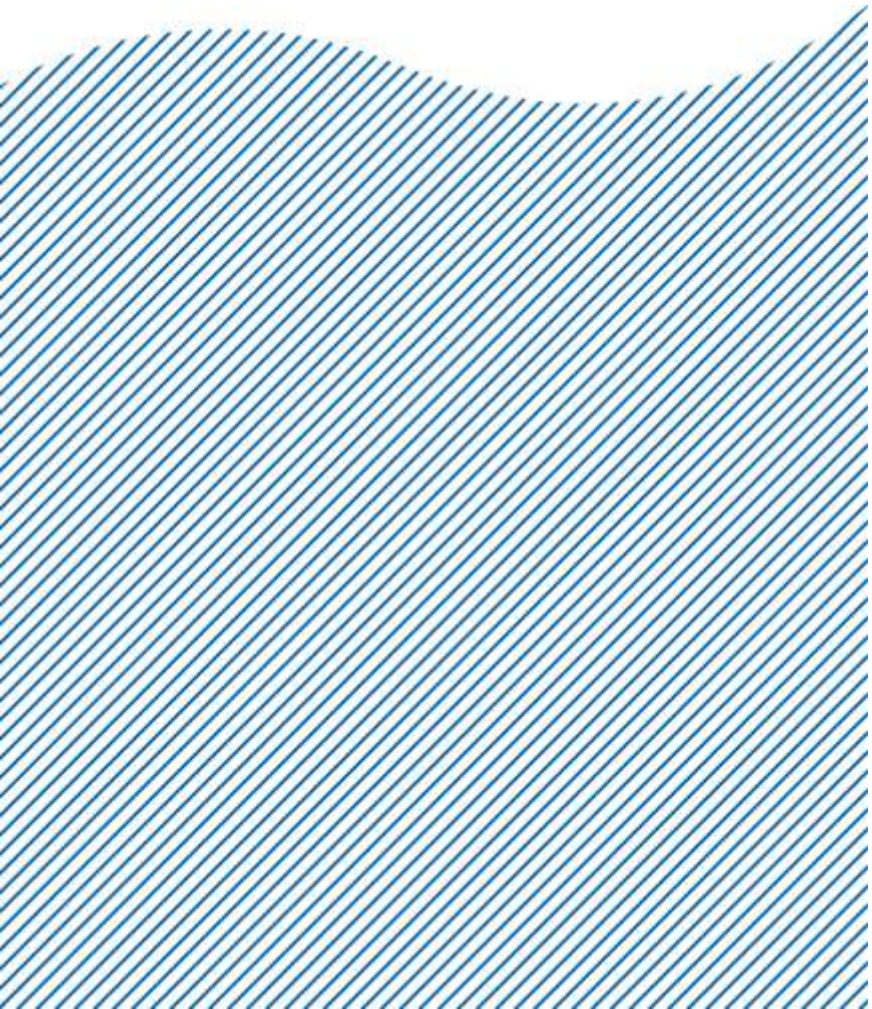
amadeus

CISO Office

Policy: Acceptable Use Policy

PL 15. Acceptable Use Policy



amadeus

Index

Document control

Security level	Confidential & Restricted			
Company	Amadeus IT Group SA			
Scope	All Business Units			
Audience	Amadeus user, HR department, Business Unit Security Officer			
Department	CISO Office			
Author	Damien Colomban			
Reviewed by	Ruairidh Wynne		**Date**	13/06/2017
Reviewed by	Sideth Chhor		**Date**	10/07/2017
Approved by	Alain Simon		**Date**	10/07/2017
Reviewed for applicability by	Julie Lorrain		**Date**	20/07/2023
Version	**Date**	**Change**	**Comment**	**By**
1.0	07/07/2017	Creation of a first version	Previous AUPs were already validated.	LEG-SEC-SMF (CISO Office)
1.1	05/09/2017	Minor updates following review from Risk and Compliance		LEG-SEC-SMF (CISO Office)
1.2	25/07/2022	Minor updates		LEG-SEC-SMF (CISO Office)

INTRODUCTION

1.1. Prologue

Sentences put in bold in the body of this document are the highlights of the mandatory control objectives.

This corporate policy is, by default, applicable according to the scope mentioned hereafter. In the case that a "localization" of this policy has been developed (e.g. due to local applicable laws and regulations) and approved by the CISO Office, this local policy takes precedence over the corporate policy for this location.

1.2. Purpose

Information, equipment and tools necessary for the use of information represent fundamental assets for Amadeus that must be secured for reasons including business security, legal, regulatory, ethical and contractual compliance and the protection of the Amadeus brand. Consequently, all information processing facilities under the control of Amadeus, which handle information important to the business of Amadeus, must be adequately protected.

This policy sets out the rules to be followed by all Amadeus users (employees, temporary employees, trainees, contractors, third parties and other personnel) regarding secure handling of business information/data and the usage of information systems under Amadeus control. In order to achieve this objective, it is vital that all Amadeus users conduct their daily business in a responsible, professional, ethical and lawful manner in accordance with this policy.

The required conduct is listed in a set of rules defining the acceptable and, in some cases, the non-acceptable use of information systems against illegal and/or damaging actions or omissions, whether such acts or omissions were committed knowingly or unknowingly.

SCOPE

This document is applicable to all Amadeus users (employees, temporary employees, trainees, contractors, third parties and other personnel), named hereafter "users", with access to Amadeus information across Amadeus Group's companies worldwide (fully & majority owned).

amadeus

RELATED DOCUMENTS

The Security Policies and Standards (SPS) comprises the "Global Information Security Policy" (GP), at the top level of the pyramid, detailed by "Policies" (PL) which explain at a high level the objectives of each area. These policies are detailed in "Corporate Standards" (CS) that define the controls to be implemented. In addition, Business Unit Standards (BS) and Technical Standards (TS) may be developed when specification is required, respectively for a business environment/location or for a specific domain of activity (e.g. development, operations, internal IT, etc.). Procedures (PP), with detailed steps to follow for a specific control implementation, may also be created to ensure compliance with the security policies and standards.

DESCRIPTION

This policy covers the use of all information and information processing facilities including any information systems, technical equipment or items owned or leased by Amadeus, regardless of whether they are operated within or outside Amadeus premises.

1.3. Code of conduct

a) Every user shall respect the following general rules concerning:

Adherence to information security policies, standards and procedures: As defined within the Amadeus Security Policies and Standards (SPS) and in the standards & procedures specific for the relevant Business Unit/Domain.

Compliance with legal requirements: As defined in applicable laws, rules and regulations for data protection, protection of Amadeus, its customers, suppliers, and other 3rd parties.

Non-disclosure of business information/data: This rule requires every user to not disclose any business information/data of the company during and after his or her employment/contractual relationship. In addition, the user is not allowed to publish any information that may harm the Amadeus corporate image or brand.

Application and use of implemented security measures: This rule requires every user to apply all implemented security measures. This includes, but is not limited to, the protection, non-disclosure, and the non-sharing of personal badges, personal tokens, personal user-IDs, user and system passwords and encryption keys; to the usage of encryption facilities, virus scanners and screen savers. It is not allowed to damage, bypass or deactivate any implemented security measures.

Use of privileges and access rights: This rule requires each user to use his/her personal unique identifier to access business information/data under Amadeus control.

Use of Amadeus facilities only for business purposes: This rule requires every user to access or use any facility under Amadeus control only for business-related purposes, except where other usage is explicitly permitted.

No use of private equipment: This rule forbids access to information systems and networks under Amadeus control by means of private technical equipment or items, except where other usage is explicitly permitted.

Protection of Amadeus equipment: This rule requires every user to adequately protect all equipment owned by Amadeus under their personal control, e.g. laptops, phones, tablets within or outside company premises. Users are also responsible for backing up of all files, data, applications or any other data stored on their workstations or devices.

Security weaknesses/security incidents reporting: This rule requires every user to promptly report any observed security weakness or security incident by following the incident notification procedure.

No scan of the infrastructure: This rule forbids the scan of the Amadeus infrastructure (network, systems, etc.) by any user (with the exception of duly authorized personnel tasked by Amadeus through their job description that shall be validated by the Information Security Organization).

Use of social and collaboration platforms for business purposes: This rule requires every user to use social networks during their work only to perform business activities.

1.4. Internet Usage

1.4.1. General

Internet access is intended solely for business purposes. Private usage is allowed as long as it does not conflict with your work.

Users will prioritize the safety and reputation of Amadeus whenever using the Internet by means of Amadeus infrastructure. This includes, but is not limited to, complying with all applicable laws and regulations.

1.4.2. User obligations

a) In order to limit the risk to Amadeus, users shall:

- Not access Internet sites or participate in discussions in forums such as Internet user groups that:
    - Contain any kind of illegal or offensive content (e.g. extremist groups (e.g. ISIS), Nazi propaganda, racism, anti-Semitism, child pornography, glorification of violence, etc.).
    - Are inappropriate, disrespectful, or offensive to colleagues' sex, religion or culture or constitute harassment.
    - Violate the company's Corporate Policy.
- Publish Amadeus information on the Internet according to the information classification and handling policy.
- Not publish:
    - Any illegal content (e.g. content related to extremist groups (e.g. ISIS), Nazi sites, racism, anti-Semitism, child pornography, glorification of violence, etc.).
    - Any information which may harm the corporate image of Amadeus.
    - Non-business related information (e.g. pornography, mp3, software, etc.).
- Only access the Internet in a responsible and ethical manner as it relates to security, and legal and business threats.
- Only download content from trusted sources.

1.4.3. Usage of Amadeus Managed & Authorized Browsers

a) Users shall only access the Internet via Amadeus managed and/or authorized web browsers.

A managed browser is a browser deployed & supported by Internal IT[1]. The configuration of such a browser is strictly controlled by Internal IT to ensure that there are no issues with corporate web applications. **A managed browser shall not be altered by the user.**

An authorized web browser is a browser that, although not supported by Internal IT (though causing no additional security risks), is therefore not necessarily tested with corporate web applications.

1.5. Hardware and Software

1.5.1. General

The use of hardware and/or software under Amadeus control shall only be permitted for business purposes except where other usage is allowed.

1.5.2. Use of Amadeus equipment

a) Users shall not change, alter or deactivate the configuration of Amadeus controlled equipment.

This includes, but is not limited to:

- Changing the hardware configuration (e.g. installation of WLAN-adapters).
- Changing, altering or deactivating the configuration of software, tools or parameters which are installed to protect Amadeus IT systems and limit the risk of attacks (e.g. antivirus, patch management, auditing, inventory, etc.).

1.5.3. Hardware and software usage on Amadeus LAN

a) Only Amadeus managed equipment (i.e. purchased by Amadeus, known by Amadeus and centrally managed by Amadeus) shall connect to the Amadeus network, unless explicitly validated by the Information Security Organization. This will help to achieve and maintain an appropriate security level.

b) User shall not use or setup external hosts to access the Amadeus network from the Internet, including the use of tools that provide remote access through unauthorized methods.

Examples of tools that may not be used on Amadeus workstations for remote access include, but are not limited to: GoToMyPC, LogMeIn, PCAnywhere, TeamViewer and Chrome Remote Desktop.

[1]Whether provided centrally, regionally or locally.

c) User shall only install and use Amadeus managed & authorized software. Installation of unauthorized software is prohibited. Specific needs shall be motivated by business justifications and are subject to the prior approval of the Information Security Organization.

Amadeus managed software is defined as software, which is purchased, licensed, centrally registered and supported by Amadeus Internal IT (e.g. MS Office, Adobe Reader).

Amadeus authorized software is defined as software, which is not supported by Internal IT, though explicitly allowed by the Information Security Organization (e.g. certain Freeware, Shareware, Open Source).

Unacceptable use includes, but is not limited to:

- Private software, even if the user has a valid license.
- Freeware or shareware not registered at Amadeus.
- Unauthorized modification or copying of Amadeus managed or authorized software.

d) Users shall comply with all the terms and conditions of the licensing agreement of any third-party software installed.

e) In the case of authorized software, the user shall ensure that he/she is always using the most up-to-date version.

f) In addition, all users shall request access to software or the implementation of new software on his/her workstation/device via his/her normal software request procedure.

1.6. Email use

1.6.1. General

a) Amadeus provides an e-mail system for business purposes only. Private usage is allowed as long as it does not conflict with business needs.

b) User shall send e-mail in accordance with the information classification standard.

c) User shall send report suspicious e-mail *(e.g. via a button for suspicious email in the email system if available)*

1.6.2. Unacceptable usage of the E-mail platform

a) User shall not:

- Share the login and password used to access his/her e-mail account(s).
- Send unsolicited e-mail messages which are not related to Amadeus business, including the sending of ´junk mail` or other advertising material to individuals who did not specifically request such material (e-mail spamming).
- Forge or attempt to forge e-mail messages in order to make people believe that the e-mail was sent by another person.
- Create or forward ´chain letters`, ´Ponzi` or other ´pyramid` schemes of any type.
- Send or forward e-mails containing libelous, defamatory, offensive, racist or obscene remarks. When receiving an e-mail of this nature, supervisors or the Information Security Organization shall promptly be notified.
- Setup "automatic forwarding" to third party e-mail systems.
- Open attachments from uncertain source.

1.7. Clean desk and clean screen

1.7.1. Clean Desk

(1) Confidential Data

a) User shall:

- Store sensitive physical materials *(e.g. printouts, daily planners, notebooks, etc.)* in a lockable storage facility *(e.g. lockable drawer/cabinet)*, especially when away from desk for an extended period of time.
- Not leave portable media such as USB sticks, portable HDD, DVD, Blue-Rays or CDs in drives.
- Never write passwords or PIN codes on a sticky note or hide them anywhere in the office.
- Remove printouts from printers before leaving the office.
- Use secure printing for sensitive documents or ensure to pick up sensitive printouts immediately.
- Shred sensitive printouts when no longer required or dispose of them in locked bins.

b) Confidential documentation shall not be left in open sight when the user leaves his/her desk (even for a short period), to avoid illegitimate people to access to this sensitive information.

(2) Access tools

a) User shall:

- Keep devices with them and lock mobile devices (e.g. smartphones, tablets, etc.) with a pass code.
- Never leave their badge/access cards, keys or token out of sight.
- Notify security staff immediately if badge/access cards, keys or token are stolen or missing.

(3) Spatial configuration

a) User shall:

- Position desks and furniture in such a way that sensitive material is not visible from either the windows or the hallway.
- Close blinds on windows if necessary.
- Erase whiteboards and remove meeting charts.

(4) Beyond desk

a) User shall:

- Avoid using bookshelves to store binders containing sensitive information.
- Keep file cabinets, etc. closed and locked and not leave keys in the locks.
- Lock the office door (if possible) when absent for extended periods.

1.7.2. Clean screen

a) In order to mitigate the risk of exposing sensitive information to unauthorized persons, user shall use a screen filter to minimize the viewing angle on a computer monitor if working in public areas.

b) user shall lock its workstation when not present

1.7.3. Good Samaritan

a) A user noticing that the clean desk or clean screen policy has not been followed shall ensure that no sensitive information is accessible by unauthorized personnel by performing the following actions:

- Collect and safeguard the documents found and encourage the owner to follow the clean desk policy.
- Lock or turn off the workstations/terminals and encourage the owner to follow the clean screen policy.
- If sensitive information is found with the absence of an owner at printers, copiers or faxes, collect and destroy documents.

1.8. Social and collaboration platforms

1.8.1. General

Social media are present in our daily activities, both in the professional and private realm. On the Internet, social engineering for competitive or malicious reasons is increasing (e.g. using various search engines, social networks, social media, collaboration platforms, etc.) to obtain access to sensitive information.

1.8.2. Basic principles on social media & collaboration platforms

a) Users shall complete the security e-learning as soon as employed by Amadeus and, prior to using the social networks and collaboration platforms.

b) Users are responsible for the way they use (confidential) Amadeus information in their social network activities and following the requirements described in this policy.

1.8.3. Usage of social networks and media & collaboration platforms outside of Amadeus

a) Users shall not publish sensitive information about Amadeus (e.g. technical diagrams, user IDs / Office IDs and passwords, internal documentation, etc.) or belonging to Amadeus (see information classification standard).

b) Corporate email accounts shall not be used to register on any social networks, social media or collaboration platforms, unless explicitly authorized by the Information Security Organization.

c) Passwords used within Amadeus shall not be reused on social networks, social media or collaboration platforms.

d) Users shall not automatically synchronize any professional contacts on any social networks, social media or collaboration platforms.

e) Any official presence of Amadeus on social networks, social media or collaboration platforms is reserved to selected and authorized Amadeus personnel.

f) If an end user discovers any sensitive information published in social media, he/she shall report this incident immediately to their local IT helpdesk.

g) Non-public information[2] relating to Amadeus shall only be communicated in social media by authorized personnel using validated channels[3] .

1.9. Amadeus managed mobile devices

1.9.1. General

Amadeus may provide Amadeus managed mobile devices, which can be accessed only by duly authorized personnel tasked with the administration of such devices, as it is already the case for Amadeus managed devices (e.g. workstations, laptop).

a) By accepting such a device, the users implicitly understand and shall comply with the following requirements:

- Amadeus managed mobile devices and all information transmitted by or stored in them (such as emails, voicemail messages, documents and log files) are Amadeus property.
- There are no expectations of privacy with regard to the use of Amadeus managed mobile devices, except in cases where local law sets requirements for privacy of personal data on corporate systems and the user has followed appropriate procedures to identify the information or files as personal.
- Users shall use the received Amadeus managed mobile devices for their professional use. Private usage is allowed as long as it does not conflict with business obligations and needs.
- Users shall not share it and shall not disclose information relating to, obtained or accessed with the mobile device to anyone outside Amadeus.
- Similarly to all devices provided to the users, such as laptops, the user should take all reasonable precautions to protect the Amadeus managed mobile device and the information it contains against damage, loss and theft. For instance, they shall not be left unattended, especially in public areas, such as airport or hotel lounges or plainly visible in cars.
- In case the device is lost, or stolen in spite of these precautions, the user shall immediately report this incident to their regional helpdesk. The Helpdesk may initiate a remote wipe of

[2] See definition of non-public information in "Corporate Standard 4.2: Information Classification & Handling policy".

[3] Relay of information published through validated channel (e.g. Amadeus official LinkedIn page, Amadeus official Facebook page, etc.) is authorized.

the device to prevent the disclosure of Amadeus data and user data still present on the device.

- Sensitive business information shall not be stored on mobile devices, unless the risk of accidental disclosure of information is mitigated by the application of recommended and available security measures described in this policy and adherence to the provisions of this usage policy.
- Protecting Amadeus information and maintaining information security is the responsibility of the individual user. Users shall understand the security requirements within their functional domain and strive to protect any company information with highest priority.

b) In the event of any conflict, the issue shall be resolved in consultation with the Information Security Organization.

1.9.2. Usage & Obligations

(1) IT Support procedures

a) Users shall implement procedures published and required by Amadeus IT support within a reasonable time. For instance, configuration changes or Operating System or application updates. Delays in implementing such procedures may result in the restriction of services.

(2) Security configuration

a) Users shall not disable or disrupt security or management functions configured on the device (e.g. the configured password rules or the Amadeus Mobile Device Management system configuration)**.**

(3) Storage of data & backup

a) Users shall not store Amadeus data on accessories that were not part of the original delivery of the Amadeus managed mobile device by Amadeus to the user (e.g. user-provided memory cards, etc.).

Such accessories may not have adequate technical protection, such as data encryption, that is configured by Amadeus for the Amadeus managed mobile devices.

b) Users shall not store Amadeus data in the Cloud or other services unless the Information Security Organization has explicitly approved the use of such services.

This includes, but is not limited to, file hosting services or web applications accessible over the Internet, such as Dropbox and iCloud.

c) If Cloud storage is a default setting of an application, the user shall not use such options, and shall store Amadeus data locally on its Amadeus managed mobile device or use approved Amadeus services (e.g. "Amadeus Workplace OneDrive").

d) Users shall perform regular backups of Amadeus data and settings contained on their Amadeus managed mobile device using only their professionally assigned Amadeus workstation.

(4) Use of the Amadeus corporate network and services

a) Users shall only access those selected Amadeus systems & services that are designed to be accessed by an Amadeus managed mobile device, but not all. And users shall therefore not try to access them.

For some Amadeus systems not designated to be accessed by Amadeus managed mobile devices, access from mobile devices might be forbidden by policy, even while still technically possible.

(5) Software and App installation

a) Users may install third-party developed software ("Apps") on their Amadeus managed mobile devices on the condition that:

- It is for business purposes only
- It is not prohibited by Amadeus or the Information Security Organization
- The user has the necessary license or copyright (solely the user's responsibility).

b) Amadeus managed devices found not to be compliant with software installation policies shall be treated as compromised and may be remotely wiped.

Users should exercise caution and good judgment when custom-installed applications ask for permission to access:

- Location data or services.
- Contacts.
- Calendars.
- Reminders.
- Photos.
- Bluetooth settings.
- Twitter or Facebook account data.
- Other information not already contained in the application.

Users should consider the potential for malicious use or disclosure of accessed data and grant appropriate access only to trusted applications, for example access to location data to a mapping application.

(6) International Usage

a) Users shall configure their Amadeus mobile devices according to the most up-to-date applicable recommendations for international use provided by the regional helpdesk.

It is the user's responsibility to prevent network or telephone charges that incur as a result of misconfiguration.

(7) Return of equipment

a) Users shall return their mobile device to Amadeus upon request or when leaving Amadeus, and as part of the "return of equipment / leavers process".

The user will return the Amadeus managed mobile device including all accessories such as SIM cards, cables or power adapters, issued to him/her (in case of a leave process, by the official leaving date, and before leaving the Amadeus premises).

b) User shall be aware that Amadeus will dispose of the devices and the data they contain in compliance with legal, procedural and environmental requirements.

1.10. User access

a) User shall protect against unauthorized system access using their account by:

- Keeping their (personal) usernames/passwords secret (i.e. it shall not be written down on paper or stored unencrypted).
- Refraining from disclosing their credentials (e.g. password) on questionnaires, security forms or when asked personally, including helpdesk and support teams (in conversation, over the phone, in e-mails, on questionnaires, etc). If someone demands a password, the user should refer him or her to the Information Security Organization.
- Avoiding use of the same password in different applications with different levels of trust (e.g. the same password should not be the same on an Amadeus system and on the system of a business partner).
- Changing passwords regularly (at least every 90 days), or whenever there is an indication that their password has been compromised, and not reusing old passwords.
- Not using the "remember password" features of applications (especially in the Internet).
- Not using the same password for business and non-business purposes.
- Locking the computer manually when leaving the desk.
- Not use another user's credentials to access company devices or services. If a user suspects his passcode, account or password has been compromised, the user must immediately report the incident to the Service Desk and change the relevant passwords.
- While users may use Amadeus managed mobile devices to access their private e-mail accounts, users shall diligently check settings and content of messages to prevent disclosure of Amadeus information (e.g. not responding to business partner's e-mails from a private e-mail address).

b) In addition, each user shall protect his/her 2nd factor authentication *(e.g. RSA token, secure-ID cards, private keys)* against misuse or fraud.

This includes, but is not limited to, secure handling (shall not be left unattended or shall be kept in a locked cabinet, nor shall it be shared).

c) In case of incident (e.g. theft, loss, etc.) the employee shall immediately notify his local IT contact and escalate it to his Manager.

In case of major cyberattack or threats, Amadeus reserves the right to block access to all or selected web sites.

1.11. Privileged access to workstations

1.11.1. Users' and managers' responsibility

a) Users shall provide a business justification when requesting privileged access to Amadeus managed workstations (local administrative rights), as to why they need such privileges.

b) Managers shall review and approve the privileged access requests based on business justifications.

c) Managers shall also promote and ensure that all users within their teams with privileged access to Amadeus managed workstations have read, reviewed and approved this AUP and have an appropriate business justification.

d) Managers shall request timely removal of privileged access to Amadeus managed workstations when no longer required (e.g. termination or change of employment, contract evolution, change of assignment).

1.11.2. Protection of workstations

a) Users shall not change, alter or deactivate any network and OS configurations provided by Amadeus including, but not limited to local administrator accounts and passwords, domain or group membership, global domain policies and IP settings

b) **When Amadeus managed workstations are shared among several users, the ownership of the workstation is assigned to the Amadeus manager responsible for the service or the group of users. In this case, the Amadeus manager shall request privileged access, review and approve this AUP, and provide business justifications. The Amadeus manager becomes fully responsible for the shared workstations and must implement all appropriate controls to avoid any misuse.**

1.12. Enforcement of rules

1.12.1. Recording, Monitoring and Investigations

a) By having a contract with Amadeus, every user shall acknowledge that events are recorded ('logged') and may be reviewed and audited.

This includes the following aspects:

- Recording: Events are recorded. Every user may be held accountable for all activities carried out under his or her personal user-ID.
- Auditing: Records (logs) are regularly analyzed and evaluated. As far as necessary for proper evaluation, information/data related to the use of resources by individuals may be correlated.
- Investigations: Investigation may include an inspection of any equipment and information/data under Amadeus control. Amadeus is authorized to access and verify any information/data stored or processed by the user on any resource under Amadeus control, in accordance with local law and regulations.

b) User shall be aware that he/she is not permitted to obstruct or undermine investigations or destroy information/data covering any evidence.

c) User shall be aware that, when Amadeus provides Internet access, Amadeus reserves the right to implement and operate 'Web Filter' Software to prevent, record and/or automatically block Internet sites.

d) User shall be aware that, when using an Amadeus software and/or an Amadeus equipment (e.g. workstation, mobile device, server, etc.), Amadeus reserves the right to 'clean' it up.

e) Users of an Amadeus company's e-mail platform shall be aware that Amadeus reserves the right, in accordance with applicable laws and regulations, to:

- Log, trace and archive mails,
- Retain mailboxes after the user leaves the company.

1.12.2. Discipline

a) User shall be aware that any substantial violation of this policy by an individual is taken very seriously and disciplinary action, as appropriate, may be taken in accordance with local laws. Amadeus may also be entitled to claim and pursue any legal action against such employee committing the violation.

b) Managers shall ensure compliance to this AUP and initiate the required disciplinary action in case of violation.

1.13. Exception management

a) Any exception to this Policy shall be granted with the approval of the Information Security organization and based on a business justification.