Information Security Policy

Author: Rutger Bremer & Dennis van Eijk

Document reference: MMISP1706

Confidentiality: Confidential

Company internal:

Colofon

Filename	MMISP1706		
Reference	MMISP1706		
Author	Rutger Bremer	Confidentiality	Company Internal
Version	2.0	Date	14 August 2020

Document History

Version	Date	Author	Remarks
1.0	23-09-2013	Rutger Bremer	Initial document
1.1	14-11-2015	Rutger Bremer	Update security standards
1.2	11-01-2016	Rutger Bremer	Password policy update
1.3	23-03-2016	Rutger Bremer	Patch management policy
1.4	21-12-2016	Rutger Bremer	Account / user role update Update security standards
2.0	03-06-2017	Rutger Bremer	Complete review Information Security standard
2.0	12-07-2018	Rutger Bremer	Reviewed without changes
2.0	18-08-2019	Rutger Bremer	Reviewed without changes
2.0	14-08-2020	Rutger Bremer	Reviewed without changes

1 Introduction

Information and information systems are important assets of Momice. We have policies and procedures in place to ensure that information and information systems are properly protected. At Momice we foster our open and accessible business culture and strong connection with our clients. Our clients trust us with their data and we have therefore established this document as part of our efforts to establish a security framework that meets and exceeds industry standards for information security.

2 Responsibility for Information Security

It is the responsibility of the Information security manager (ISM) to maintain the ISP for Momice. It is the responsibility of all involved at Momice to uphold the principles of this policy and safeguard the information. All employees, contractors and third parties working with Momice are expected to comply with the ISP.

At Momice the ISM holds a special role. The Information Security Manager should:

- Be a contact person for inside and outside contact regarding information security.
- Oversee supplier related information security issues.
- Identify security related processes, documents and assets in the organisation, ensure ownership and accountability, and assign access levels or responsibility to assign these access levels.
- Act as key contact with authorities in case of an information security breach
- Ensure proper documentation.

If there are any questions concerning information security, its policies, documents, requests, exceptions, compliance or any oversight, please contact:

- Rutger Bremer (ISM for Processes)
- Arjan Slaager (ISM for IT management)

3 Information Security Policy

This ISP provides management direction and support for information security in accordance with business requirements and relevant laws and regulations.

4 Information Security at Momice

4.1 Internal Focus

The ISM and Risk & Compliance Manager monitor and evaluates the information security program's effectiveness throughout the year. The ISM ensures the information security program is modified, as appropriate, to respond to changes in technology, business objectives (acquisitions, outsourcing, third-party agreements, etc.), and relevant threats (both internal and external) and oversees any necessary policy changes.

4.2 External Focus

The security of client data is Momice's main concern and point of focus. Momice operates with a risk based approach. The security of information and Momice's information processing (facilities) must not be reduced by the introduction of external party products or services. Any access to Momice it's information processing (facilities) and processing and communication of information by external parties must be controlled.

5 Asset Management

5.1 Responsibility for Assets

Assets shall have a designated owner and be accounted for. For specific guidance regarding this policy, please contact the ISM.

Momice's assets include hardware, software, information, documents, databases, keys, knowledge and everything else that holds value to Momice. Assets that hold sensitive information are deemed relevant from a security perspective and should therefore all be tracked.

Downloading or installation of software programs not authorized by the ISM is strictly prohibited. Connection of personally owned computers or other personally owned devices to Momice's core network is allowed after obtaining prior approval from the ISM.

Employees may use many forms of communications including, but not limited to: e-mail, instant messaging, blogging, voice communications, and written communications to perform their jobs and provide value to the company. When communicating, each employee needs to exercise good judgment in a manner that ensures the privacy and safety of clients, other employees, contractors and third parties, as well as the privacy, safety and confidentiality of Momice and its information and data as well as third party information and data.

5.2 Data Classification

Information assets must be classified to indicate the need, priorities, and expected degree of protection when handling the information.

Classification	Applies to	Access allowed by
Secret	Asset or information defined in Process Access and Identity Management document as secret (possible example: personally identifiable client data). As determined by Momice employee or contractor and clearly labelled as such on every page or part.	Parties designated by the data owner. Vetted employees, suppliers and contractors after explicit executive permission by Momice.
Restricted	Asset or information defined in sensitive assets (possible example: marketing plan). As determined by Momice employee or contractor and clearly labelled as such on every page or part.	Parties designated by the data owner. Employees, suppliers, contractors and specific clients or other external parties that have signed an NDA and have been given access to this data by Momice.
Public	Any other document	No restrictions apply.

5.3 Physical media

Physical media such as USB sticks or memory cards that can contain sensitive data are particularly prone to data breach. They are plentiful, small, easy to forget somewhere, and a single can contain massive amounts of information. At Momice we discourage using physical media for transferring sensitive information. In case it is really necessary, the following procedure are in place:

- Always use trusted media that you have received from the company itself, or have acquired yourself. If you find a USB stick, mouse, keyboard, or other media somewhere without a clear owner, label where it was found and deposit it at the Information Security Manager or your manager. Under no circumstances put it in a Momice computer.

- Delete all existing data from the media in an unrecoverable way.
- Transfer the data with the media to the target device. If possible use encryption. If using encryption is not possible, be extremely cautious about using it outside of Momice premises.
- After finishing, delete all existing data from the media in an unrecoverable way, or destroy the media if that is not possible.

5.4 Inventory

When transferring systems from one person to the other, all information carrying media like hard drives are overwritten in an unrecoverable way, or destroyed. The ISM are ascertain that the people responsible for this are aware of proper ways to make data unrecoverable. Only the assets that fall under the above headings are relevant to this information security policy.

The following restrictions apply to company assets:

- The ISM are determine security measures that are applied to the device
- Whenever possible, company assets are use encryption, a backup solution and a virus scanner.
- Employees only use the company asset that contains or has access to sensitive information for performing company related tasks. If the employee wants to perform other tasks (read news, user social media, use private email, install games), the employee will use a different machine that doesn't include sensitive information.
- Security measures provided by the company such as a VPN connection, virus scanner,account restrictions and automatic updates are not disabled.
- In case of loss or theft of device, the ISM are notified immediately

6 Human Resources Security

6.1 Prior to Employment

When selecting and onboarding new employees or contractors the security aspects should also be considered. Screening and background checks are to be performed depending on the role of the new person.

In order to reduce the risk of theft, fraud or misuse of assets; employees, contractors and third party users must understand their responsibilities and must be suitable for the roles for which they are being considered.

6.2 During Employment

Employees, contractors and third party users must be aware of information security threats and concerns, their responsibilities and liabilities, and be equipped to support the ISP in the course of their normal work.

6.3 Termination or Change of Employment

Employees, contractors and third party users shall exit the organization or change employment in an orderly manner.

7 Access Control

7.1 Business Requirement for Access Control

Access to information, information processing facilities, and business processes must be controlled on the basis of business and security requirements.

7.2 User Access Management

Formal procedures must be in place to control the allocation of access rights to information systems and services including user registrations, privilege management, password management and review of access rights.

7.3 User Responsibilities

The cooperation of authorized users is essential for effective security. Users are responsible for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

7.4 Network Access Control

Access to both internal and external networked services must be controlled.

7.5 Operating System Access Control

Security facilities must be used to restrict access to operating systems to authorized users.

7.6 Application and Information Access Control

Security facilities must be used to restrict access to and within application systems.

7.7 Mobile Computing and Telecommuting

When using mobile computing the risks of working in an unprotected environment must be considered and appropriate protection applied.

8 Information Systems Acquisition, Development and Maintenance

Momice IT will assist with the implementation of any technical security control deemed necessary by the information security program. Momice will ensure to employ, contract or purchase sufficient expertise regarding the security of its information systems.

8.1 Security Requirements

Security requirements must be identified and agreed upon prior to the development and/or implementation of information systems, as part of the overall business case for an application/information system.

8.2 Correct Processing in Applications

Appropriate controls must be designed into Momice applications, including user developed applications, to ensure correct processing. Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls must be determined on the basis of security requirements and risk assessment.

8.3 Cryptographic Controls

Controls, including key management, must be in place to support the use of cryptographic techniques, such as for example with SSH tunnel.

8.4 Security of System Files

Access to system files and program source code must be controlled and IT activities conducted in a secure manner.

8.5 Security in Development and Support Processes

Project and support environments must be controlled. Employees, contractors and third parties must ensure that all proposed system changes are reviewed to check that they do not compromise security.

8.6 Technical Vulnerability Management

Technical vulnerability management must be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness.

9 Physical and Environmental Security

9.1 Secure Areas

Critical or sensitive information processing assets must be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They must be physically protected from unauthorized access, damage, and interference. The protection provided must be commensurate with the identified risks.
Momice only partners with third parties that can ensure secure areas.

10 Communications and Operations Management

10.1 Operational Procedures and Responsibilities

Responsibilities and procedures for the management and operation of all information processing facilities must be established. This includes the development of appropriate operating procedures. Segregation of duties must be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

10.2 Third Party Service Delivery Management

The implementation, compliance and service delivery of third party agreements must be reviewed and changes managed to ensure that the services delivered meet all requirements.

10.3 System Planning and Acceptance

The operational requirements of new systems must be established, documented, and tested prior to their acceptance and implementation, including the Software Development Life Cycle.

10.4 Protection Against Malicious and Mobile Code

Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code.

10.5 Back-Up

Routine backup procedures must be established and implemented to ensure the integrity and availability of information.

10.6 Network Security Management

Information assets and the supporting infrastructure must be adequately protected by use of Network Controls and Security of Network Services.

10.7 Patch/update management

Production servers should be updated and patched at least monthly and/or in case of serious events. An administrator approved by Momice management may perform these patches. Backups should be in place in case a patch goes wrong.

10.8 Media Handling

Media must be controlled and physically protected. Operating procedures must be established to protect information, in all forms, from unauthorized disclosure, modification, removal, and destruction.

10.9 Exchange of Information

Exchanges of information and software between Momice and other organizations must be carried out in line with formal exchange agreements. Procedures and standards must be established to protect information including during transit.

10.10 Electronic Commerce Services

The integrity and availability of electronic commerce services must be secured.

10.11 Monitoring

Key systems must be monitored and information security events recorded to include audit logging, system use, administrator and operator logs, fault logging, and synchronization of

system clocks. Protection of log information is the responsibility of the ISM and the retention of logs must meet requirements defined in the Records Management Policy.

In case of an attempt to access data that the user is not allowed to access, system administration should be notified and an administrator needs to check the access log for this user to check for any unusual patterns. In case of an attempted breach, appropriate actions should be taken, including immediately limiting the ability of this user to make further attempts at breaching.

Log files may contain personally identifiable information, and are therefore considered sensitive data. Additional security is applied to the log as necessary.

11 Third party supplier relationships

11.1 Third party suppliers

Momice software is built upon industry standards, and external dependencies for parts that are critical in terms of sensitive data are limited. However, in the case that a supplier does need to touch upon sensitive parts, the following policy is enacted:

- The business registration details of the supplier are verified
- The supplier is requested for its information security policy
- The security policy is compared to our own policy, and differences are considered by management to see if they are acceptable
- In case the supplier doesn't have a security policy, we will on a case-by-case basis determine the parts of our security policy that apply to our situation, and try negotiate an agreement to make a SLA that covers our security requirements. This is of course not always possible. On a case by case basis it are determined what is acceptable
- An agreement is reached with the supplier about acceptable use of our data and adhering to our classification and security policies
- There are explicit agreements in place what happens if the supplier cannot adhere to the conditions put forward, or an information security breach takes place
- Management will decide if it's necessary to negotiate a right to audit with the supplier
- Suppliers can have sub-suppliers. Measures are in place to ascertain that our sensitive data is still protected in the supply chain
- Supplier relationships are always validated and approved by management and tracked by the ISM
- Sub-suppliers are not allowed to work on the source code.

12 Information Security Incident Management

12.1 Reporting Information Security Events and Weaknesses

Information security events and weaknesses associated with the applications and information systems must be communicated in a manner allowing timely corrective action to be taken.

12.2 Management of Information Security Incidents and Improvements

A consistent and effective approach must be applied to the management of information security incidents. Please also refer to Momice end-to-end Incident Management process document.

13 Business Continuity Management

13.1 Information Security Aspects of Business Continuity Management

A business continuity management process must be implemented to minimize the impact on the events and data of Momice clients and Momice itself and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls.

14 Compliance

Appropriate measures must be in place to avoid the violation of any law, statute, or regulation and the breach of any contractual obligations and security requirements.

14.1 Compliance with Legal Requirements

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements. Momice follows the upcoming GDPR regulation and the Dutch 'Wet bescherming persoonsgegevens' (Wbp).

14.2 Compliance with Security Policies and Standards, and Technical Compliance

Compliance with security policies and standards is required and regularly reviewed.

14.3 Information Systems Assessment Considerations

Controls must be implemented to maximize the effectiveness of and to minimize interference with the information systems assessment process.