



iVigee Services a.s.

Information Security Whitepaper

IVI-QM-007


Version number: 1.0

Effective Date: *31-JAN-2022*

Supersedes: Not applicable

ivigee	Information Security Whitepaper	
	QUALITY MANUAL (QM)	
Effective date: see the title page	Code: IVI-QM-007	Version Number: 1.0

1 APPROVAL SIGNATURES


Printed Name:	Robert Scheiner	Date:	
Role/Position:	Author / CIO	Signature:	
Printed Name:	Tomáš Musil	Date:	
Role/Position:	Content Reviewer / CFO	Signature:	
Printed Name:	Marcela Fialová	Date:	
Role/Position:	Approver / COO	Signature:	

2 REVISION HISTORY

Version	Effective date	Author	Revisions
1.0	See the title page	Robert Scheiner	Initial version

– CONFIDENTIALITY AND PROPRIETARY INFORMATION –

This document contains confidential information. Any use, distribution, or disclosure without the prior written consent of iVigee Services, a.s. is strictly prohibited except to the extent required under applicable laws or regulations.
It is the responsibility of the user to verify that this copy is of the latest revision.

	Information Security Whitepaper	
	QUALITY MANUAL (QM)	
Effective date: see the title page	Code: IVI-QM-007	Version Number: 1.0

3 TABLE OF CONTENTS

1	APPROVAL SIGNATURES	2
2	REVISION HISTORY	2
3	TABLE OF CONTENTS	3
4	ABBREVIATIONS AND DEFINITIONS	4
5	PURPOSE, SCOPE AND USERS	4
6	REFERENCES	4
6.1	EXTERNAL	4
6.2	INTERNAL	4
7	ACCEPTABLE USE OF INFORMATION ASSETS	5
7.1	ACCEPTABLE USE.....	5
7.2	TRUSTED CLOUD-PROVIDERS	5
7.3	SECURING DATA IN TRANSIT AND AT REST	5
7.4	RESPONSIBILITY FOR ASSETS	5
7.5	EMPLOYEE BACKGROUND CHECKS.....	5
7.6	SECURITY TRAINING FOR ALL EMPLOYEES.....	6
7.7	PROHIBITED ACTIVITIES	6
7.8	TAKING ASSETS OFF-SITE.....	6
7.9	RETURN OF ASSETS UPON TERMINATION OF CONTRACT.....	6
7.10	BACKUP PROCEDURE	6
7.11	ENTERPRISE-GRADE ANTIVIRUS	7
7.12	AUTHORISATION FOR INFORMATION SYSTEM USE	7
7.13	USER ACCOUNT RESPONSIBILITIES.....	7
7.14	PASSWORD RESPONSIBILITIES	7
7.15	CLEAR DESK AND CLEAR SCREEN POLICY	8
7.16	E-MAIL AND OTHER MESSAGE EXCHANGE METHODS	8
7.17	INCIDENTS & DATA BREACHES.....	8

– CONFIDENTIALITY AND PROPRIETARY INFORMATION –

This document contains confidential information. Any use, distribution, or disclosure without the prior written consent of iVigee Services, a.s. is strictly prohibited except to the extent required under applicable laws or regulations. It is the responsibility of the user to verify that this copy is of the latest revision.

ivigee	Information Security Whitepaper	
	QUALITY MANUAL (QM)	
Effective date: see the title page	Code: IVI-QM-007	Version Number: 1.0

4 ABBREVIATIONS AND DEFINITIONS

Term/Abbreviation	Definition
Information system (IS)	Includes all platforms, servers and clients, network infrastructure, system and application software, data, and other computer subsystems and components which are owned or used by the organisation, or which are under the organization's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, e-mail, etc.
Information assets	In the context of this document, applies to information systems and other information/equipment including paper documents, mobile phones, portable computers, data storage media, etc.

5 PURPOSE, SCOPE AND USERS

The purpose of this document is to present to iVigee's business stakeholders its commitment to information security best practices. Many of the controls listed are applied to the entire scope of the company's Information Security Management System (ISMS), and to all personal data processing activities.

6 REFERENCES

6.1 External


Document Reference /Title
ISO/IEC 27001 standard, clauses A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2
EU GDPR Article 32

6.2 Internal

Document Reference	Title
IVI-SOP-GEN-002	Document Management
IVI-SOP-GEN-016	Incident Response Procedure

– CONFIDENTIALITY AND PROPRIETARY INFORMATION –

This document contains confidential information. Any use, distribution, or disclosure without the prior written consent of iVigee Services, a.s. is strictly prohibited except to the extent required under applicable laws or regulations. It is the responsibility of the user to verify that this copy is of the latest revision.

	Information Security Whitepaper	
	QUALITY MANUAL (QM)	
Effective date: see the title page	Code: IVI-QM-007	Version Number: 1.0

7 ACCEPTABLE USE OF INFORMATION ASSETS

7.1 Acceptable use

Information assets may be used only for business needs with the purpose of executing organisation related tasks.

7.2 Trusted cloud-providers

All iVigee platform systems are cloud-based by preference. Only leading trusted cloud vendors are used which:

- implement the best security practices within the field,
- meet regulatory compliance, e.g., GDPR, GxP,
- offer EU-sovereign data centres which guarantee EU data residency, meet EU privacy and security requirements, and allow iVigee to protect its most sensitive data as required.

7.3 Securing data in transit and at rest

For iVigee cloud-based providers, data in transit and at rest is encrypted using strong encryption protocols and technologies including Transport Layer Security/Secure Sockets Layer (TLS/SSL) and Internet Protocol Security (IPSec) or Advanced Encryption Standard (AES).

For data residing (temporarily) at workstations, data at rest is protected based on workstations using encrypted disks, as well as enforcing relevant set of CIS Benchmark policies, e.g., clear screen policy.

7.4 Responsibility for assets


Each information asset has a described purpose, owner and access controls designated in our company's internal Inventory of Information Assets. The asset owner is responsible for the confidentiality, integrity and availability of information of the asset in question.

7.5 Employee background checks

For each new employee, iVigee verifies an individual's education, previous employment, criminal record check and possibly other sources relevant to the position and local labour regulations.

– CONFIDENTIALITY AND PROPRIETARY INFORMATION –

This document contains confidential information. Any use, distribution, or disclosure without the prior written consent of iVigee Services, a.s. is strictly prohibited except to the extent required under applicable laws or regulations. It is the responsibility of the user to verify that this copy is of the latest revision.

	Information Security Whitepaper	
	QUALITY MANUAL (QM)	
Effective date: see the title page	Code: IVI-QM-007	Version Number: 1.0

7.6 Security training for all employees

All iVigee employees undergo cyber-security awareness training as part of the induction process and relevant updates throughout their careers. They also agree to the company's Code of Conduct, highlighting various aspects of information security.

7.7 Prohibited activities

It is prohibited:

- to use information assets in a manner that unnecessarily takes up capacity, weakens the performance of the information system or poses a security threat,
- to download image or video files which do not have a business purpose, send e-mail chain letters, play games, etc.,
- to install software on a local computer without explicit permission,
- to use cryptographic tools (encryption) on a local computer, with the exception of password managers,
- to download program code from external media,
- to install or use peripheral devices such as modems, memory cards or other devices for storing and reading data (e.g., USB flash drives) without explicit permission.

7.8 Taking assets off-site

Equipment, information, or software, regardless of its form or storage medium, cannot be taken outside of usual places of work without prior permission. If said assets are outside the organisation, they must be controlled by the person who was granted permission for their removal.

7.9 Return of assets upon termination of contract

Upon termination of an employment contract or other contract on the basis of which various equipment, software or information in electronic or paper form is used, the user must return all such information assets.

7.10 Backup procedure


All important business information must be stored within company's designated Document Management System.

iVigee uses cloud vendors for its information assets. The two major vendors where iVigee's critical business information is stored are Microsoft Azure and Atlassian Cloud. They implement the following facilities:

- Internal frequent active backups, typically daily. Although these are for internal vendors' needs mainly, they may be provided based on ad-hoc justified request.

– CONFIDENTIALITY AND PROPRIETARY INFORMATION –

This document contains confidential information. Any use, distribution, or disclosure without the prior written consent of iVigee Services, a.s. is strictly prohibited except to the extent required under applicable laws or regulations. It is the responsibility of the user to verify that this copy is of the latest revision.

	Information Security Whitepaper	
	QUALITY MANUAL (QM)	
Effective date: see the title page	Code: IVI-QM-007	Version Number: 1.0

- SW facilities where all deleted content is by-default placed into “trash bins”, minimizing the risk of losing information or being unable to retrieve accidentally deleted items for a reasonable time. The trash is kept for 60 days for Atlassian Cloud, or 93 days for Office365/SharePoint. After this, the information is permanently deleted.

iVigee implements ad-hoc back-ups within own bespoke solutions based on business and clients’ needs.

7.11 Enterprise-grade antivirus

An endpoint protection solution is installed on each workstation, with activated automatic updates. This solution is managed centrally and identified threats and alerts are acted upon swiftly.

7.12 Authorisation for information system use

Users of the information system may only access those information system assets for which they have been explicitly authorised by the asset owner. Users may use the information system only for purposes for which they have been authorised, i.e., for which they have been granted access rights. It is explicitly forbidden for users to take part in activities which may be used to bypass information system security controls.

7.13 User account responsibilities

Users must not, directly or indirectly, allow another person to use his/her access rights, i.e., username, and must not use another person’s username and/or password. The use of group user names is forbidden. The owner of the user account is its user, who is responsible for its use, and all transactions performed through this user account.


7.14 Password responsibilities

Users must apply good security practices when selecting and using passwords:

- passwords must not be disclosed to other persons, including management and system administrators
- passwords must not be written down
- user-generated passwords must not be distributed through any channel (using oral, written or electronic distribution, etc.)
- passwords must be changed if there are indications that the passwords or the system may have been compromised – in that case a security incident must be reported
- password must be changed at first log-on to a system

– CONFIDENTIALITY AND PROPRIETARY INFORMATION –

This document contains confidential information. Any use, distribution, or disclosure without the prior written consent of iVigee Services, a.s. is strictly prohibited except to the extent required under applicable laws or regulations. It is the responsibility of the user to verify that this copy is of the latest revision.

	Information Security Whitepaper	
	QUALITY MANUAL (QM)	
Effective date: see the title page	Code: IVI-QM-007	Version Number: 1.0

- passwords must not be stored in an automated log-on system (e.g., macro or browser) except for an approved password vault tool
- passwords used for private purposes must not be used for business purposes

For its critical systems and services, iVigee uses central Identity Management of Azure AD within its Office 365 subscription. It provides authentication and SSO capabilities for other systems (e.g., Atlassian, e-learning, workstations), and enforces strong password policy and multi-factor authentication.

7.15 Clear desk and clear screen policy

If the authorised person is not at his/her workplace, all paper documents, as well as data storage media labelled as “confidential” or higher, must be removed from the desk or other places (printers, fax machines, photocopiers, etc.) to prevent unauthorized access. Such documents and media must be stored in a secure manner in accordance with the Information Classification Policy.

If the authorised person is not at his/her workplace, all sensitive information must be removed from the screen, and access must be denied to all systems for which the person has authorisation. In the case of short absence (up to 30 minutes), the clear screen policy is implemented by logging out of all systems or locking the screen with a password.

7.16 E-mail and other message exchange methods

Users may only send messages containing true information. It is forbidden to send materials with disturbing, unpleasant, sexually explicit, rude, and slanderous or any other unacceptable or illegal content. Users must not send spam messages to persons with whom no business relationship has been established or to persons who did not require such information.

7.17 Incidents & data breaches

Each employee, supplier or third person who is in contact with data and/or systems of iVigee must report any system weakness, incident or event pointing to a possible incident as specified in the Incident Response Procedure.

The end of the document.

– CONFIDENTIALITY AND PROPRIETARY INFORMATION –

This document contains confidential information. Any use, distribution, or disclosure without the prior written consent of iVigee Services, a.s. is strictly prohibited except to the extent required under applicable laws or regulations. It is the responsibility of the user to verify that this copy is of the latest revision.