INFORMATION SECURITY POLICY FOR SUPPLIERS

1. OBJECTIVE

The purpose of this document is to establish information security policies and requirements for service providers, regardless of service type, to protect the confidentiality, integrity and availability of EM&E and its customers' information.

2. SCOPE

The following policy applies to all suppliers who have access to EM&E information and who share, process, store, modify or create new confidential information owned by EM&E or who use EM&E's technology infrastructure. It is designed to protect the confidentiality, integrity and availability of information.

3. GENERAL SECURITY PRINCIPLES FOR SUPPLIERS

3.1. PROVISION OF SERVICES TO EM&E

The activities carried out by the personnel employed by the supplier companies shall be completed in accordance with the provisions of the applicable regulatory contract and the rules and procedures established for this purpose between EM&E and the supplier.
The supplier company shall ensure that all its personnel providing services to EM&E have the appropriate training and qualifications for the development of the contracted service, both at a specific level in matters relating to the activity associated with the provision of the service, and at a general level in the field of information security.
It is understood that any exchange of information between EM&E and the supplier will take place within the framework established by the service provision contract and that such information shall in no case be used outside this framework or for purposes other than those associated with this contract.

3.2. INFORMATION CONFIDENTIALITY

All relationships with service providers who have access to EM&E information are covered by the relevant service contracts and non-disclosure agreements (NDAs).
All information, documentation, programmes and/or applications, methods, business strategies and activities relating to EM&E to which service providers have access for the purpose of performing the service shall by default be considered confidential information. Only EM&E information accessed through the means of public dissemination of information may be considered non-confidential information.
Information to which the supplier has access may only be used for the purposes described in the service contract.
The supplier shall maintain such confidentiality throughout the duration of the service and after termination of the relationship with EM&E.
Failure to comply with these obligations may constitute an offence of disclosure of secrets as provided for in Article 197 of the Criminal Code, which may entitle the supplier to claim damages.
In order to guarantee the security of personal data, the removal of computer media containing such data from EM&E's premises must be authorised by EM&E and shall be carried out in accordance with the defined data protection protocol.

3.3. INTELLECTUAL PROPERTY RIGHTS

Compliance with legal restrictions on the use of material protected by intellectual property rights will be ensured. Service providers may only use material authorised by EM&E in the performance of their work. The use of software in EM&E's information systems without the appropriate licence is strictly prohibited.

Similarly, the use, reproduction, transfer, transformation or public communication of any type of work or invention protected by intellectual property rights without due authorisation is prohibited.

3.4. EXCHANGE OF INFORMATION

Any exchange of information between EM&E and service providers shall be deemed to be within the scope of the relevant service provision contract and such information shall not be used for other purposes.
In relation to the exchange of information within the existing contractual framework between the parties, the following activities are considered to be unauthorised:

- Infringement of copyright law by sending or receiving copyrighted material.
- Transmitting or receiving any kind of pornographic material, messages or communications of a sexual nature, racially discriminatory statements and any other kind of statement or communication that may be considered offensive or unlawful.
- Disclosure of confidential information to unauthorised third parties.
- Sending or receiving files in violation of personal data protection regulations.
- Any activity that may damage the image and reputation of EM&E is prohibited.

Upon termination of the service or upon request by EM&E at any time, the supplier shall immediately cease to use any information provided and shall return all information in his/her possession, regardless of the medium on which it is stored, and destroy any copies made.

3.5. APPROPRIATE USE OF RESOURCES

The resources made available to service providers shall be used exclusively to fulfil the obligations and purposes for which they have been made available. Under no circumstances may they be used for activities unrelated to the purpose of the service or for activities that could be considered illegal. EM&E reserves the right to implement the control mechanisms it deems appropriate to verify the correct use of these resources. Any file introduced into the EM&E network or any device connected to it, whether through automated media, the Internet, electronic mail or any other means, must comply with the requirements set out in this policy and in the organisation's internal regulations.

3.6. USER LIABILITY

Service providers shall ensure that all personnel who perform work for EM&E and who may have access to information systems comply with the following basic principles in their activities:

- Any person with access to EM&E information is responsible for the activity carried out under his or her user ID and all that results from it. It is therefore essential that each person maintains control of the authentication systems associated with their user ID and ensures that the associated password is known only to the user and is not shared with other staff under any circumstances.
- Users shall not use any user identification of another user, even if authorised by the owner.
- Users are aware of and apply existing requirements and procedures concerning the information handled.
- Anyone with access to EM&E information should follow the password policy.
- Anyone with access to EM&E information should ensure that equipment is secured when left unattended.
- Anyone with access to information must adhere to the Clean Desk policy to protect paper documents, computer media and portable storage devices and reduce the risk of unauthorised access, loss and damage to information.
- Authorisation is required for all personnel accessing EM&E information and/or systems.

3.7. SECURITY REQUIREMENTS FOR DEVICES

All devices with access to EM&E information must meet the following considerations:

- Access to systems must always be authenticated, at least by means of a user ID and associated password.
- All devices must be adequately protected against malware. They should be kept up to date with the latest available security updates. Anti-virus software should always be enabled.
- Devices shall be updated with the latest available version of security patches for the software and operating system installed.
- Devices shall not include tools or files that conflict with EM&E's security policy or that may interfere with company software.

3.8. COMMUNICATION OF INCIDENTS

All suppliers must immediately report any incident, vulnerability or threat that may affect the confidentiality, integrity or availability of EM&E information to the IT Department by emailing soporte@eme-es.com or to the person responsible for the contract.

4. SPECIFIC SECURITY PRINCIPLES FOR SUPPLIERS

4.1. PHYSICAL SECURITY

All suppliers who provide services from the premises of the supplier shall ensure that the following physical security measures are complied with:

- Have an access control system to prevent theft, destruction or interruption of service.
- Have automatic detection and response systems in the event of severe environmental conditions, mainly fire.
- If a copy of EM&E information is kept, the systems that store and/or process such information shall be located in a specially protected area.

4.2. SYSTEMS SECURITY

All suppliers whose services are delivered using their ICT infrastructure shall ensure that the following considerations are met:

- Information systems that host or process information under the responsibility of EM&E shall be adequately protected against malicious software. Systems in test, development and production environments shall be updated with the latest available security updates. In addition, anti-virus software shall always be enabled.
- The supplier shall establish a backup policy to ensure the protection of any data or information relevant to the service provided.
- In relation to the use of electronic mail, the transmission of EM&E confidential information is not permitted unless the electronic communication is encrypted and the sending is expressly authorised.
- Access to information systems hosting or processing EM&E information shall always be authenticated, at least by the use of a unique user ID and associated password.
- The provisions of section Safety requirements for devices shall be complied with.

4.3. NETWORK SECURITY

All suppliers whose services are provided through the use of their ICT infrastructure shall ensure that the following network security measures are complied with:

- All networks over which information flows shall be properly managed and controlled to ensure that there are no uncontrolled accesses or connections whose risks are not properly managed.

- Services available on networks over which information flows should be limited as much as possible.
- Networks allowing access to EM&E's ICT infrastructure should be appropriately secured.

4.4. CHANGE MANAGEMENT

All providers of services involving access to EM&E information systems shall ensure that the following considerations are met:

- All changes to the ICT infrastructure used to deliver the service are controlled and authorised to ensure that no uncontrolled components are included.
- All changes must be made in accordance with a formally established and documented procedure.

5. POLICY UPDATE

Due to evolving technology, security threats and new legal requirements, EM&E reserves the right to amend this policy as it deems necessary. Any changes made will be communicated to all service providers to whom it applies by any means deemed appropriate. It is the responsibility of each company to ensure that

Alcalá de Henares, October 10, 2022

Ángel Escribano Ruiz
President