Actico SaaS Technical Documentation

Technical Documentation of Actico Services in regard to Security, Privacy and Architecture.

Version: 1.3
Date: May 26, 2025

Inhalt

Cloud Services Overview and Scope

Actico Services are subscription-based software services operated at AWS data centers, used as Software as a Service (SaaS) and designed to provide high performance, scalability, security, data privacy and protection, management capabilities and service levels required for mission-critical applications.

The scope of this description is the operation of all Actico Cloud Services.

The development process is not in scope of this document.

Location of Services

Actico hosts in the following AWS regions and can be chosen by the customer. All data is processed within the chosen region. No customer data is transferred from one region to another.

- Europe – Frankfurt (Region eu-central-1)
- USA – North Virginia (Region us-east-1)
- Asia Pacific – Singapore (Region ap-southeast-1)

Audits and Certifications

Actico Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments performed at least on annual basis.

The following and privacy-related audits and certifications are applicable to one or more of the Actico Services:

- SOC 2 (AICPA)
- ISO 9001 Quality Management
- ISO 20000-1 Service Management
- ISO 22301 Business Continuity Management
- ISO 27001 Information Security Management

The design and operating effectiveness of security, availability, processing integrity, and confidentiality controls are analyzed by a third party at least once per year. These assessments include external (e.g. ISO audits, IDW PS 951 audit, SOC 2) and internal evaluations (e.g. risk assessments and vulnerability scans). The results and findings from these assessments are addressed with corrective actions, which are tracked by the Quality Manager (QM) or Internal Audit (IA) to substantiate that they are addressed in a timely manner.

Actico uses infrastructure provided by AWS to host or process customer data submitted to Actico Services. Information about security and privacy-related audits and

certifications received by AWS, including information on ISO 27001 certification and SOC reports, is available from the AWS Security Website and the AWS Compliance Web site.

Control Environment

Actico maintains reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect customer data against accidental loss, destruction or alteration as well as unauthorized disclosure or access.

The collective control environment encompasses management and employee efforts to establish and maintain an environment that supports the effectiveness of specific controls. Actico maintains an internal Management System describing the policies, boundaries and user responsibilities.

Actico has written agreements with their sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to the processing activities provided by them. Compliance with such obligations as well as the technical and organizational measures implemented by Actico, and its sub-processors are subject to regular audits.

General Architecture and Data Segregation

Actico composes specific AWS services (like AWS RDS for databases) and container-based workloads to build Actico Services and manages those containers in Kubernetes clusters. AWS EKS is used as managed Kubernetes Service for orchestration. Actico Services are operated in two models:

- Shared Setup: The Kubernetes Cluster hosts multiple customers. It is a multitenant architecture with mostly physical and partly logical separation of customer data. Data for user management is logically separated (by “realm”) and other customer data is completely separated physically from other customer data by dedicated databases and storage volumes. Furthermore, every customer has its own set of application instances processing those data. Kubernetes namespaces separate those application instances from other customers. Private connectivity to the application endpoints is not possible in shared setups as endpoints are exposed to the internet (secured with client certificates or IP Whitelisting).

- Dedicated Setup: Single tenant architecture with a dedicated Kubernetes Cluster for the individual customer with physical separation of customer data. Every customer has its own Network (VPC = Virtual Private Cloud), Databases, Storage Volumes, OpenSearch instances and application instances. The infrastructure used for hosting is not shared with any other customer. Application endpoints are not exposed to the public internet. On demand this setup allows private

communication with AWS accounts of the customer (e. g. by VPC peering, AWS Transit Gateways) or allows VPN connection to the VPC Network of the customer hosting.

Infrastructure Components

The Actico Services depend on infrastructure components like network, compute instances or databases for providing a fully functional cloud service. Actico leverages facilities, services and infrastructure components offered by AWS and currently uses following AWS Services:

- AWS IAM (Identity and Access Management) - Access and Service Roles
- AWS VPC (Virtual Private Cloud) - Networking
- AWS Security Groups – Firewall
- AWS Secrets Manager – Secret Management
- AWS KMS – Key Management
- AWS EKS (Enterprise Kubernetes Service) - Container Orchestration
- AWS EC2 – Compute Resources for Workload
- AWS EBS – Shared Storage for Workload
- AWS RDS – Databases
- AWS OpenSearch – Search indices
- AWS Route 53 – DNS service
- AWS S3 – Block Storage
- AWS ECR – Container Registry
- AWS Code Commit – GitOps Repositories
- AWS Cloud Watch – Monitoring and Alerts
- AWS Shield – DDoS Protection
- AWS Backup – Backup Management

The mentioned AWS Services are provided by infrastructure automation software to avoid manual processes and danger of misconfiguration. All customer infrastructure configurations are held in Git repositories and state stores.

GitOps

Actico implements the GitOps Principle as management method for software components and for managing infrastructure components. This means that the desired state of software and infrastructure components is defined in Git repositories, and a GitOps tool continuously synchronizes the desired state against the actual state. Every change to the system can be tracked and audited via Git commits. Furthermore, GitOps provides the possibility for self-healing systems because if the managed environments deviate from the desired state, it is constantly and automatically trying to bring the system back to that desired state. Changes to the systems are approved by at least one

other person in pull requests and the change itself is tracked in the internal ticketing system with referencing the pull request.

Physical Security

Our IT infrastructure providers are responsible for providing appropriate physical security measures. Further information about the physical security provided by AWS is available from the AWS website at:

https://aws.amazon.com/compliance/data-center/controls/

Operational System Access

Actico has an Authorization Policy in place which handles access management principles, rules and procedures.

Actico is using AWS Access Management Services to protect all access to our assets managed in AWS. Corporate password requirements are defined by company policy and implemented in those Access Management Services. These requirements include password complexity, length, history, and duration. The users are mapped to IAM roles which are used to manage access to AWS services.

All other tools used to manage customer environments (non-AWS Tools) are also access-restricted by Actico's user directory with same password policies applied.

All access to Actico's systems is restricted by either (often a combination of multiple methods)

- User Login with 2-factor-authentication
- Access restriction via VPN
- Whitelisting of IP's
- Security Groups in AWS (Firewall rules)
- IAM Policies

Which access restriction is used for which communication channel is documented in the managed list of access points in our internal management system. We aim to have a combination of at least two of the mentioned methods. AWS root account access is secured via hardware-based multi factor authentication.

Granting and Changing Access

Management of access is regulated by a policy which specifies a process how to request, document, grant and revoke access to AWS and other technical systems. Approvals follow the 4-eye principle.

Each request for getting and changing access requires an access request via ticket in the ticketing system which must be approved by the asset owner and CISO (Chief Information Security Officer) before access is granted or changed. The process is

documented in the workflow of the ticket. This process is also required for setting up technical users.

When individuals leave the company tasks are triggered to check for termination of access to management and customer systems. If there was a granted access, it is terminated and documented within the offboarding process. Without the appropriate access rights, the user cannot access services within the Actico and AWS environment.

Periodic User Access Review

A manual user access review is performed on a regular basis to ensure that access for each user is up-to-date and in line with job responsibilities. Any required access alterations identified during the review are addressed in a timely manner.

Network segmentation

Actico Services are based on AWS VPC Networking and use network separation as a guiding principle. In the dedicated setup customers have an own dedicated VPC network completely separated from other customers and our shared setup implements network separation by Kubernetes Network Policies. AWS Security Groups are used in both types to control network traffic on another level. Furthermore, production and non-production setups are operated in different subnets for network separation.

Actico Services operate with different set of IP's outgoing (NAT) which allows IP filtering on customer side for incoming traffic from Actico Services.

Encryption

Actico Services use industry-accepted encryption products (leveraging at least 2048-bit RSA server certificates and 128-bit symmetric encryption keys) to protect customer data and communications during transmissions between a customer's network and Actico's services, including through Transport Layer Encryption (TLS). Customer data is also encrypted at rest.

Actico has a Cryptography Policy in place which regulates use of encryption. Actico encrypts information assets where possible and appropriate, e. g. databases, database backups and open search indices are encrypted at rest. Actico documents information assets being encrypted as well as corresponding key management.

Actico encrypts information assets with keys managed in AWS Key Management Service. Keys are generated by automation scripts or managed by AWS itself. If possible, Actico activates regular rotation of the encryption key. *Bring Your Own Key* is not supported yet.

Following entities are encrypted:

Entity	Key Management	Automatic Key Rotation
Database Data at Rest	AWS KMS	Yes
Database Snapshots/Backups	AWS KMS	Yes
ECR repositories	AWS S3 Managed Keys / AWS KMS	Yes
Secrets Manager Secrets	AWS KMS	Yes
EC2 Instance Volumes	AWS KMS	Yes
EC2 Volume Snapshots/Backups	AWS KMS	Yes
S3 Buckets	AWS S3 Managed Keys	Yes
EKS Secrets (etcd)	AWS KMS (TF managed)	Yes

Private Interconnectivity

Private connectivity to customer's services is only possible in the dedicated setup where application endpoints are not exposed to the public internet by default.

In shared setups private connectivity to the application endpoints is not possible as endpoints are exposed to the internet (secured with client certificates or IP Whitelisting).

Our dedicated setup supports AWS VPC Peering which is connecting to an AWS VPC or an AWS Transit Gateway of the customer. Furthermore, VPN connectivity via AWS Site-To-Site VPN is possible (extra pricing). This allows completely private traffic between Actico Services and customer's IT infrastructure. If configured no traffic will be routed via Internet.

If AWS Site-To-Site VPN is used, then high availability can only be guaranteed if customers provide configuration for both tunnels. Otherwise, AWS cannot switch to a redundant tunnel when applying updates.

Firewall

We ensure network security with AWS Security Groups, Network ACL's and IP Whitelisting. A security group acts like a virtual firewall at the instance level. It controls inbound and outbound traffic for specific instances within a Virtual Private Cloud (VPC). Security Groups are also attached to our network load balancers and databases which only allow specific patterns and types of incoming and outgoing traffic.

A Network ACL is a layer 3 firewall that controls traffic at the subnet level within a VPC. Network ACL's define rules that allow or deny traffic based on source/destination IP addresses, ports, and protocols.

IP Whitelisting on the ingress controller restricts access to a specific customer deployment to a set of trusted IPs which can be defined by the customer.

Services System Access

Access to Actico Services requires authentication via one of the supported mechanisms, including user ID/password, OpenID Connect, OAuth, API Key or delegated authentication as determined and controlled by the customer.

Actico Services use HTTPS protocol for communication. All services use the latest TLS standards which is currently TLS 1.2 and TLS 1.3. Server certificates, which have at least RSA 2048 bit standard.

Actico Services require one of the following two methods as additional authorization layer:

- IP Whitelisting (max. 10 IP's)
- Use of client certificate with mTLS (certificate provided by Actico)

IP Whitelisting is not possible for offerings in combination with Salesforce platform.

User access log entries will be maintained, containing date, time, user ID and source ip address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by the customer or its ISP.

Services User Management

Customer applications provided by Actico Services have their own user management which is within responsibility of the customer and not in scope. By default, we apply our Actico password policies on new customer setups. We recommend revising and to activate multi factor authentication.

Actico Services use an OpenID Connect identity provider for managing user access to our services. Every customer gets its own "realm" where it can manage its users. No customer has access to a "realm" of another customer. The realms are logically separated which means all customer realms are managed within one cluster of Actico's identity provider. Only dedicated setups have an own instance of the identity provider cluster and with that a physical separation of the user management. Both non-production and production environments have its own identity provider and with that its own realm so that you can distinguish user access management between productive and non-productive environments.

Connectivity Identity Provider Customer

If licensed by separate package, then Actico user management allows the connectivity of our identity provider with the customer's identity provider (not available for setups in combination with Salesforce). Actico supports identity providers with standard OpenID Connect and OAuth2 protocols like EntraID or Okta. The customer gets an user from our identity provider which has the rights to fully configure and control the connectivity to the customers identity provider. It is possible to have different identity providers configured for productive and non-productive environments.

Passwords

Customer passwords are stored (if stored at all) using a one-way salted hash. Currently the default algorithm for user management passwords is PBKDF2 with SHA256. Passwords are not logged. Actico personnel will not set a defined password for a user. Passwords are reset to a value which must be changed on first use.

Reliability

(This section does not apply to non-production environments.)

Actico Services are configured and deployed in a highly available manner. Highly available refers to the overall fashion in which the service and its underlying infrastructure are operated and deployed. Services are deployed across multiple availability zones within a region. Systems are designed to recover from failure in a minimally disruptive way. Minimally Disruptive means that the system is designed to continue operating during failure events in the infrastructure. The infrastructure is designed to recover from failure in an automated fashion. For example, productive databases have a read replica in another availability zone for failover purpose or productive application instances have at least 2 replicas.

Actico uses following general concepts to achieve reliability:

- Usage of second availability zone in an AWS region
- Usage of database replication to another instance / read replicas
- Usage of storage volume replication to other nodes
- Usage of redundant container instances

Data Backup and Disaster Recovery

Actico Services use various solutions for data backup, such as:

- AWS Services Backup functionality
- AWS Backup Manager
- Velero Backup Solution

Database backups are continuous, incremental and quickly restorable to any point within the backup retention period. Backups are taken daily and kept for 14 days. Furthermore, Actico keeps monthly backups for 6 months. Backups are encrypted.

Actico Services' disaster recovery plans have the following target recovery objectives: (a) restoration of the service (RTO - recovery time objective) within 12 hours after Actico's declaration of a disaster; and (b) maximum customer data loss (RPO - recovery point objective) varies between 10 minutes and 24 hours depending on the scenario. However, these targets exclude a disaster, or multiple disasters causing the compromise of multiple availability zones at the same time and exclude non-productive environments.

Actico Services' disaster recovery processes are built on top of the standard deployment process; this ensures that disaster recovery is done using a well understood and reproducible process. We are doing several disaster recovery tests during the year.

Governor limits

In order to protect Actico Services from unusual and excessive workload and/or to protect from monopolizing resources in shared tenant architectures Actico enforces governor limits operating the services. Agreed values for governor limits can be found in a separate agreement.

Security Monitoring and Analysis Tools

Actico uses the following systems to secure its provided services and data as well as protecting the system against malicious activities.

AWS GuardDuty (Intrusion Detection)

AWS GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behaviour to protect the customers' AWS accounts and workloads. With the cloud, the collection and aggregation of account and network activities is simplified, but it can be time consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, Actico performs a continuous threat detection for Actico systems at AWS.

AWS Security Hub

AWS Security Hub gives customers a comprehensive view of their high-priority security alerts and compliance status across AWS accounts. With Security Hub, customers can have a single place that aggregates, organizes, and prioritizes their security alerts, or findings, from multiple AWS services. Findings are visually summarized on integrated dashboards with actionable graphs and tables.

Actico has enabled following security standards in Security Hub and acts accordingly to alerts:

- AWS Foundational Security Best Practices v1.0.0

- CIS AWS Foundations Benchmark v1.4.0

AWS Config

AWS Config enables Actico to assess, audit, and evaluate the configurations of their AWS resources. AWS Config continuously monitors and records AWS resource configurations and allows Actico to automate the evaluation of recorded configurations against defined configurations. With AWS Config, Actico can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine overall compliance against the configurations specified within the Actico's internal guidelines. This enables Actico to simplify security analysis, change management, and operational troubleshooting.

AWS Health Dashboard

AWS Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact customers. While the AWS Health Dashboard displays the general status of AWS services, AWS Health Dashboard gives Actico a personalized view into the performance and availability of the AWS services underlying Actico's AWS resources. The dashboard displays relevant and timely information to help Actico manage events in progress and provides proactive notification to help Actico plan for scheduled activities. With AWS Health Dashboard, alerts are triggered by changes in the health of AWS resources, giving event visibility and guidance to help quickly diagnose and resolve issues.

IAM Access Analyzer

An AWS Identity and Access Management (IAM) feature that monitors and analyses policies applied to Actico's AWS resources. E. g. when Access Analyzer identifies a policy that allows access to a resource from outside of your account or if accounts are unused, it generates a finding.

AWS Trusted Advisor

AWS Trusted Advisor provides recommendations that support following AWS best practices, optimize AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas.

AWS ECR Image Scanning

Amazon ECR uses the Common Vulnerabilities and Exposures (CVEs) database from the open-source Clair project to scan container images in the registry. Actico does not allow to promote images with vulnerabilities to releases. Vulnerability scanning is also integrated into the development.

AWS Shield Standard

AWS Shield Standard is used to prevent DDoS attacks.

Further information about security provided by AWS is available from the AWS Security Website.

Vulnerability and Patch Management

There is a continuous process for vulnerability scanning, reporting, patching and review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported through a centralized process. Responses are tracked from compliant and non-compliant services and hosts, to ensure timely resolution of incidents of non-compliance.

Vulnerability Management System dictates that regularly scans of all products which are delivered to production environments must take place. Every detected vulnerability will be assessed by risk. According to criticality and impact a timeline for the fix will be defined.

Regular vulnerability scans are conducted for each product release which has not reached end of life.

AWS automatically scans artefacts after pushing into the artefact management (ECR). Assets with vulnerabilities rated “High” or “Critical” are not allowed to be deployed on production.

Underlying infrastructure like Kubernetes clusters, worker nodes, databases and other add-ons like storage drivers or network plugins are regularly security patched and updated to the newest versions. This also includes basic infrastructure software components like ingress controller or our identity provider software.

Viruses

For Actico Services that allow the upload and execution of code, the customer is responsible that uploaded executable code does not contain any viruses or critical vulnerabilities.

Penetration Tests

The main objective of penetration testing is to assess the security posture of the product and the underlying infrastructure. This process helps Actico to understand the product resilience to cyber threats and ensure that sensitive data and functions are adequately protected. By performing penetration testing, vulnerabilities can be proactively addressed before they are maliciously exploited.

Penetration testing is performed by external parties regularly. Regular testing ensures that security measures remain effective over time as new threats and vulnerabilities emerge.

By conducting penetration testing, we promote a security-focused approach and protect the data of our customers and partners. This is a critical aspect of our security strategy, which aims to protect sensitive data and secure our company in today's constantly evolving threat landscape.

Review Process (Security Logs)

In addition to the automated systems check, manual checks (e. g. log file inspections or security reviews) are also carried out. These tasks are essential to ensure that compliance is up to date, in line with regulations, and consistently followed throughout the organization. Regular inspection and review of protocols involves a series of tasks intended to assess the effectiveness, relevance, and compliance of policies.

Log file protocol inspection involves the analysis and review of log records to detect anomalies, security breaches, operational issues, and other critical information.

In the reviews a protocol is created, and every finding will lead to a ticket in the internal ticketing system and be handled in a timely manner.

Security Monitoring

Actico defines a Security Incident as a security-related adverse event in which there was a loss of data confidentiality, disruption of data or systems integrity, or disruption or denial of availability. Actico monitoring tools are implemented to detect unusual or unauthorized activities and conditions at ingress and egress communication points. Depending on the intended use case, these tools monitor server and network usage, port scanning activity, application usage, and unauthorized intrusion attempts.

Actico has a documented information security process which outlines an organized approach for responding to security breaches and incidents. The Security team is responsible for monitoring systems, tracking issues, and documenting findings of security-related events. Records are maintained for security breaches and incidents, which include status information, information required for supporting forensic activities, and evaluation of incident details.

As part of the process, potential breaches of customer content are investigated and escalated to General Management and Legal. Affected customers and regulators are notified of breaches and incidents when required.

Incident Management

Actico has implemented incident response procedures, which consist of technical mechanisms, organizational infrastructure, and other procedures to detect, respond, and help preventing security incidents. Actico's technical infrastructure includes monitoring systems for detecting and alerting Actico personnel of security events and incidents. Actico personnel identifies potential incidents and documents findings for investigation. Incidents with significant risk to the environment are prioritized for response and mitigation.

If an incident is assigned a sufficiently high severity, applicable contingency plans are invoked. When an emergency response plan is invoked, personnel work with all necessary resources on the topic.

Incident response procedures are in place (Management of Information Security Incidents Process) that outline the activities. Actico CISO tracks detected security events, checks for necessary actions and coordinates follow up processes.

Actico notifies impacted customers without undue delay of any unauthorized disclosure of their respective customer data of which Actico becomes aware to the extent permitted by law.

Change Management

Actico applies a systematic approach to manage changes so that changes to systems are reviewed, tested, approved, and well communicated. The goal of Actico's change management process is to prevent unintended service disruptions and maintain the integrity of service to the customer.

Each change is tracked within a ticketing system. Appropriate authorizations and approvals needed for the changes are defined in the tickets and corresponding workflows.

Changes pushed into production are closely monitored so that the impact can be evaluated. Rollback procedures are documented so that the service can be reverted to the previous state if needed.

Emergency changes need approval from the Emergency Change Advisory Board (ECAB). The ECAB focuses on risk analysis and risk minimization. Appropriate decisions are made as a balanced tradeoff between risk and reward. Depending on the change other people (e.g. General Manager, ISB or DSO) could be involved if necessary.

Examples of Emergency Changes:

- Implementing a security patch to a zero-day exploit
- Isolating the network from a large-scale Distributed Denial of Service (DDoS) attack

Release Management and Maintenance

Actico uses semantic versioning to ensure clarity and predictability in how we manage updates to our services. Major version updates (X.y.z) may require your attention to adjust your systems due to significant changes. However, minor and patch updates are designed to be seamless. These updates include new features, improvements, and bug fixes that are backward-compatible, meaning you can deploy them without any manual intervention or compatibility issues. This allows you to benefit from the latest enhancements and fixes with minimal effort.

Patch version updates (x.y.Z) can be applied without any additional effort for the customer. If a patch release is caused by "high" or "critical" vulnerabilities, it will be

deployed as quick as possible. The customer will be informed about the deployment. There is no impact for the customer as patch releases don't contain new functionality. Patch releases guarantee a secure setup of the customer environments.

Minor version updates (x.Y.z) should be reviewed by our customers to ensure they meet their expectations in functionality, compliance and performance but can also be applied without additional effort for the customer. They are designed to be non-disruptive and do not contain breaking changes in functionality or API's. They are backward-compatible and do not require any changes or manual actions on their part, ensuring smooth and effortless transitions. This aspect ensures that customers can take advantage of improvements and new features without worrying about integration issues or downtime.

Minor releases are announced in advance and can be tested on non-production environments prior to installation on production environments. After 30 days of testing, new Releases get promoted to upper-level environments until they reach production in the end. The customer gets informed about the promotion to the next environment to be able to repeat its tests if necessary. Minor releases may be associated with downtimes. If so, the deployment is done in our maintenance windows and will be communicated with the customer.

Major releases contain major new functionality, are announced at least 30 days in advance and can be tested on non-production environments prior to installation on production environments. After 90 days of testing, they get promoted to upper environments until they reach production in the end. The customer gets informed about the promotion to the next environment to be able to repeat its tests if necessary. If there are no or only minor breaking changes, test period on pre-production environments can be decreased. Major releases may be associated with downtimes. If so, deployment is done in our maintenance windows and will be communicated with the customer. Major releases may contain breaking changes in functionality and API's. If so, this is communicated in advance.

Maintenance work regarding general infrastructure changes or upgrades not directly related to Actico Services' functionality will always be communicated at least 7 days in advance.

Actico asks for an email address from the customer for notifications. This needs to be a distribution list to be long-lasting and to prevent that customers miss any notifications.

There is no difference in the release management for shared and dedicated infrastructure setup.

Maintenance Windows

For some patches, releases or maintenance work a downtime is required for the deployment. We are improving constantly to reduce the number of releases which need a downtime (e. g. by using rolling upgrades). If a downtime is implied, the deployment or

maintenance work takes place in specific maintenance windows which are different in every deployment region and are set to be outside of business hours. The following table shows current maintenance window definitions for the different regions:

Region	Day	Time
Europe		
	Thursday	20:00 - 22:00 CET/CEST
	Sunday	15:00 - 22:00 CET/CEST
US		
	Monday – Thursday	02:00 am - 05:00 am EST/EDT
	Sunday	09:00 am - 04:00 pm EST/EDT
Asia-Pacific		
	Monday - Wednesday	22:00 - 24:00 SGT (when CET in Germany) 21:00 - 23:00 SGT (when CEST in Germany)
	Thursday	01:00 - 03:00 SGT (when CET in Germany) 00:00 - 02:00 SGT (when CEST in Germany)
	Sunday	22:00 - 05:00 SGT (when CET in Germany) 21:00 - 04:00 SGT (when CEST in Germany)

Availability Monitoring

(This section does not apply to non-productive environments.)

Systems are designed to monitor key operational metrics and alarms are configured to automatically notify operations when alarm thresholds are crossed. An on-call schedule is implemented with personnel available 24/7 to respond to operational issues.

Actico Services utilize different tools to monitor and evaluate their service's health (i.e., capacity, resiliency, and availability). Additionally, application metrics are monitored and alerts for those application metrics are defined. These tools are configured to automatically alert assigned team members of issues impacting service health.

Business Continuity

Actico has undergone ISO 22301 certification for Business Continuity Management. Procedures for Business Continuity Management are in place, to provide the organization with the ability to effectively respond to threats such as natural disasters or data breaches and protect the business interests of the organization. Actico Services are part of that BCM process and have own BCM plans active to reflect the different scenarios and take appropriate action.

Actico uses a common set of criteria to determine the relevancy and frequency of failover exercises. Where relevant, failover exercises are conducted on a regular basis to test applications and related data.

Actico's business continuity plans are tested and updated through the due course of business.

Analytics

Actico may track and analyze the usage of services for the purposes of security and helping improve both services and the user experience in using the services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.

Additionally, Actico may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our services.

Actico will not share customer data consisting of personally identifiable information, nor any data that will or could be used to identify customers, their users, their consumers, or any individual, company or organization. Actico may use Customer Data on an anonymized aggregate basis for purposes such as research, marketing, analysis, and benchmarking, and other purposes reasonably required to develop, deliver, and provide ongoing innovation to Actico Services.