

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

INDEX

1	General Security Requirements	2
2	Rules for controlling physical access	3
2.1	Rules for working in the safe area	4
3	Rules for controlling logical access	4
3.1	Rules for registering users	4
3.2	Assignment of credentials and first use	4
3.3	Credentials management	5
3.4	Deactivation/varation	6
3.5	Loss, bocking of the system and registration	6
3.6	Credential monitoring	6
3.7	Cessation of use of personal credentials	6
3.8	PWD of applications and domain access	6
3.9	System Administrator PWD (Domain, Production Server, Networking)	7
3.10	Change Management	7
3.10.1	Change Management Process	7
4	Rules for the desk and the clean screen	8
5	Rules for unattended equipment	8
6	Rules against malicious codes and mobile codes	9
7	Media Rules	9
8	Rules for safe disposal of media	9
9	Rules for managing communications	10
10	Rules for the installation and control software	11
11	Encryption Laptop devices	11
12	Rules for Business Continuity	11

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

1 General Security Requirements

The purpose of this document is to define the physical and logical safety rules active in MYMOON and to inform the staff about them.

Here are the rules to prevent unauthorized physical and logical access, which can cause damage or interference to critical information and to the performance of activities relevant for the purpose of certification of the ISMS. The guidelines, shown below, refer to the perimeter of the object of purpose. Furthermore, general safety rules are defined to which each resource is subject, internal or external to d MYMOON, which comes into contact with the company's activities.

All MYMOON personnel are required to apply and comply with the following safety regulations.

There are no network devices and / or devices other than the Firewall owned by the Internet Provider. An administrative credential is available only to personnel authorized by authentication and authorization (userid / password) in order to configure only some aspects such as DHCP and Wifi. In case of loss of access, a reset of the device can be carried out which, at the next boot, re-downloads the centralized configuration from the provider.

Company information cannot be disclosed outside MYMOON unless otherwise communicated or authorized by the Management.

It is specified that all resources operating on behalf of MYMOON are required to guarantee compliance with the principle of confidentiality, integrity and availability (RID) of company information, or of our customers.

The reference legislation and any contractual obligations regarding information security are specified for each person operating in the perimeter on the basis of the assignment.

Each user (internal or external authorized personnel) is enabled to access according to production needs. L and credentials are periodically updated.

The level of access to applications, systems or documents is profiled by inserting the personal credentials into Groups according to the operational and production needs established by the Management, on which the permissions to access the various resources are then enabled. The only exception is made for the Company PC, where the defined user is the administrator of the same.

The security perimeter coincides with the offices of the building in Via dei Prati Fiscali 199 where Mymoon is based. These relate to the office on the second floor where access and exclusively on technical, commercial and administrative. Processes are carried out within the premises present in the office and primary assets are located and secondary ones supporting business processes are located. Within the perimeter, the risk assessment was carried out and the countermeasures defined in the SOA with the exclusions justified in the latter are applicable.

The following document therefore describes in detail the measures aimed at guaranteeing company standards:

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

- Physical Security Rules of the Area in which the activities subject to certification are provided , i.e. against access to the physical perimeter ;
- Logical safety rules in the use of information processing systems and services.

2 Rules for controlling physical access

Physical access controls guarantee supervision on all environments that contain company information, network equipment, LANs, electrical systems, air conditioning systems, transmission lines, backup media, documents and any other element required for the management and maintenance of systems.

Physical access controls guarantee the safe use of company information and not only, and the protection of premises containing MYMOON systems.

In particular, the following controls were taken into consideration and implemented:

Given the particular nature of the operational procedures in place, physical access to the perimeter is allowed only to management and employees. There is currently no access for guests, even if a guest registry has been prepared in advance (see: *I know 27k_RIN - RegistryIngressi "*) with the following information :

- *Entry date*
- *Surname and name*
- *Company affiliation*
- *Mymoon contact person authorizing access*
- *Time of entry and exit.*

There is currently no technical area. Since all the data is on Microsoft Office 365, there is nothing inside the office as a technical infrastructure (the only exception is the presence of the Firewall owned by the Internet Provider)

Given the specific nature of the activities carried out within the operational headquarters , loading and unloading activities of materials related to personal productivity (notebooks and accessories they need) are possibly provided for at the entrance of the office itself, subject to prior staff checks by Mymoon .

All Mymoon personnel are required to promptly report any attempt (real or presumed) to violate the procedures for accessing the physical perimeter to the security manager.

The physical safety perimeter is protected by doors with controlled opening through the use of a mechanical key.

Currently there is no alarm for access afterhours, since after the office hours there is no " sensitive " material inside the office itself. All company laptops are taken away by their respective assignees. The only things left in the office are the printer and the firewall (which alone connects to the internet).

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

2.1 Rules for working in the safe area

Mymoon personnel are trained and trained in the security procedures in place in the security perimeter in accordance with current legislation. The classic identification of the Technical Area with the security perimeter in this case is confirmed and coincides with the offices in via dei Prati Fiscali 199 , even if the connectivity inside the office takes place with Wireless connections and not on wired LAN. (A wired network is available, but there is currently no device connected to it. The only exception is that of the printer)

3 Rules for controlling logical access

Logical access controls provide a technical tool to supervise a user's access to system resources and information. This is in order to guarantee the control of the information that users can use, view and / or modify.

A computer authentication system is adopted to regulate access to the system, network or data. Mymoon users can access the system, the network or an internal database using authentication credentials consisting of an identification code (user-id) and a reserved password (password) known only by the interested party.

Is on going also the installation of a domain controller that guarantee centrally manages access for users, PCs and servers on the network. It does this using Active Directory.

Credentials are specified in the system present in Office365, and are necessary to access the documents. Each personal credential is then assigned to one or more groups created by function, such as Marketing, Administration, Technical Support, Members, etc ..) and the various document resources present on the have specific authorizations assigned to the various groups. In the online sharepoint, there are documentary sections accessible only to members, or only to personnel belonging to the Technical Support group, etc. etc ..

3.1 Rules for registering users

All personnel operating within the perimeter or having access to perimeter resources have credentials which must be checked and updated periodically by the Technical Director (DT).

Occasional suppliers and uninvited guests are not allowed, that is, as already indicated above, access is guaranteed only to the management and staff you depend on.

The first credentials are assigned by the Technical Director (DT). Credentials are created with the flag that imposes the obligation to change the password at the first access. At the first logon, Office365 requires the change of the password used.

The passwords are secret, improper typing, even repeated, will not lead to the blocking of the user id, but the restoration of the password can only be resolved by means of a request to the DT.

3.2 Assignment of credentials and first use

Personal credentials (e.g. userid and password) are assigned and customized according to the activities, responsibilities and authority (profile) of people in accordance with Mymoon processes. The profiles can be updated to meet specific needs but, in any case, always authorized by the Management.

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

The profiles authorize people to access the applications, information and systems necessary for the work activity related to the role covered. The profile assigns a degree of confidentiality in relation to the type of information that the person can access, it also safeguards the integrity of the information accessed by limiting the possibility of modification if not expressly authorized and accessibility to the information necessary for the performance of its activities. It is possible that a user gets different credentials to access different systems, in this case, for example, the user id will be different as well as the passwords to be used. This situation occurs in the case of access to the corporate laptop, which takes place with different credentials than those of the data and Office 365 applications. A copy of the data is made quarterly to an external hard disk.

Local credentials are completely managed by the user. Centralized management of laptops given to users is not possible, as the system does not allow this. Laptop disks are still encrypted, in this way they guarantee superior security levels.

Logical access to information processing systems and infrastructure systems refers to the following systems:

- PC laptop access the system Microsoft Office 365 and, limited access to the administration software of management accounting. It can be accessed via an authenticated connection and a Citrix client. No component of the Management software is stored on the company laptop.
- Virtual machines (which are created on the laptops of the technical staff if necessary) to test any new software to be evaluated or software for which certification is in progress. The environments live inside virtual machines and never have contact with data on Office 365 or with company resources (except for internet access).

The authorization profiles allow those who access the systems to operate with specific rights on the information. The credentials for accessing the applications and systems with the relative authorization levels are assigned to the individual users:

- Logically: from the functions directly responsible for the services to which the authorized users will access through the information systems;
- Technically: by system and application administrators who set rights based on the configuration screens of each individual system / application, if any.

3.3 Credentials management

Personal codes are confidential and secret, any violation will be punished and prosecuted as required by the Policy and possibly by applicable laws.

It is forbidden to keep any form of unprotected registration of the assigned personal codes (user / password), unless specifically authorized and in the manner specifically described from time to time defined by the Technical Director DT.

Personal codes must be modified according to the Security Policy, however within the expiry period, safeguarding the generation criteria.

The user can decide to change their personal codes more frequently than that formally defined by the Security Policy.

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

In case of suspected compromise of security, the user is obliged to immediately change his personal codes and to notify the Technical Director of any compromise detected.

It is forbidden to enter users and passwords in the automatic logons of the operating system operating on laptops, or save them locally or activate services to remember them. This policy does not apply to operating systems on test virtual machines.

3.4 Deactivation/variation

The user unused -id for more than 6 months are switched off, this mode increases the level of security when the systems are also used by third parties or external users that carry out tests on suitably prepared environments.

3.5 Loss, blocking of the system and registration

If the pwd of simple users is blocked, a request must be made directly to the system manager by the requesting user. The procedure for replacing the first access is that previously described. No registration is required for this activity.

If the administration passwords are lost, the password recovery procedures made available on the Microsoft Office 365 platform are used.

3.6 Credential monitoring

Current credentials and profiles about the information on Office 365 is regularly monitored every six months or at least on the occasion of the internal audit, by the R ESPON s skilled IT or his delegate. This check is carried out against changes in the organization in terms of hiring / role changes / resignations. Any discrepancies must be immediately remedied and the causes analyzed to prevent recurrence. The profiles are reviewed annually to ensure their consistency and compliance with security policies. This review is handled by the IT Manager.

3.7 Cessation of use of personal credentials

If an MYMOON employee or a regular supplier ceases his activity which led him to act within the security perimeter (resignation, dismissal, etc.) or in any case is reassigned to other activities (transfer, promotion, requalification etc.) his credentials will be deleted and / or regenerated as necessary according to the new profile.

It is admitted that the Management will disable the user instead of deleting it, for the mere need to verify and historicize the user.

The absence of credentials does not allow the user to access MYMOON systems .

3.8 PWD of applications and domain access

Upon assigning the default password on first access, the user is obliged to modify it with the rules imposed by the Microsoft Office 365 platform ; the passwords for access to laptops instead follow the following rules :

- the length must be between 8 and 16 characters ;
- The password must contain elements of the following groups : AZ, az, 0-9, and at least one of the following special characters : ! @ # \$ % ^ & * - _ + = [] { } | \ : ' , . ? / ` ~ " < > () ;
- Passwords cannot contain the username alias, i.e. the part preceding the @ symbol

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

- the password does not expire , but the user is required and remembered via email to update their password periodically at least every 180 days.
- the passwords cannot contain the username or the name and surname of the user.

In addition, the following confidentiality requirements must be guaranteed for the password :

- it must be kept confidential;
- it is of strictly personal use;
- It is strictly forbidden to circulate credentials on electronic media (e.g. e-mails , documents of various kinds) or record them on paper (e.g. post it and / or documents of various kinds).

3.9 System Administrator PWD (Domain, Production Server, Networking)

Currently in the infrastructure there is no Active Directory Domain and / or Firewall / Networking equipment that needs to be managed.

3.10 Change Management

Change Management is an essential IT Service Management discipline, which ensures that changes to services and configuration items are documented, approved and implemented in a planned and controlled manner. Change Management enables beneficial changes while minimising disruption to IT Services. Mymoon utilises the software JIRA, to provide a process driven approach to the management and delivery of IT Services. Any change to production information systems including changes to hardware (servers, storage, network components etc.) and software (operating system, database, application code, configurations etc.) may introduce security risks to environment. The purpose of this Standard is to ensure that Requests for Changes (RFCs), handled through the Change Management Process are assessed for potential information security risks.

3.10.1 Change Management Process

- A formal Change Management Process must exist providing a consistent approach to initiate, execute and manage changes to the production environment. The Change Management process is reviewed annually.
- All changes must follow the Change Management Process.
- Key process compliance areas include:
 - a) All changes must be logged in the Change Management system.
 - b) Changes are to be assessed (by change reviewer / approvers) in line with the operational risk profile of the change to ensure that:
 - Change details, attributes and description have been documented correctly in the RFC.
 - The Change has been documented into the Forward Schedule of Change which must ensure that the Change conforms to specified, lead times and is being performed at an appropriate time which reduces the impact to business, students and collision with other proposed changes and operational schedules.
 - Appropriate level of testing has been undertaken which provides a high level of confidence that the change will be successful, and will not negatively impact production functionality.
 - Additional supporting documentation has been attached to the change or stored in an appropriate document storage repository, and

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

- Any changes deemed to present unacceptable level of risk are to be denied.
- c) All changes (other than those which a Change Manager has approved as emergency / retrospective change) must be fully approved in the Change Management system prior to implementation. Emergency changes are recorded retrospectively in the Change Management system within the next business day.



4 Rules for the desk and the clean screen

Depending on the classification of information, legal and contractual risks and internal risks, Mymoon has prepared the following rules:

- put sensitive and critical business information (e.g. on paper or electronic storage media) in a safe (locker or other safety-related furniture) when not needed.
- personal computers, workplaces, unattended must be locked (system lock);
- protection of information contained in mail, faxes, printers and copiers when unattended;
- the use of photocopiers and reproduction devices (eg scanners, digital cameras) must:
 - take place under the control of Mymoon personnel;
 - documents containing sensitive or confidential information must be immediately removed from the printer (which also acts as a fax, copier and scanner) .

5 Rules for unattended equipment

All the equipment assigned to a user (notebook, pen drive etc.) is regularly registered in the company inventory which also highlights its responsibility for protection and safekeeping.

Upon delivery, the user countersigns a document of acceptance and acceptance of the resulting responsibilities, including the information security provisions.

This document is kept by the Personnel Manager.

The applicable requirements are:

- CLOSURE working sessions at the end of activities.

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

- 5-minute screen saver activation with password protected re-activation .
- In the event of prolonged non-use, the equipment must be placed in special areas or protected with suitable means by the Personnel Manager.

6 Rules against malicious codes and mobile codes

The use of unauthorized software is prohibited.

The exchange and installation of software from outside such as peer to peer networks for the exchange of multimedia and recreational files, installations from pen drives and / or optical / magnetic media of any nature is prohibited.

It is forbidden to answer and / or start "chains of S. Antonio" or to collect and exchange e-mails that are not for business purposes.

The choice of anti-virus software and the sources of information about threats is made by DT and communicated to RISMS , relies hig her to suppliers of products with the presence of qualified and recognized market.

Currently, as part of Mymoon's IT infrastructure, there is the console of the Kaspersky platform delivered in « On Premise » mode.

The RISMS carries out the following activities with six-monthly and sample checks :

- that periodic updates are made and checked with security patches for the server systems used;
- to update their knowledge about new threats and vulnerabilities caused by malicious codes ; this update can take place in different ways such as newsletters, sector magazines, participation in working groups or conferences dealing with the indicated topics.
-

As part of the training programs implemented, the topic relating to the danger of using unauthorized software and browsing on unauthorized sites is always renewed.

For maintenance activities on systems, only authorized diagnostic and recovery software is used , no other type of software can be used unless previously assessed in terms of risk and approved by the technical director.

Each new software, potentially subject to installation, is checked (by the DT) before authorizing its use in the company environment.

7 Media Rules

Mobile devices (tablets / smartphones) are not allowed to access them within the company network. The use of portable memory devices is not authorized.

8 Rules for safe disposal of media

The following devices are considered removable media :

1. Laptops.
2. PDAs / Smartphones / Cell Phones / Tablets.
3. Pen drive.
4. CD / DVD / Floppy / DAT / LTO.
5. Printed paper.

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

The supports belonging to the first of the four categories are inventoried by the Safety Manager, and present in the hardware asset inventory.

For the latter, the applicable procedures apply according to the classification of the information.

Furthermore, all the supports are however treated as follows:

- when the content of a support is no longer necessary, it is destroyed through mechanical, electrical, electronic and / or IT precautions ;
- the disposal of the supports belonging to the first category must be authorized by the RISMS;
- the supports are stored in environments whose climatic factors have no influence on the physical-chemical characteristics of the supports themselves. Particular attention is paid to the specifications of the support supplier and diving into electromagnetic, humid and dusty fields is avoided ;
- for information managed on media whose life could be less than the retention time required for the information, there must be at least two copies and the same must be regenerated with a time shift equal to half the useful life of the medium;
- It does not authorize the use of external drives, CD, DVD, DAT personal pen-drives for data movement; only those made available by MYMOON must be used .

Failure to comply with this procedure is considered serious non-compliance while the loss of a support is a security incident and must be immediately reported by investigating the significance of the information lost in order to start any reporting procedures to the competent authorities.

9 Rules for managing communications

It is forbidden to reply to unknown links (phishing). Furthermore, all staff are required to verify the exact addressing of the sites to avoid the phenomenon of pharming (*manipulate the web addresses contained in a DNS server - Internet domain database - in order to camouflage the path that leads to the site*).

E-mail cannot be used outside of corporate communication needs. In the event of blatant SPAM, it is forbidden to open the message and especially the potentially dangerous attachments.

The Responsible for Safety (RISMS) (or in his place the Head of Communication), is responsible for periodically training and sensitizing all staff on the use of these rules.

The use of personal PDAs, smartphones and / or mobile phones is not recommended for storing any type of confidential information.

It is forbidden to make confidential communications to the mobile phone, even outside of MYMOON , in the presence of third parties who are not expressly authorized to learn about them, also by virtue of the possibility of telephone interception.

It is forbidden to leave confidential information (e.g. passwords) in the form of messages on the answering machine, as it could be listened to by unauthorized persons or the wrong recipient number could have been dialed.

During the copying and / or printing phases of the documents, if the operation was not successful, the document could have been stored / blocked in the printing device, in which case the user is asked to cancel his / her queue. print or remove the originals.

For the Portable PC, if it changes owner, a new nominal user is created. The old woman is erased with an erasing tool.

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

For a laptop that goes into decommissioning, data is erased before decommissioning.

Encryption is activated on smartphones by entering the PIN.

Pen Drive: Pen Drive are not allowed within the Mymoon facility. L and Uniche Pen Drive am put are encrypted but their use should be managed and supervised by the RISMS.

The use of CD / DVD is not foreseen

10 Rules for the installation and control software

The installation of software on operating systems is regulated as follows:

The software update is carried out according to the manufacturer 's default rules , or only by personnel authorized by the person responsible for the network infrastructures and technologies ;

The Office 365 infrastructure is managed directly by the Service Provider, while the local component of the Laptops has a single management, that is, each installation of a software is carried out by the office of the technical part, or in the presence or remotely , after checking the 'system administrator. Each installation provides a strategy for restoring to the state prior to the implementation of the changes;

Any decision to upgrade or to a new version must take into account the business requirements for change and the security of the new version. The removal or reduction of security weaknesses can also be implemented through patches as long as they are tested, authorized and approved by the systems and infrastructure manager.

11 Encryption Laptop devices

Corporate laptops are configured with active disk encryption, in order to raise corporate security levels. This further prevents the possibility of potentially sensitive data being lost or stolen. This action is initially carried out on the systems of the System Engineers, and starting from January 2019 it is extended to all company laptops. The encryption system envisaged is Microsoft's BitLocker, included in Windows 10. BitLocker is a data protection feature that integrates with the operating system and manages threats of data theft or exposure caused by loss, theft or theft. inappropriate computer shutdown. Data on a lost or stolen computer is vulnerable to unauthorized access, either by running a software attack tool or by transferring the computer's hard drive to another computer. BitLocker helps reduce unauthorized access to data by enhancing file and system protection , and also makes data inaccessible when computers protected with BitLocker are disabled or recycled.

12 Rules for Business Continuity

Continuity operating is guaranteed in full by the system Microsoft Office 365.

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

13 Prohibitions

In Mymoon, the principle applies that what is not expressly authorized is considered prohibited.

The following activities are generally prohibited (they can be carried out for verification purposes and to guarantee security only by IT or by previously authorized personnel):

- 1) use tools that are potentially capable of allowing unauthorized access to IT resources (verification software);
- 2) configure or reconfigure services already made available by IT, such as shares, access permissions, user profile settings, mailing services.
- 3) it is absolutely forbidden to access the premises and boxes reserved for network equipment, or make any changes to them without the authorization of IT;
- 4) it is forbidden to wire or connect equipment to the Company's network outlets without the authorization of IT;

Furthermore

- 5) any other illegal activity not listed here are expressly prohibited.
- 6) in any case, all activities that may represent a violation of the law on the legal protection of software and / or copyrights are expressly prohibited, including the unauthorized copying or dissemination of data and / or patented software.
- 7) in any case, all activities that can compromise in any way the intrinsic security of IT resources and the network are expressly prohibited.
- 8) it is forbidden to use network configurations and names not expressly assigned to the User by DT;
- 9) it is forbidden to use programs not authorized by DT;
- 10) it is not allowed to browse Internet sites not relevant to the performance of the assigned duties;
- 11) it is not allowed to carry out any kind of financial transaction, including remote banking operations, online purchases and the like, except in cases directly authorized by the Management and with compliance with the normal Company purchase procedures;
- 12) during the work activity, any form of registration (explicitly or through pseudonyms) to sites, forums, chat lines or messaging in general, whose contents are not related to the work itself, is prohibited;
- 13) it is not allowed to enter files (whether data or programs and / or software) on company-owned IT resources that have no bearing on one's work performance;
- 14) it is forbidden to install modems, especially if configured in call-back; (automatic recall)

MyMoon N.V.	INFORMATION SECURITY POLICY	Date 18/11/2025 Rev. 2
-------------	------------------------------------	------------------------------

15) it is forbidden to use devices or media (CD / DVD players, external disks, pen drives, etc.) not authorized by DT

It is also forbidden to take actions in order to:

16) degrade system resources,

17) prevent authorized users from accessing resources,

18) obtain resources higher than those already allocated and authorized,

19) accessing IT resources, both from the Company and from other non-corporate entities (Customers, Suppliers or other Entities in a general sense), violating their security measures;

20) access the system configuration files, make copies and transmit them to others;

21) disclose the passwords of others, as well as transmit in clear, publish or print technical information that can make the login known/ User accounts, host names and corresponding IP addresses of the Company's IT resources.