POLICY

Information Security

Last Updated: 15th December 2020

Sendmarc

1 Sturdee Avenue, Rosebank
Johannesburg
South Africa

www.sendmarc.co.za
+27 10 900 0972
info@sendmarc.com

Table of Contents

1 Overview

Sendmarc's purpose is to make the Internet a safer place.

We achieve this by enabling organisations to protect their staff, customers, suppliers, and the whole world from email phishing and spoofing attacks originating from their own domain

This document presents Sendmarc's Information Security Policy and governs all information security procedures & processes.

Sendmarc is a SAAS web application that processes DMARC reports from reporters about a customer's domain. Approval is required by the domain owner for Sendmarc to receive DMARC reports.

1.1 Purpose

The purpose of this policy is to define Sendmarc's Information Security Policy regarding the following areas:

1. Application Environment
2. Application Security
3. Disaster Recovery & Backups
4. Data Processing
5. Change Management
6. Internal Controls
7. Incident Management

1.2 Scope

Sendmarc's information Security Policy contained within this document apply to all Sendmarc employees and contractors

1.3 Legal, Regulatory and Governance

Sendmarc is compliant with the following legislative, regulatory or good governance requirements of South Africa:

1. Electronic Communications and Transactions Act
2. Consumer Protection Act
3. Criminal Procedure Act
4. Protection of Personal Information Act
5. Promotion of Access to Information Act

2 Application Environment

Our application and its services are hosted in Microsoft Azure using their high-availability, highly scalable platforms. Sendmarc's production environment is designed for maximum uptime, scalability and performance.

2.1 Server Setup

All Sendmarc services exist on a virtual private network and are not accessible outside of the Sendmarc Azure environment. Traffic on the private VLAN is fully encrypted using SSL and TLS.

Only the web application's interface is accessible publicly to authorised users through a load-balancer and firewall. The firewall has intrusion prevention technology and inspects all traffic passed onto the web application service.

The web application has built-in DDoS protection to ensure we prevent attacks on the customer portal.

Sendmarc's Azure services include the following:

- Azure Kubernetes Service (AKS) instance to run the application portal and associated workloads. https://azure.microsoft.com/en-in/services/kubernetes-service/
- MariaDB Database Service to store the structured application data. https://azure.microsoft.com/en-in/services/mariadb/
- Redis Caching service for message brokering between job queues and for in-memory storage. https://azure.microsoft.com/en-in/services/cache/
- Azure DNS service provides the backend to host system-generated DNS records. https://azure.microsoft.com/en-in/services/dns/
- File storage for file access and management – see Section 2.3

2.2 Server Access Control

Sendmarc ensures that access to services is strictly controlled. Sendmarc uses Microsoft's Active Directory to manage employee access and all sever access is controlled using 2FA.

This is consistently audited and maintained to remains in line with our internal policies. Only approved staff have access to our server infrastructure for maintenance and client service purposes.

2.3 Data Storage

All data is stored using Azure General Purpose V2 storage as described here:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview

Azure General Purpose V2 ensures the security of customer data and has redundant infrastructure which encrypts the data-at-rest as well as in-transit.

2.3.1 Data Encryption

All data-at-rest in our file storage and databases is encrypted using managed private keys. This data is decrypted when accessed and then encrypted during transit using SSL and TLS protocols.

2.3.2 Logical Separation

Data is logically separated both in the file store and the database. The application has strict controls in place to ensure that all data is segregated correctly and there is no possibility of a crossover.

2.3.3 Backups

All backups are encrypted using AES 256-bit encryption.

3 Application Security

Sendmarc been designed and developed from the ground up with the strictest security standards in mind. Principles common to web-based applications are built into every layer of the software. Industry-leading technology is used to ensure resilience to attacks and malicious use.

3.1 Attack Mitigation

The following are just some of the attacks we protect against:

- Distributed Denial of Service (DDoS) attacks – This is built into our network layer and sits in front of the public IP address to access the application.
- Cross-Site Scripting attacks – all user data displayed in the user interface is escaped to ensure that scripts cannot be executed in the browser.
- Cross-Site Request Forgery attacks – All forms contain a special key to ensure that attackers cannot attempt requests to the system outside of the product.
- SQL Injection attacks – The application validates all input for data type and structure. On top of this, all data sent to the database is escaped to prevent query execution.

3.2 HTTPS

All Sendmarc web traffic is transmitted using HTTPS. The certificates used for this encryption are automatically rotated every three months.

3.3 Application Access Control

Access to the Sendmarc application is controlled using a combination of secure user logins and user roles. The users, as well as their associated permission levels, can be controlled by an account administrator using the user management built into to application.

3.3.1 Passwords

All passwords in Sendmarc are encrypted using strong, one-way encryption algorithms. The algorithms are run using a unique salt value to ensure that the encryption is unique. Passwords are required to have a minimum length and complexity.

3.3.2 User Roles & Access Control

Sendmarc users can be limited to certain functions and areas of the product. This is done using role-based controls. The access rights are controlled by the account administrator nominated by your company.

3.3.3 Event & Activity Logging

All updates to Sendmarc data are logged with a timestamp and user identifier to allow us to build an audit trail of modifications.

Sendmarc tracks and monitors user login and password resets to detect any activity that is out of the ordinary. This allows us to prevent attacks on the system and ensure data integrity.

System errors are logged, and those logs are analysed to create reports on system health as well as potential bugs. These errors are fixed and shipped daily, maintaining the quality and dependability of the application.

3.4 Change & Quality Control

Sendmarc has services monitor performance, health, status and availability of the application. These systems automatically alert our administrators of any downtime, malicious attacks, or spikes in server load. With this real-time monitoring runs around the clock to keep the application online.

3.5 Quality Assurance

Sendmarc ships updates and bug fixes into production daily. In order to do this, while ensuring no downtime, there are several quality assurances practises that we follow.

3.5.1 Code Reviews

All code that is added to our version control system is reviewed before it can be shipped live. When performing a review, we look at the quality of the code to prevent bugs as well as ensuring the code is secure and not open to abuse.

3.5.2 Automated Testing

Our code and systems are run through a series of automated unit tests and quality assurance pipelines. If any of these fail at any point in time, the process is stopped, and administrators are alerted about the problem. Steps are then taken to resolve the issue and a post-mortem performed to prevent similar errors from occurring again.

3.5.3 System Rollback

Azure Kubernetes Service (AKS) allows us to rollback any update to the system at any point in time. If there is a problem with an update we can revert to a prior version at the click of a button.

4 Disaster Recovery & Backups

Sendmarc is hosted on Microsoft Azure hosting environment and is designed for high availability. However, there is always the possibility of a system or data centre outage. Sendmarc has implemented a fully geo-redundant system in Azure that can recover from an outage in a short amount of time. DR testing is performed every 6 months.

4.1.1 Application Redundancy

The application itself runs inside of an Azure Kubernetes Service (AKS) cluster with multiple nodes. This allows us to scale up the individual parts of the system during periods of high workloads. In addition to this, the multiple node configuration means that if one node goes down there are additional nodes in place to take over.

4.1.2 Geo-Redundant Infrastructure

Sendmarc has built a fully redundant setup with failover across geographic regions. All persistent data is replicated across at least two Azure regions ensuring availability if one data centre goes down. Along with this, our infrastructure configuration is version controlled and scripted allowing us to ensure an exact copy of our deployment during disaster recovery.

4.1.3 Backups

Our database service takes full, differential, and transaction log backups which are also geo-redundant. The backups allow us to restore the server to any point in time within a 7-day period.

5 Data Processing

Sendmarc processes the incoming DMARC reports that are generated globally by other DMARC reporterting servers. Within the DMARC specification there are two types of reports:

1. Aggregate reports
2. Forensic reports

5.1 Aggregate Reports

Aggregate Reports contain meta data on the email traffic of your domain(s) and do not contain any personal information.

The meta-data is received in an XML file formate and can include:

1. Summary of authentication results
    a. IP identified in the email
    b. Total of IP addresses identified
    c. Disposition of the message, to show if the policy was applied
    d. DKIM authentication result, the domain and result
    e. SPF authentication result, the domain and res
2. Receiving ISP information
    a. Report ID number
    b. Reporting Organisation Name
    c. Reporting Organisation sending email address and additional contact information
    d. Beginning and ending data range in seconds
3. Description of a DMARC record
    a. Header domain/from domain
    b. Alignment settings for both DKIM and SPF
    c. Domain policy (reject)
    d. Subdomain policy (reject)
    e. Percentage of messages to which the DMARC policy is to be applied

Sendmarc collects these reports and coverts all this raw data into reporting that is easier to read, analyse and use as an action list. Please refer to our Product information document for examples of what this visualised reporting looks like and how we use this data to protect your domain.

5.2 Forensic Reports

Forensic reports are optional and sent by a limited number of DMARC report senders. These are parts or copies of specific messages that failed the DMARC checks. The contents of these messages could contain Personally identifiable information (PII). Sendmarc offers 3 methods on storing these messages:

1. Default: We store the message encrypted and the message is only viewable by the client, the domain owner.
2. Encrypted: Sendmarc can provide the client with a PGP key and only the client can decrypt the Forensic Report using their private key and password,
3. No Storage: The client can request that Sendmarc does not receive or store forensic reports.

The terms of use and retention periods of the (various types of) Personal Data:

	Basic	Basic Plus	Advanced	Enterprise
Reporting & Data				
Reporting Interval	24 Hours	24 Hours	4 Hours	1 Hour
Reporting History	3 Months	3 Months	12 Months	2 Years

If a customer cancels their Sendmarc services all data will be destroyed within 14 days of cancellation.

6 Overview of Controls

Access to a client's Sendmarc services is limited to approved staff that are required to access our systems for client service or maintenance purposes. This section outlines the measures that Sendmarc has taken to ensure client data is kept safe even within the walls of Sendmarc's offices.

6.1 Identity Access

Sendmarc employs the following physical safety measures within the Sendmarc Offices

1. Gated security
2. Key Card entry
3. Biometric scanners
4. A receptionist to identify/welcome anyone who does not have access
5. CCTV

These access records and procedures are reviewed by management regularly.

6.2 Employees

Sendmarc employees can only access client data if they have permission to do so.

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

1. General procedures
2. Paper records
3. Email and personal productivity software
4. Electronic remote access
5. Laptops/Notebooks
6. Mobile storage devices
7. Data transfer
8. Breach management

6.3 Employee & Contractors

Background checks that include a criminal record and credit checks are conducted on all employees before they are hired. New employees are carefully coached and trained before being allowed to access confidential or personal files.

Employees 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 employees ensure 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 cloud drive.

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.

Negligence or malicious behaviour are required to be dealt with as follows:

1. In the case of contractors or service provider representatives, such shall immediately be escorted off-site and remediation sought in line with any contractual agreement or binding usage policy.
2. In the case of employees, the Disciplinary Process shall be invoked.
3. Law enforcement shall be informed where required, or legal action may be instituted where deemed necessary.

6.4 Network Security

Sendmarc IT Network Administrators are responsible for ensuring network infrastructure is securely designed, deployed and maintained, by adhering to all the requirements of the Sendmarc information security documentation, including the System Security Policy, and security configuration standards.

Network segregation is a key design principle that shall be implemented between networks that have different trust levels. Segregation includes appropriate segmentation of networks and implementation of network filtering, such as implemented through network filtering (firewall) access rules, between network segments of different trust levels.

Systems that have access to and are used to manage network infrastructure shall be appropriately secured and should be segmented on a network level.

6.5 WIFI

Wireless networks shall adhere to current best practice and enterprise-class configuration which includes:

Using an appropriately secure wireless security protocol to ensure the confidentiality of information transmitted over wireless networks.

Appropriately authenticating users and/or devices to wireless networks. Authentication mechanisms such as pre-shared keys (PSK) were designed for use in-home or small office environments and are not considered suitably secure for use in an enterprise environment.

Network infrastructure should appropriately log activity, including security events.

6.6 Paper Records

- Papers with confidential data are locked away when not in use.
- 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.
- Sendmarc shreds all paper records that contain confidential information. Other secure disposal methods are in place and properly used for confidential material, not on paper.
- Sendmarc does not make use of facsimile technology (fax machines) for transmitting documents containing personal data.

6.7 Email & 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.).
- Sendmarc scans outgoing emails and attachments for keywords that would indicate the presence of personal data and, if appropriate, prevent its transmission.

6.8 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.

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

Sendmarc 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.

6.9 Laptops & Mobile Storage

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 Sendmarc-owned computers. Sendmarc 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.

6.10 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 Sendmarc staff delivered directly to, and be signed for, by the intended recipient.

7 Incident Management process

7.1 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

7.2 Identification and Classification

Though Sendmarc 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.

7.3 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.

7.4 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.

7.5 Notification of Breaches

If inappropriate release/loss of personal data occurs it is reported immediately, both internally and to the Data Protection Officer and, if appropriate in the circumstances, to the persons whose data it is. When notifying individuals, Sendmarc will consider using the most appropriate medium to do so.

7.6 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.