Retarus Global Messaging

Customer Data Management Overview

Information Security: ISAE 3402 Based Approach

As a global provider of hosted messaging services, Retarus operates according to ISAE 3402 principles. These principles ensure transparency and compliance to standards such as PCI, HIPAA, and SOX, as well guidelines for data security, privacy, and threat protection for both internal and external risks. To meet Enterprise requirements, all processes are supported by and cross-linked with other vital and central processes like Information Security Management, Business Continuity, Disaster Recovery, Financial Controls, Governance, Risk Management, Asset Management and Training / Awareness altogether covering the central disciplines of ISO 2700x, but better adapted to services as provided by Retarus.

About the ISAE 3402 Approach

ISAE 3402 is an international standard, developed and published by the International Standard on Assurance Engagements (ISAE). It represents an opportunity of reporting for Service Provider organizations within a worldwide institutional report format. In its focus are all processes and risks which are relevant for the balance outsourced to service providers. To provide organizations these assurances, Retarus works in close cooperation with a leading ISAE 3402 auditor to implement the framework for security and operations. Retarus' ISAE 3402 and IT Security policies can be provided upon request.

Retarus' ISAE 3402 Framework is based on ITIL V3. It is set up as a Type II Report and is processed by independent service auditors, demanding management assertion and provides a system description, tests performed by service auditors and test results. ISAE 3402 incorporates internal audit plans and evidence which is exactly what ISO does as part of the management system. The ISAE 3402 standard provides assurance to clients that the service organization has an appropriate and working risk control system in place, specifically addressing the needs of publicly listed companies, global clients and in particular enterprises that decide to outsource central business processes.

Scope of Retarus' ISAE 3402 Approach Includes:

- Physical Security
- Network and Security
- User & Access Management
- Customer Service Setup
- Service Desk
- Request Fulfillment
- Change Management
- Incident Management

Guiding Principles of Information Security

Retarus operates with a simple directive: all customer data is confidential and needs to be protected. To ensure confidentiality, the following rules apply to all systems processing data on behalf of Retarus' customers, partners or employees.

- **Principle of confidentiality, principle of need to know:** data shall not be accessed by unauthorized persons. “Data owners” and “data processors” are clearly defined for all systems and all type of information. Only authorized personnel have physical and/or logical access to the information, and shall use their respective access rights only in accordance with the applicable regulations
- **Principle of integrity**: data shall not be modified or manipulated. “Data owners” and “data processors” are clearly defined for all systems and all type of information. Only authorized personnel have physical and/or logical access to the information and shall use their respective access rights only in accordance with the applicable regulations
- **Principle of availability**: infrastructure components and data shall be available according to contractual arrangements. Access is only permitted to staff members that have been duly authorized by the information owner.
- **Principle of authenticity**: authorship and immutability of relevant data shall be ensured
- **Principle of legal and technical compliance**: relevant provisions for data processing shall be respected (legal obligations and accordance to third party certifications)
- **Principle of information**: customers shall be comprehensively notified in the event of damage or abuse

Protection of Information and Systems

At the physical level: Physical protection of the network, servers and data that is processed on them. SSAE16 documentation for US Data Centers provides specifics on security measures in place to physically protect Retarus hardware. Includes: Biometric scanning for access to server locations in Data Centers, closed circuit cameras monitoring both Data Centers and NOC, Security guards at both Data Centers and NOC, logging of all access in both Data Centers and NOC, and restricted access to hardware in general. All Data Centers in the United States are SOC 1 and 2 certified and are Tier 4.

At the process level, access to information and technology is managed according to a strict hierarchy and the principle of need-to-know. Confidential data shall not be accessed by unauthorized persons. Authorization is granted only according to role. For customers with PHI, PI, etc. requirements, it is highly likely that Retarus will maintain no content beyond the period it takes to deliver or receive and process the messages. Retarus does not view or review customer information. Retarus has the ability to separate the meta-data/details pertaining to a message (such as sender/recipient, time of delivery/receipt, page count, etc.) from the actual content of the message that was sent ("deliver and delete" model). In this model, no content is stored beyond the transmission. Only call data records (CDR's) are stored for billing purposes.

At the product level, all data and processing is logically separated. Client data is strictly segregated according to Customer ID. Every system has a confidentiality classification which triggers the proper rights and logical access levels. Passwords for EAS portal access are securely stored as a salted hash in a database. Transfer of data can be secured via VPN, HTTPS, TLS, FTPS etc. upon customer’s request. Encryption / VPN / TLS can be setup according to customer requirements. Some Retarus services allow customers to store content related data securely within Retarus’ infrastructure for a period beyond the service transmission itself.

Security Layers

Physical	Network	Transport	Content
Tier 4 DCs	Monitoring	VPN	AES
SSAE16	Firewalls	TLS	S/MIME
Biometrics	Antivirus	HTTPS	PGP
CC Cameras	Segmentation	SFTP	x.509
Guards	Password Policy	SSL	ETC
Access Logs	SSO		

Data Security

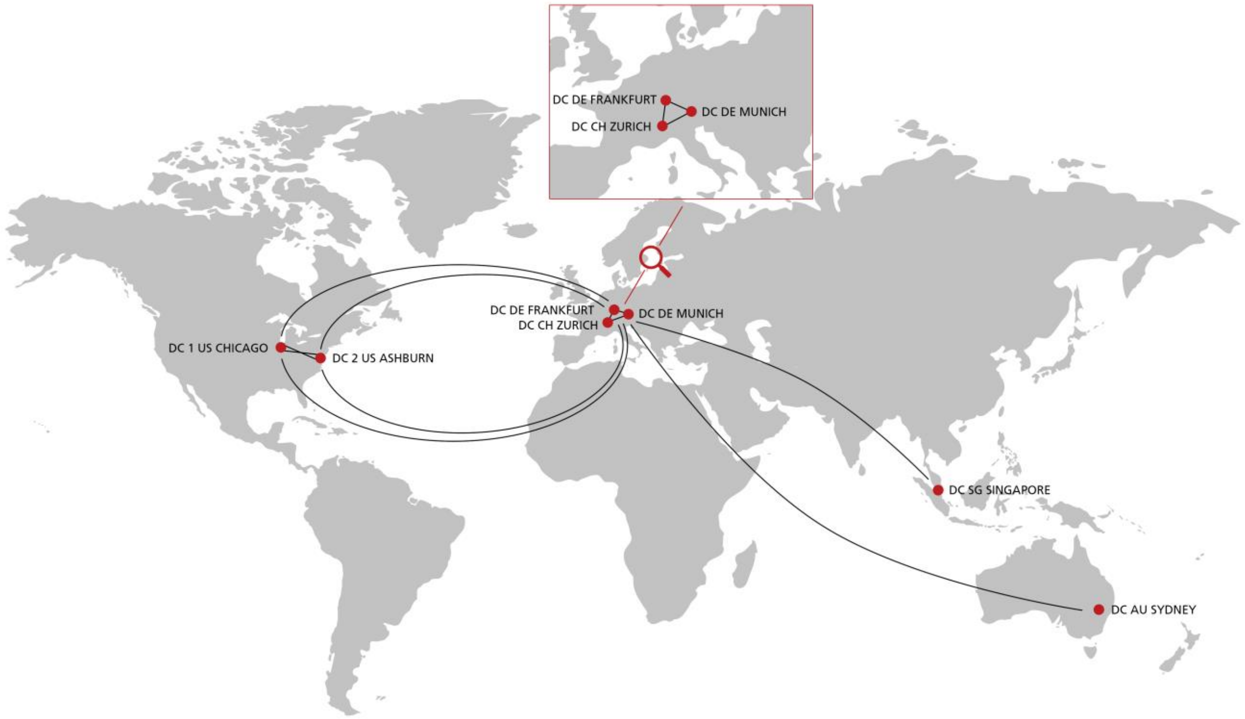
Retarus meets requirements for security, backup, audit, access control and encryption by safeguarding information security and supporting audit trail for compliance. Data in transit is protected through HTTPS, FTP(S), TLS (SSL), and VPN, among other types. Security and encryption used for data at rest includes AES encryption, PGP and S/MIME certificate encryption for data storage and access via EAS. Additionally, further protection is taken at the network and physical level to ensure that various compliance and technology standards are met, including SSAE16 and ISAE3402 certifications.

Added restrictions are designed so that organizations can prevent employees from accessing sensitive data, as well as to prevent Retarus employees from viewing data that is sent or received. Fax images can be set to be encrypted on server at rest if the images are going to be stored after delivery, but to ensure items like HIPAA compliance, Retarus also provides immediate document deletion as soon as the document is transmitted to the recipient.

Local Data Processing

Regions all around the world subscribe to differing views of how data processing should be handled, which can make international communication challenging. Retarus offers its customers the ability for local processing in case it is needed. For example, a US customer's data will only be processed in the United States whereas European customers could choose only data centers located within the European Union. This concept supports Enterprise data protection requirements and according compliance with applicable local regulation. Retarus' concept entails the maintenance of autonomous processing locations in the US and Europe. Customers can fail-over to a site in the same region without having to consider compliance ramifications due to fail-over to another region.

For example: Your organization's data security guidelines stipulate that personalized data can only be processed and stored within the European Economic Area (EEA). If your organization uses Retarus' Services, you can restrict this processing to two European-based data centers. If you use another Service Provider that maintains only one European data center, an outage will leave you unable to complete business activity while maintaining compliancy.



To enable Disaster Recovery in case of a partial or full outage at a Data Center, Retarus offers its customers the option of having data processing conducted in multiple selected data centers. The ability to react to issues and route data while still being processed locally, provides significant advantages over providers that only maintain one regional data center location. It enables organizations to lower the risk of local or partial issues, like power outages or faulty connections into a data center. For customers connected to at least two data centers, Retarus can react to local issues in a single data center and still provide the highest levels of availability, capacity and compliance.

For example: Your company would like to protect itself from a catastrophic outage at a data center. Your solution is to connect itself to three data centers and correspondingly increase the guaranteed availability.