iQ.Suite aaS Information Security Policy

Date: 07.12.2021

1 Overview

"iQ.Suite aaS" is a Security Cloud Service which integrates with customer's Office 365 / Exchange Online environment to provide various security functionalities like malware protection, SPAM protection, message encryption, data leakage prevention, key/certificate management, signature management, absence management and others.

2 Purpose

The purpose of this document is to set principal requirements and standards for "iQ.Suite aaS". It provides information to the Cloud Service Customer (CSC) on the security landscape of the services, as well as on the shared responsibilities between the customer and the Cloud Service Provider (CSP).

3 Scope

This Policy applies to "iQ.Suite aaS" and all assets related to it – employees, customers, processes, policies, infrastructure and data.

4 Policy

4.1 Baseline information security and data privacy

During the design and implementation of „iQ.Suite aaS", the team behind adhere to different industry standards, guidelines and best practices. ISO/IEC 27001:2013 security controls are implemented considering the additional guidelines set in ISO/IEC 27017:2015 "Code of practice for information security controls based on ISO/IEC 27002 for cloud services". The service runs on West Europe instances of Microsoft Azure, which is one of the leading cloud providers, with proven high level of security and compliance to international standards and regulations. "Secure development and deployment guidance" by the National Cyber Security Centre is followed for the software development and deployment. Continual security tests are performed, including checks for OWASP vulnerabilities and execution of regular penetration tests. The configuration and deployment of underlying cloud infrastructure follows the Azure security baselines. "iQ.Suite aaS" is designed and operates in accordance to requirements set in EU General Data Protection Regulation (GDPR). As defined in Art. 28 GDPR, appropriate technical and organizational measures are taken to ensure compliance with the regulation.

4.2 Shared roles and responsibilities

Depending on the delivery model, the split of responsibilities between the CSP and CSC are different. These responsibilities vary for the three primary cloud delivery models: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Services), where for IaaS the CSC hold the majority of responsibilities, and for SaaS on the majority of responsibilities are with the CSP. Following this definition for SaaS, „iQ.Suite aaS" accounts for the security on physical, infrastructure, network and application level. Regarding identity, access and rights management, responsibility is shared between the CSP and the customer, where the CSP provides the means for secure management of users and the customer is responsible for their proper use. Ensuring that data is classified correctly and usage of „iQ.Suite aaS" is compliant with applicable to the customer regulatory obligations, is responsibility of the customer.

4.3 Risks from authorized insiders

Azure Security Center is used to detect insider threats and attempts to compromise assets from authorized personnel. It uses new, continuously improved behavioral analytics algorithms to detect malicious activities. All personnel involved in the development, implementation and operation of "iQ.Suite aaS" pass regular training on his/her information security and data privacy obligations.

4.4 Multi-tenancy and cloud service customer isolation

„iQ.Suite aaS" is a multitenant service, which segregates data storage and processing of every customer, to ensure that its data is not accessed or combined with other customer's or internal for the service data. The

logical tenant isolation is implemented on database level with dedicated Azure SQL database for each client. The service's virtual infrastructure is situated in separate and isolated network.

4.5 Access to cloud service customer assets by staff of the cloud service provider

„iQ.Suite aaS" support administrators do not have default access to cloud customer data. Upon need the customer can grant permissions to the support administrator to impersonate a role in the customer tenant, to assist with troubleshooting issues.

4.6 Communications to cloud service customers during change management

The architecture of "iQ.Suite aaS" allows seamless maintenance and implementation of changes without downtime and disruption to the cloud service customer, supporting the ability of the cloud service provider to meet its availability SLAs. Information about important changes as well as features and fixes in new releases, is communicated to customers in advance to the release.

4.7 Service logging

Records related to the usage of "iQ.Suite aaS" are gathered and logged in the cloud service logs with (UTC) timestamps. Cloud service customers are provided with read only access to these logs through the web user interface of the service, which automatically converts the timestamps to the clock of the customer's computer. CSP administrators do not have access to the logs generated by the CSC as this information is stored in the customer database. Records are protected from tampering and can serve as evidence during forensics and incident investigations.

4.8 Access to and protection of cloud service customer data

Access to "iQ.Suite aaS" by both CSC users and CSP support administrators and users is available only to authorized Microsoft 365 accounts. Additionally, two-factor authentication is supported to ensure more secure sign-in. The service is accessed through web over TLS encrypted connection, which protects all data in transit. Confidentiality of customer data is ensured by using Azure Defender for Azure SQL, Transparent Data Encryption in Azure SQL and holding all data on 256-bit AES encrypted storage. Azure hosted firewall protects virtual infrastructure and restricts unauthorized network traffic.

4.9 Lifecycle management of cloud service customer accounts

During the initial provision of iQ.Suite aaS, the customer provides own Azure AD account to be configured as tenant global admin in iQ.Suite aaS. After configuring this access, the customer has all the capabilities to add/remove users to the service, change roles and rights, create custom roles and assign them to users. Customer administrators of the cloud service are responsible for the end-to-end management of all cloud service customer accounts.

4.10 Service monitoring

Continuous 24/7 monitoring and alerting provides "iQ.Suite aaS" support team with information on the service's health and performance, as well as information about any security events or incidents. Both Azure and third-party monitoring solutions are used for better coverage of the monitoring needs. The CSC can monitor specific aspects of the operation of the cloud service in the logs made available in the web user interface.

4.11 Handling of security incidents and data breaches

In cloud services both the CSC and the CSP share the risk of security incidents and data breaches, which makes their proper and timely handling of great importance. Each party is obliged to report to the other party any detected or suspected security incident or data breach, which may have adverse impact on either of them within 24 hours (e.g. confidential data leak, personal data disclosure, severe service failure, etc.). Notifications

from CSP to CSC are sent to the official contacts provided in the service contract. Notifications from CSC to the CSP are sent to security@digitall.com. The Cloud Service Provider has implemented 5-phased process for managing security incidents and data breaches – Detection, Assessment, Containment, Resolution and Closure. Both parties shall actively collaborate to mitigate the negative impact and resolve the security incident, sharing digital evidence or other information between each other to the detail level needed for effective resolution. The CSP and CSC must comply with their obligations for communication of data breaches to the relevant authorities.

4.12 Data backup

Different strategies are implemented to backup customer data. Point-in-time-restore (PITR) is available for the last 7 days. Additionally, differential backups are made every 12 hours. Long-term retention is configured to keep full backups for 4 weeks. Geo-redundant backups are performed in West Europe and North Europe datacenter and are securely stored on encrypted Azure storage. Backup jobs are monitored by CSP personnel and actions are taken in case of failure. CSC can request restore from CSP by contacting iQ.Suite aaS Support Team.

4.13 Technical vulnerability management

Continuous vulnerability management is performed by Azure Defender for Azure SQL and Azure Defender for Servers, which has integrated vulnerability assessment solution by Qualys. Identified vulnerabilities are remediated in a timely manner, according to their criticality.

4.14 Service and business continuity

"iQ.Suite aaS" is built for resiliency. To ensure its continuous operation, an approach for redundancy is taken in the design of the service. Availability and integrity of the service are ensured through the implementation of data backups, load balancing and Azure availability sets. Different business continuity scenarios, including pandemic, are defined, and tested on annual basis.

5 Related documents

- Information Security Policy – BP-IS-PLCY-00
- ISO/IEC 27001:2013 standard, clauses Annex A.
- ISO/IEC 27017:2015 standard

6 Definitions and Terms

CSP – Cloud Service Provider

CSC – Cloud Service Customer