Exclaimer

Microsoft 365 Security

An overview of the security measures used by Exclaimer
to protect its customers and their data.

Content

What is Exclaimer?

Exclaimer is a cloud hosted solution that your organization can use to centrally manage your email signatures; simplifying the process, saving yourself time, and expanding what email signatures accomplish.

Consistency is key to an effective email signature strategy and using Exclaimer guarantees fully branded and legally compliant signatures get applied to every email, which is difficult to accomplish with functionality native to Microsoft 365 and Outlook.

Built around an intuitive and straightforward user interface, Exclaimer turns management of your organizations email signatures into a straightforward and largely automated task. This includes designing email signatures, populating them with user information, and rolling these designs out to your users. Management of signatures will take less time and technical skill, resulting in the ability to delegate the work to individuals within your marketing team and the removal of bottlenecks.

For marketeers, sales teams, customer success, and many other parts of your organization, email signatures can become a new opportunity to realize the full potential of your emails. They can use signatures to communicate with important audiences and measure the impact of this engagement.

Why choose Exclaimer?

Responsible for creating the first ever solution for email signature management, Exclaimer is recognized as being best-in-class. Exclaimer provides value to its customers by being both easy-to-use and effective.

Additionally, Exclaimer is committed to being the most secure solution on the market. No other vendor can provide a similar solution with same level of security, privacy, and reliability.

Key to providing you with this assurance is the extensive, independent auditing we undertake to achieve recognized certifications, including SOC 2 Type II, ISO 27001, ISO 27018, HIPAA, Cyber Essentials and many more.

Over 50,000 customers worldwide including renowned international organizations such as NBC, the Government of Canada, and Lloyds Bank PLC, trust in Exclaimer to handle their data and process billions of business-critical emails securely on their behalf.

Compliance

SOC 2 Type II

Exclaimer has received the SOC 2 Type II attestation report that tested the operating effectiveness of Exclaimer's global systems and operations for the Trust Services Principles for Security, Availability, Confidentiality.

This report is proof that Exclaimer keeps data private and secure while processing or storing it, that data is always accessible and that specific controls are implemented to keep customer data confidential and private. The advanced type II report not only confirms Exclaimers systems and controls meet the criteria necessary but extend to monitoring continuous compliance with the Trust Principles.

ISO/IEC 27001

The ISO/IEC 27001 is an international standard on how to manage information security, providing requirements for an information security management system (ISMS).

Exclaimer has been accredited for the ISO/IEC 27001 Certification by the BSI (British Standards Institution) since 2016. Certification requires that the BSI, a third-party accredited independent auditor, regularly performs thorough assessments to confirm Exclaimer operates in alignment with ISO security standards. The standard adopts a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving your ISMS.

ISO/IEC 27018

ISO/IEC 27018 is an addition to the ISO/IEC 27001 Standard which adds over 50 new control objectives, specific to helping cloud service providers store and process Personally Identifiable Information (PII) securely. ISO/IEC 27018 specifies detailed requirements and guidelines for data processors that cover the storage, processing, and maintenance of PII in public cloud environments as well as outlining users rights relating to their data.

Technical overview

Exclaimer is comprised of multiple services hosted within Microsoft Azure that together allow for central management of email signatures for your organization. Below is an outline of these services which are explored in further detail within this document.

Server-Side

Server-Side can be used by customers to roll out their signatures across their organization. Server-Side automatically applies email signatures to emails that their organization sends, including those sent from mobile devices.

This is accomplished by processing these emails as they are sent, directing them temporarily to the Exclaimer imprinting service. Exclaimer securely applies a signature to the email, as specified by the rules established by administrators, and the email is returned to Microsoft 365 to be sent to the recipient as normal.

Client-Side

Client-Side deployment can be used to make signatures available to users within specific email clients. This method offers a more traditional user experience when compared with Server-Side, as the email signature is applied during email composition, before the email is sent.

Client-Side deployment is achieved utilizing Exclaimer's Add-In for Outlook for Windows, Mac and OWA which connects to Exclaimer to collect the signatures appropriate for the user. This ensures that end-users can both see and, where appropriate, select the email signature that is applied to their email.

User Information

The data used to populate email signatures is automatically synchronized from the Azure Active Directory to Exclaimer, where it sits encrypted at rest in a cache. This cached information can be used by Exclaimer to merge into all necessary signature designs ready for application or deployment. Once established this synchronization occurs automatically twice a day and can also be triggered manually.

In addition, using features to edit user details causes this additional data to be stored more permanently within Exclaimer used in place of the synchronized cached information.

Analytics and Feedback

On select plans, Exclaimer provides customers with additional functionality that can be used capture further data on how email recipients interact with the email signature elements attached.

When recipients engage with hyperlinks within signatures this anonymous activity is captured and stored by Exclaimer.

Similarly, when recipients engage with 1-click surveys included on a design their sentiment and any further comments are collected and stored by Exclaimer, however these can be set to be identifiable via the respondents email address.

Microsoft Azure

Exclaimer has been designed to work hosted within Microsoft Azure, which is highly trusted by IT professionals worldwide. Azure provides both scalability and flexibility and ensures that no email processed by Exclaimer ever leaves the Microsoft Cloud environment.

Knowing that online security is one of the biggest concerns for organizations when considering cloud architecture, Microsoft has designed Azure with security in mind, creating a compliance framework to meet regulatory requirements.

Exclaimer ensures that all connections are secured through SSL Certificates and TLS, which are constantly checked to meet current cloud standards. The Exclaimer Azure setup uses load balancing to provide a single network service from Exclaimer's regional Azure datacenters around the world. If one of Microsoft's Azure datacenters were to cease operating, our high-availability service ensures uptime and reliability.

Additionally, measures are in place to ensure that the service scales with increased number of tenants, maintaining reliability and uptime. Any updates to Exclaimer services hosted in Azure are scheduled to occur 'out-of-hours' for each region, minimizing any disruption. Updates are built and tested by Exclaimer's head office-based Development and Quality Assurance teams before going into production. This intensive process includes stress testing beyond normal usage, and no code is ever deployed to Azure until it has passed rigorous anti-virus checks, in addition to being scanned by native antimalware on all Azure servers.

Message Processing

When using Server-Side, email messages are securely processed for a signature by Exclaimer once sent by the sender. To accomplish this Exclaimer must be established as a proxy for sent messages, with connectors established within your Microsoft 365 tenant that can transport outgoing email messages to, and back from, the Exclaimer imprinting service.

Exchange Online Connectors

Connectors are automatically created by Exclaimer during setup, alongside a transport rule that controls when these connectors are used. One connector sends emails to be processed by Exclaimer, the other receives emails imprinted with a signature which can then be sent to the recipient as normal.

Both connectors between Microsoft 365 and the Exclaimer service use negotiated Transport Level Security (TLS) encryption to ensure the security of this connection and the data in transit. And as Exclaimer is hosted within Microsoft Azure so emails do not leave the Microsoft Cloud and continue to adhere to Microsoft's strict security standards.

By default, this transport rule will send all outgoing messages to Exclaimer to be processed, however it can easily be modified to only send selected emails, for example those sent from members of a specific mail-enabled group.

Exclaimer will only accept an email for processing when it can confirm the ability to return the email and close the loop. Should the Exclaimer service become unavailable, outgoing messages affected by the transport rule will hold in the queue until the service becomes available or the transport rule is disabled.

Exclaimer successfully applies signatures to outgoing messages without needing to behave like an MTA or SMTP relay. This means whilst your emails are sent to Exclaimer for processing, they still always exist within your queue of outgoing messages until they are sent. This ensures no message can ever be lost, due to Exclaimer's service becoming unavailable, and can always be tracked using message tracing.

Exclaimer Imprinting Service

When an email reaches the Exclaimer service, the message ‘envelope’ is automatically scanned for the subject line, sender address and recipient address, which are used to determine which, if any, signatures should be applied to the email.

Exclaimer then decodes the MIME (Multipurpose Internet Mail Extensions)/ TNEF (Transport Neutral Encapsulation Format) carrier to ascertain where the signature needs to be inserted in the email, as well as if a signature design should be disqualified based on the presence of specific text.

If the email is in the Rich Text or Plain Text format, Exclaimer will convert this email to HTML to apply a full HTML signature to it.

Next the sender's information is pulled from the cached Azure Active Directory data and any stored custom details. These details are subsequently merged into the appropriate signature design.

The signature is then inserted in the correct location in this new email, which is sent back to the Microsoft 365 tenant through the Receive connector. This attribution to the correct tenant is authenticated through use of a unique certificate.

Emails are never permanently stored by Exclaimer and exist, encrypted at rest, only for the duration required by Exclaimer to process the email. The only details regarding the email that are logged and stored by Exclaimer for 7 days are the recipient's address, sender's address and which signature was applied, which aid in troubleshooting and providing support.

If the message has received any form of encryption prior to being processed by Exclaimer (e.g. S/MIME, OME, IRM) the Exclaimer imprinting service cannot process the email and it is simply returned to be sent as standard.

Message Handling Datacenters

When normal service is running, email is processed by Exclaimer within the High Availability Cluster (HAC) in your assigned region as per our load balancing policy. This active/active configuration ensures reliability, resiliency, and high performance of the service.

In the rare event of an issue occurring that stops the signature imprinting service at one of Exclaimer's Microsoft Azure datacenters, Exclaimer has a comprehensive method in place that ensures mail flow continues to occur as normal through the alternate datacenter automatically. The primary goal is to maintain mail flow for all Exclaimer customers. Exclaimer can through this practice, as well as additional state-of-the-art tools and technologies, ensure 99.99% service availability for all of its customers.

Region	Primary Datacenter	Secondary Datacenter
Europe	West Europe – Netherlands	North Europe - Ireland
USA	East US - Virginia	West US - California
Australia	Australia East - NSW	Australia Southeast - Victoria
UK	UK South - London	UK West - Cardiff
Canada	Canada Central – Quebec	Canada East - Toronto
Middle East	UAE North - Dubai	UAE North - Dubai

Load Balancing Policy

Exclaimer acknowledges mail flow as mission critical and uses load balancing to mitigate the risks to this service.

If an incident occurs at one of Exclaimer's two regional datacenters, a comprehensive system is in place to ensure mail flow for all tenants is maintained. Tenant data is continuously synchronized in both datacenters simultaneously.

Load balancing is fully automated and is controlled intelligently by Microsoft Azure services. Should an incident occur, one of Exclaimer's regional Azure datacenters can be independently removed from the load balancer. This is a fully automated process but can also be controlled manually if required.

The Outlook Add-In

Client-Side roll out of signatures into Outlook is achieved through use of an Add-in. This Add-In can be centrally deployed from within the Microsoft 365 Admin Center and is compatible with Outlook for Windows, Mac, and the Outlook Web App.

The Add-In needs a method to authenticate the user as a valid user within your organization and Exclaimer makes use of Azure Active Directory and single-sign-on (SSO) to accomplish this. An enterprise application is added to your Microsoft 365 tenant during setup of Client-Side with the following permissions:

- Microsoft Graph: User.Read
- Azure Active Directory Graph: User.Read

Subsequently to the authentication of the user, event-based activation triggers the Add-In to populate the correct signature into the email as it is composed using the email signature API native to the Outlook client.

Connection to the Exclaimer solution to retrieve the signatures assigned to the user occurs securely through HTTPS and the only details regarding the email being composed are the sender, the email's subject and its intended recipients which help determine which signature should automatically be applied. No content within the composed message is ever sent to Exclaimer.

Data Handling

When using Exclaimer all data related to the operation of your Exclaimer subscription is hosted securely in Microsoft Azure and in such a way that for most customers, data residency can be guaranteed.

Data is stored in a High Availability Cluster (HAC) in your assigned region and is never permitted to be stored by Exclaimer anywhere else. In this way we assure compliance to data residency laws such as the General Data Protection Regulation (GDPR), and Californian Consumer Privacy Act (CCPA) as well as compliance established by regulatory bodies like the Dubai International Financial Centre (DIFC) or Abu Dhabi Global Market (ADGM).

The datacenters used for storing all data is as follows:

Region	Primary Datacenter	Secondary Datacenter
Europe	West Europe – Netherlands	North Europe - Ireland
USA	East US - Virginia	West US - California
Australia	Australia East - NSW	Australia Southeast - Victoria
UK	UK South - London	UK West - Cardiff
Canada	Canada Central – Quebec	Canada East - Toronto
Middle East	UAE North - Dubai	UAE North - Dubai

Active Directory Data

To correctly assign users their signatures, as well as populate signatures with their information, each Exclaimer subscription automatically collects data from Azure Active Directory.

During setup you grant read permissions for your Azure Active Directory to Exclaimer. This access is established using OAuth and Microsoft Graph is the API used to conduct each read of the directory through a HTTPS connection. The OAuth application has the following permissions:

- Microsoft Graph: User.Read
- Microsoft Graph: Directory.Read.All
- Azure Active Directory Graph: User.Read
- Azure Active Directory Graph: Directory.Read.All

These permissions allow the Exclaimer service to access the fields from the directory listed on the next page.

The scope of the data collected can be controlled from within the Exclaimer portal and can be restricted from the initial synchronization. By specifying a mail-enabled security group, the subsequent synchronizations with your Azure Active Directory will only collect the information associated with mailboxes belonging to the group.

Synchronizations with the Azure Active Directory take place twice a day automatically, although users with admin access to the Exclaimer portal can trigger a synchronization manually within the settings there when required.

All information collected in these synchronizations is cached encrypted at rest within Azure so it can be used continuously to populate the signatures that have been setup.

Display Name	LDAP Name
City	l
Country	co
Department	department
DIsplayName	displayName
EmailAddress	mail
FaxNumber	facsimileTelephoneNumber
FirstName	givenName
LastName	Sn
MobileNumber	mobile
Office	physicalDeliveryOfficeName
State	st
StreetAddress	streetAddress
TelephoneNumber	telephoneNumber
JobTitle	title
PostalCode	postalcode

Custom User Information

Exclaimer also provides functionality on select plans to manage user information away from the Azure Active Directory, either in addition or in place of this synchronized data. This additional data can be sourced from users directly via an online page or by uploading CSV files.

Access to the online User Details Editor page is controlled with SSO, to enable this access an application is added to Azure with the following permissions:

- Microsoft Graph: Openid
- Microsoft Graph: Profile
- Microsoft Graph: User.Read

The data submitted either via the online page or by CSV upload within the portal is submitted to storage within Azure via a HTTPS connection. No information is written to your Azure Active Directory in either instance.

Engagement Analytics

Exclaimer also offers functionality to anonymously track how recipients interact with email signatures in a way not dissimilar to a web analytics tool.

To accomplish this Exclaimer transforms URLs applied during email signature design into a unique hash that are populated within email signatures before they are applied. When an email recipient clicks on a link within a signature applied by Exclaimer, they are first routed to Cloudflare which expands the hash and redirects the user to the intended URL.

Simultaneously a packet of data is sent securely from Cloudflare to Exclaimer that registers the click and stored by Exclaimer to populate analytics dashboards.

Feedback Data

Exclaimer has functionality to collect feedback from respondents interacting with 1-click surveys added to email signatures. This feedback can be collected either anonymously or associated with the email address of the respondent.

URLs are associated with each feedback icon within a 1-click survey and when a click takes place a packet of data is securely sent to Exclaimer's feedback service. If the respondent then chooses to supply a comment, this is also sent to the service and stored by Exclaimer as well.

The Exclaimer Portal

The Exclaimer portal is the only access point available to customers, to their Exclaimer subscription. The portal stores all signature designs and rules established for the organization. It is also the only way to access reporting, analytics, troubleshooting and diagnostic tools.

Exclaimer can only be accessed with a web browser on any web-enabled device using HTTPS for transport encryption. The Exclaimer portal is verified by COMODO RSA Extended Validation Secure Server CA and connection to the portal uses TLS 1.2 and is encrypted using 256-bit encryption (AES_256_CBC with SHA384 for message authentication and ECDHE_RSA as the key exchange mechanism).

To use Exclaimer users must establish an Exclaimer account, the data related to this account is listed below and stored securely within Exclaimer:

- First Name
- Last Name
- Full Name
- Company
- Telephone number
- Email address
- Address line 1
- Address line 2
- Town/City
- Postcode/Zip Code
- Country

Customers can choose to use Microsoft Single Sign On (SSO) to sign up for an Exclaimer account and subsequently access this account securely. Alternatively, an account can be secured using a password.

All user passwords are protected using salted password hashing. When you create an Exclaimer account, your password is 'hashed' and stored within a secure SQL database. At no point is an unencrypted password ever stored and Exclaimer cannot read these password 'hashes'.

If as password is used, 2-factor authorization is in place to add an extra level of security to the login procedure. When you login to your account for the first time or from a different device/computer, you will be sent an email with a unique authorization code to confirm that it is you trying to access your account. Each code is only valid for a maximum of 4 hours.

Payment Details

Exclaimer does not store any credit/debit card details. When you add a new payment card to your account, you are redirected to the Global Iris payment portal, powered by RealEx Payments. This is secured using a 128-bit SSL Certificate and is one of the most secure ecommerce platforms for online payments.

Sent Items Update

Exclaimer customers can enable the option sent items update feature to replace the copies of sent emails retained in the sent items folder for each user with an updated version that includes the signature added by Exclaimer when processed.

When enabling this feature, you must install an Azure application that requires the following permissions:

- Microsoft Graph: User.Read
- Azure Active Directory: User.Read
- Office 365 Exchange Online: full_access_as_app
- Office 365 Exchange Online: Mail.ReadWrite

Exclaimer uses Exchange Web Services (EWS) and requires read and write access to the user's mailbox to locate to update the emails located in the sent items older. Access to the user's mailbox through EWS is authorized using a certificate securely stored in the Exclaimer infrastructure and the Azure application. Consent for Exclaimer's Sent Items Update can be revoked by deleting the application from within the Azure Portal.

Fault Handling and Failure

Our 24/7/365 monitoring services automatically detect any service alerts, which are configured with escalation chains. This means that Exclaimer's senior technical management is notified of any problems immediately.

If an issue occurs that stops the signature imprinting service at one regional datacenter, a highly unlikely scenario, you can be assured that emails sent from your organization will not be lost.

As soon as the issue is resolved, all email continues to be sent as normal. Our Development and Quality Assurance teams are continually evolving and developing the Exclaimer service in line with changes made to Microsoft Azure to prevent any technical matters occurring.

Trust Portal

Exclaimer want to make the entire vendor review process as simple as possible for all prospective customers.

Our Trust Portal has everything that you need to complete a full review of the Exclaimer solution including a full summary, certificates, reports, and policy documents. As well as the answers to over 350+ questions.