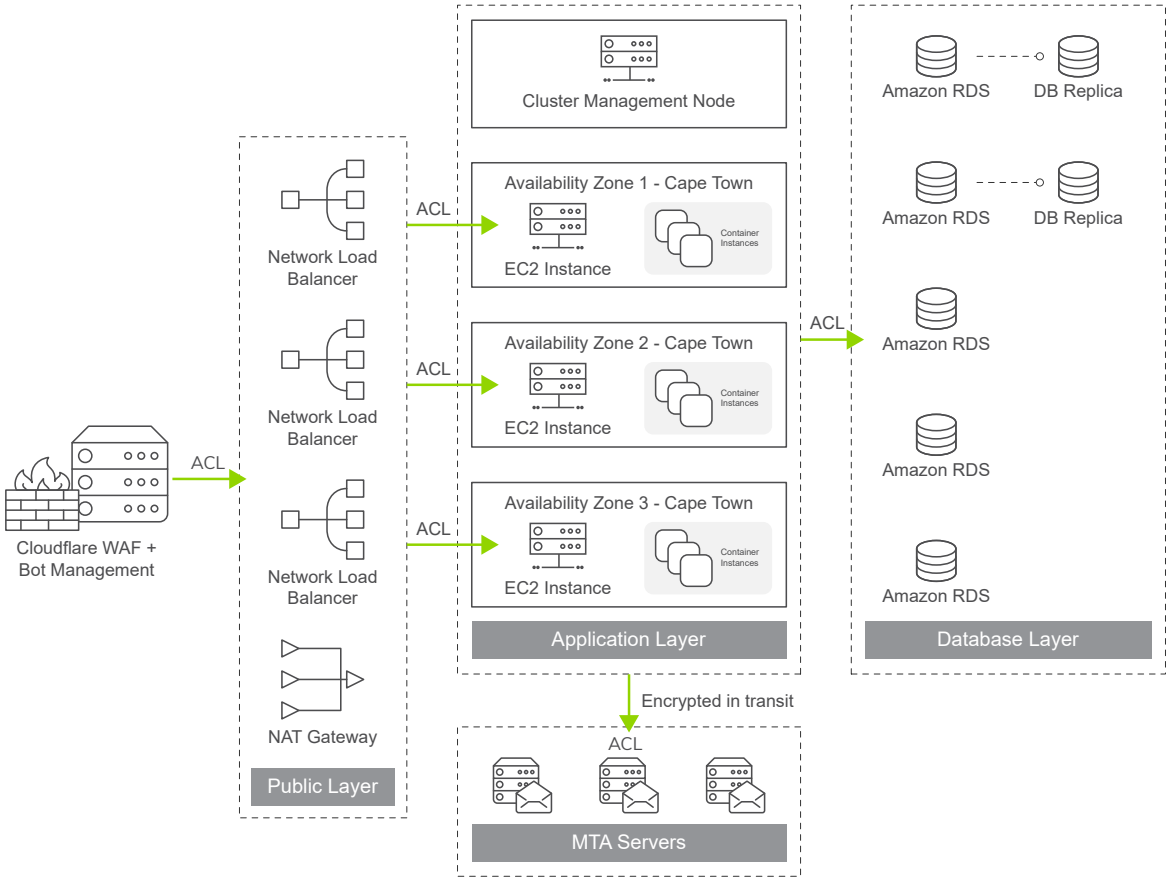
Regarding our infrastructure hosted with AWS, our certifications include:

1. ISO/IEC 27001:2013, 27017:2015, 27018:2019, 27701:2019, 9001:2015 Certification
2. CSA STAR CCM v3.0.1
3. SOC 1, SOC2 and SOC3 Certification

4. PCI Certification
5. FedRAMP Certification
6. HIPAA BAA Certification

Regarding our MTAs hosted with Teraco via Vox, our certifications include:

7. PCI Certification
8. ISO 27001:2013 and 9001:2015 Certifications
9. ISEA 3402



*Everlytic routinely evaluates and rationalises its active AWS assets of which an inventory is available via the AWS interface.

2.2 Data Storage

Our data storage is handled in the following manner:

Data Hosting

We use managed RDS instances to store and manage data. This follows strict compliance and governance rules managed by the Amazon RDS team. Amazon RDS handles routine database tasks such as provisioning, automatic software patching, backups, recovery, and failure detection. Currently, our databases reside in South Africa, with potential options to host in any AWS data centre in the world.

The following is a list of reasons we chose Amazon RDS for our data storage:

1. **Scalability:** We are able to scale our compute and storage with the click of a button.
2. **High Availability:** The Amazon RDS team will automatically replace the compute instance in the event of a hardware failure. They also provide us with an SLA and the ability to host data in multiple availability zones.
3. **Backups:** With automated backups, we are able to perform point-in-time recovery up to the last 15 minutes, should the need arise.
4. **Security:**
   a. Encryption at rest
   b. Network isolation
   c. Automatic software and OS patching
   d. Resource-level permissions
5. **Monitoring & Metrics**

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

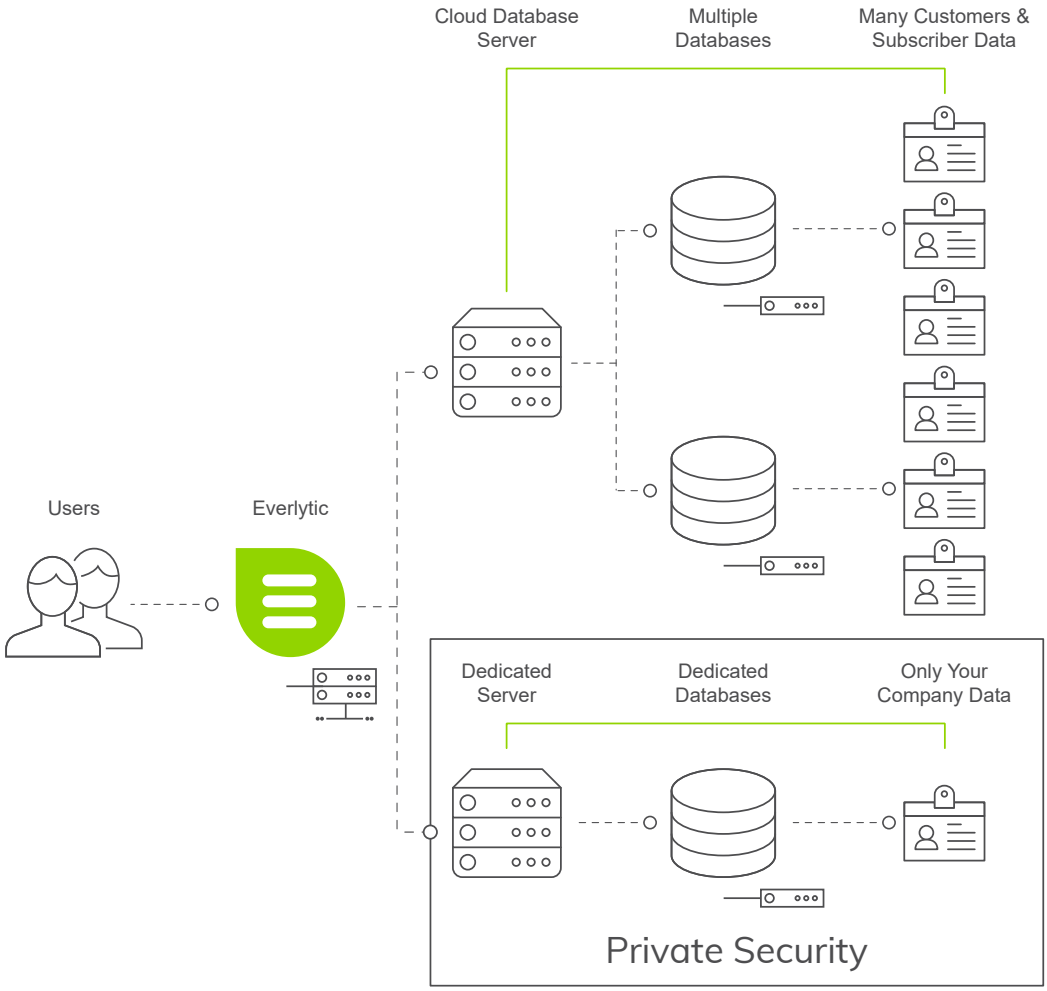
The client may request that data be stored in a separate physical database. There are various options for this, including each application being separated with separate URL logins and user credentials.

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

Everlytic's 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

Site Selection

- Careful selection of data centre locations mitigates environmental risks such as flooding, extreme weather, etc.
- Redundancy: Data centres are designed to anticipate and tolerate failure while maintaining service levels.
- Availability: Critical system components, required to maintain availability of systems and recover, are identified for use in the event of an outage.
- Capacity planning: Monitoring of service usage, so we can deploy infrastructure and support availability commitments, as required.

Data Centre Security & Facility Access Rights

- Restricted access to the data centre facility
- Keypad access
- Signs posted for restricted access to data centre
- Unique access IDs for each employee
- Employees are restricted to areas specified in their permissions
- No generic IDs granted for vendors, maintenance, or others
- Process for granting / revoking data centre access
- Periodic reconciliation of staff with data centre access

Tracking

- Live monitoring of access
- Physical access to data centres is logged, monitored, and retained
- Written visitor log in restricted data-centre area
- Camera placement at all door access points
- Camera placement at aisles / cages
- Dial and analogue, motion CCTV system
- CCTV images are retained according to legal and compliance requirements

Device Management

- Assets are centrally managed through an inventory management system
- End-of-life storage devices are decommissioned using techniques detailed in NIST 800-88

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. All queries that run on the database also use bound parameters (a method of escaping input) or SQL-escaped strings to prevent SQL injections. Additionally, we have another layer of protection against these attacks through Cloudflare.

Cross-Site Scripting Attacks

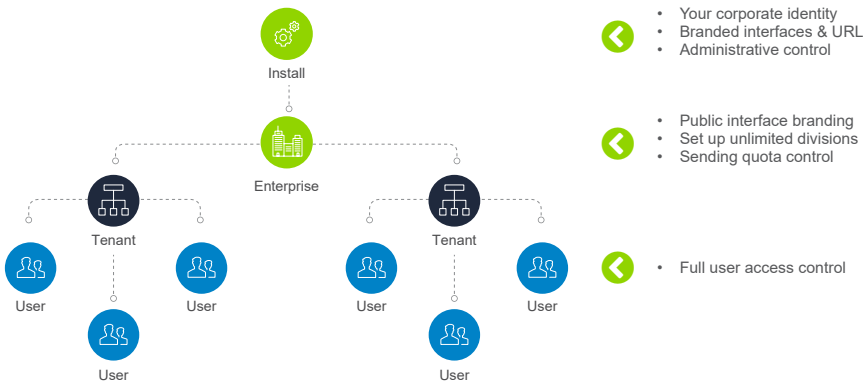
All input is validated and type cast to ensure input data is valid. Output data from the database is also sanitised before being displayed on the interface. Additionally, we include the X-XSS-Protection header in requests to enable and enforce the XSS filter built into web browsers. We also have another layer of protection against these attacks through Cloudflare.

Filesystem

The application filesystem exists as a read-only containerised node. Any customer assets are stored on a separate network drive where we apply a whitelist of allowed file types.

Session Management

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



2.5 Data Backups

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

Backups

RDS creates and saves automated backups of our databases securely in a backup vault using AWS Backup and is retained for a period of 35 days. Full daily backups are taken once a day and incremental backups are taken every 15 minutes.

Offsite Backups

Database backups are also stored across multiple availability zones within the same region to ensure proper disaster recovery.

Encryption

AWS Backup automatically encrypts our backups with a unique encryption key separate from the encryption key used for the data at REST.

2.6 API Use & 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 various communication channels.

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 that there's no abuse.

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 appropriate levels of access control.

Secure Login

We take appropriate precautions to ensure that only authorised parties can log into the system. Users have the option to enable multi-factor authentication as well, or use our AD Auth integration.

IP Locking

As with browser-based access to Everlytic, the API access and login 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
- A strong password policy is enforced
- All 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, as well as Cloudflare, 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

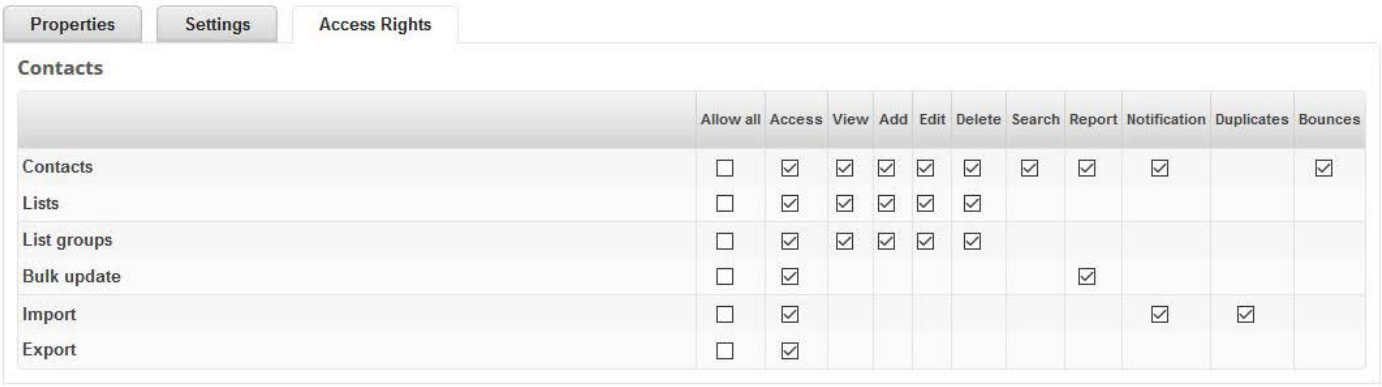
User access is managed at the application level. The client nominates an internal Enterprise Administrator who can define normal user access, user rights, and passwords. Access to subsets of features can be accommodated by creating users with access to silos of information and functions, housed per department 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, such as:

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

User Access Rights can be set by the Administrator.



Super Administrator

The Super Administrator user request and approval process is based on the principle of segregation of duties; users cannot approve their own requests. Additionally, super admin users' passwords have an increased minimum required character count and is reset on a confidential schedule. The Super Administrator is a special user who has full access to Everlytic. Use of this account is restricted to specific staff at Everlytic. Each authorised staff member has their own Super Administrator login details for monitoring purposes. Everlytic 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:

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

Application logs

We collect application logs and performance metrics to identify and respond to issues that arise within our application.

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 processes, 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. Everlytic's Business Continuity Plan is available on request.

2.9 Disaster Recovery

Everlytic's infrastructure is managed and provisioned using an Infrastructure as Code (IaC) methodology.

With regards to data, Full Data Backups are scheduled to run once daily and incremental backups every 15 minutes. These backups are automated, verified, encrypted, and are stored in the data centre and remotely, in a separate availability zone. Incidents that cause major power / system outages and internet disconnections are of the highest priority, and Everlytic ensures that the Client's use of the platform, as well as the Client's data, is factored into Everlytic's overall Disaster Recovery Plan.

Everlytic has four levels of disaster recovery planning:

1. **Application Failure**

Everlytic's infrastructure is architectured using a container orchestration system. Every application node within the load-balanced cluster is redundant and if a single application cluster node fails, traffic is routed to the remaining nodes in the clusters and a replacement node is automatically provisioned to take its place.

2. **Database Failure**

In the event that a database server failure occurs where the server becomes non-functional and is also non-recoverable, we will initiate our DR Plan to restore the database from backups. Restore time for this type of failure is 12-24 hours.

3. **Site Failure**

In the extremely unlikely event of a complete site failure, we will rely on AWS Backup to restore our databases and will run our infrastructure scripts to restore any application VMs affected in that specific availability zone. This could take up to 48 hours to complete the full restore.

4. **MTA Failure**

In the event that an unrecoverable MTA failure occurs, sending mails to those MTAs will be briefly paused. We will then switch all non-dedicated IP accounts to the remaining MTAs on our network, and resume sending for them. This risk can be mitigated within two hours and fully recovered within eight hours.

A detailed Disaster Recovery Plan is available on request.

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, which entails primary findings, remediation, and retesting.

2.11 Source Code Management

Everlytic uses GitHub as its code hosting platform for version control and collaboration. The following rules maintain code integrity and continuity:

- Branch protection - our master and release branches are only open to code owners (typically lead developers and higher designations) and developers cannot work directly off it.
- In order to merge a branch in master, all tests have to pass, and the pull request requires a review by at least two other developers.
- Any subsequent code changes require a re-approval process where the tests will be rerun and the review by two developers will need to be completed again.
- All pull requests trigger an automated test suite to run by simulating a merge of master into a development branch and then running the test suite.
- GitHub additionally scans the dependency package manager files to evaluate the vendors Everlytic is using and returns any known vulnerabilities in the software.
- It also automatically performs a pull request with the vendor updates that trigger the test suite to run, and that we can review, to include in a specific release.

2.12 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 Everlytic has taken to ensure client data is kept safe, even within Everlytic's offices.

3.1 Physical Access to Everlytic 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 Everlytic 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 restricted to the Everlytic office and VPN network 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:

- Compliance
- Privacy, including the obligations associated with Personal Information
- Cyber security

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 Everlytic are subject to a strict formal contract in line with the provisions of the relevant data protection legislation. 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.
- Everlytic has 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 at Everlytic.
- 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.
- Users are instructed to only save files to their allocated network drive.

3.4 Everlytic 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.
- 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) is 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.
- Everlytic scans and flags 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.

Anti-Malware Approach

Everlytic employs a virus prevention strategy with two main elements:

1. **End-user devices:** 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 can remotely access centrally held personal or sensitive data.
2. **Everlytic platform:** The Everlytic SaaS solution is developed on a Linux platform. A WAF prevents unauthorised access to the platform. By preventing malicious actors' unauthorised entry to the environment, together with protection against SQL injection, malware cannot enter the environment. It is common for operators of Linux environments not to deploy malware solutions inside the environment. By applying this approach, Everlytic is able to prevent malware from entering the system.

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 always kept secure. 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 that 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, 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 are made aware that this is 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 information security incident response, business continuity, and disaster recovery plans to follow should an incident occur. There are five general elements:

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

Identification and Classification

Though Everlytic applies appropriate, industry-standard technology 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 that 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.

Additionally, Everlytic applies an internal audit programme that aims to critically evaluate our information systems' governance and compliance industry standards and norms.

Containment and Recovery

Everlytic follows an Information Security Incident Response Plan which guides the appropriate handling of incidents. 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.

Everlytic's Information Security Incident Response Plan is available upon request.

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 they are likely to be.

Notification of Breaches
If inappropriate release / loss of personal data occurs, it is reported immediately internally, and if appropriate in the circumstances, to the persons whose data it is. When notifying individuals, Everlytic uses 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.