Prepared (Subject resp) Marco Baffi (ISMS Responsible)		No. MSA_ISMS_CODE_CONDUCT		
Approved (Document resp) Giovanni Campus (General Manager)	Checked Yes	Date 20190301	Version/Status 2.0/released	Reference MSA_ISMS_ CODE_CONDUCT

Classified as: PUBLIC

Information Security Management System

(ISMS)

Code of Conduct

Version	Changelog
1.0	First release
2.0	Second release

Contents

1 Normative Reference

Ref	Description
[1]	ISO/IEC 27001:2017 Information Technology – Security Techniques Information Security Management Systems - Requirements;
[2]	ISO/IEC 27002: 2017 Information Technology – Security Techniques - Code of practice for information security controls
[3]	ISO/IEC 27000: 2014 Information Technology – Security Techniques - Overview and vocabulary

2 References

Reference	Description
MSA – ISMS Information Security Policy	MSA-Multi Serass approved policy on information security

3 Introduction

3.1 Scope and objectives

MSA - Multi Serass s.r.l. (MSA) defines its Code of Conduct to state the employee's and contractor's information security responsibilities in accordance with the establishment of an Information Security Management System (ISMS), addressed by ISO 27001:2017 regulation. This Code of Conduct is compliant with MSA – ISMS Information Security Policy.

The objective of this document is to define a standard user behavioural model in order to guarantee a proper security level of information and systems, to protect MSA from losses due to malware exposure, improper use of systems and activities that can cause damages.

IT resources (technological – hardware and software – and infrastructural) provide services and store fundamental information for MSA's business activities.

This document provides operative and behavioral rules for those who use MSA's resources in the ISMS Scope with the aim of ensure performances and a secure use of facilities and services. Rules and directives addressed in this document apply both to resources assigned to a specific user and shared.

The strict application of these rules allows to operate in compliance with MSA's classification and management of information, MSA's access control policy and the regulation on the protection of personal data.

The following document addresses rules and proper behaviour employees and contractors must follow to fulfil their information security responsibilities.

4 Resources

Resources can be assigned to a specific user or shared, hardware or software, infrastructural. The following resources are addressed in this document:

- Physical Assets
  - Cabinets and drawers
  - Archives
- Network Infrastructure
  - Logical
  - Physical
- Assigned hardware resources
  - Workstations (It includes: PC or laptop, mouse, monitor, printer, scanner, telephone)
- Assigned software resources
  - Licensed and pre-installed software on workstation
- Shared IT resources
  - Servers
  - Network printers

5 General principles

In respect of privacy regulation, MSA informs employees that all data created, transmitted, received or archived using MSA's systems are under the propriety of MSA and can be monitored, reviewed, used or published when needed. These data can't be disclosed or transferred without MSA's management authorization.

Employees are accountable for the use of MSA's resources, as detailed in this document. Any action needed for MSA's operativity that is not addressed in this code, must be authorized from the management.

For security purposes, IT responsible is authorized to check servers and workstations.

Periodical checks can be performed to verify the proper application of this document.

Each user is assigned or authorized to use a workstation, connected to the network; access allowed by using the credentials provided. He needs to take care of the tools provided and is responsible for the correct use of the IT resources assigned or authorized to him.

Workstations can be used only for legal use, in respect of company regulation and applicable laws. Use of workstation is forbidden:

- in a way that can damage IT system;
- to cause damage to other users;
- to gain profit;
- to scan/monitor system's activities or network;
- to spam;
- to access ethic or morality harmful contents.

In the following paragraphs ,rules and proper behaviour directives on the use of the MSA's resources are detailed.

6 Code of Conduct

MSA bases its policy on the principles of efficacy and efficiency, ensuring the transparency of operational processes, working on the empowerment of its employees, with the aim of simplify procedures, guarantee an easy access for customers and suppliers, in respect of information security.

6.1 Management responsibilities

MSA management requires all employees and contractors to apply information security in accordance with the defined policies and procedures.

Employees and contractors who access MSA information must comply with MSA information security requirements; in particular they must be aware of their roles and responsibilities, in order to ensure confidentiality and protection of information and to comply with MSA's principles as addressed in the Ethical code.

6.2 Physical Security

Access to MSA's offices is controlled to prevent unauthorized accesses.
Access is allowed in the time slots detailed in the tables below; any other access must be authorized.

Milan	In-site and off-site employees	Monday/Friday from 7:00 to 21:00 (Saturday from 08:00 to 14:00)
	Guests (visitors and consultants)	Monday/Friday from 7:00 to 21:00 (Saturday from 08:00 to 14:00)

Trento, Moncalieri (TO), Roma, Parigi	In-site and off-site employees	Monday/Friday from 8:00 to 20:00
	Guests (visitors and consultants)	Monday/Friday from 8:00 to 20:00

6.3 Disciplinary regulation

Users must be aligned with MSA's security objectives and need to know and comply with the security rules. Users must safeguard the security of information handled by managing the assigned resources in a proper way and according to the defined security objectives.

Users are required to not disclose information to third parties. All users are required to comply with national legislation on the protection of personal data (L.D. 196/2003, GDPR).

All users are required to promptly report to their manager, the Department, any event significant for safety purposes detected during their work.

When creating the account for access to Information Systems, the user is informed, also through this document, of the rules relating to the correct creation and management of passwords and the correct use of their credentials. Therefore, the user needs to know that:

- failure to comply with the above rules will result in disciplinary action;
- in the presence of malicious actions, negligent behaviour, acts or omissions, reference will be made to what is already provided for and sanctioned by the National Collective Labour Agreement, except for any criminal implication.

6.4 Acceptable use of assets

Information, assets and processing facilities are provided for use to seek MSA's mission. Use of these facilities for personal activities is not permitted. Each subject is responsible for the appropriate use of the MSA resources assigned to him/her. Any use that is not inherent to the work activity can contribute to trigger inefficiencies, maintenance costs and, above all, threats to security. MSA resources may not be used for any unlawful or prohibited purpose.

Any information must be handled in accordance with its criticality level. Special attention must be payed when handling internal and confidential information whose unauthorized diffusion could damage the organization.
Paper documentation classified as Internal, Confidential or Secret, must be placed in locked cabinets or drawers at the end of working day or when left unattended. The disposal of this kind of information should be performed with shredders.

The use of personal storage removable devices such as USBs and SDs is forbidden except when strictly needed, upon authorization and antivirus check.

Theft, damage or loss of assets assigned to employees must be promptly reported to the company.

6.5 Unattended user equipment

Users must ensure protection when leaving unattended equipment. In particular user should:

- Terminate active sessions and/or secure equipment with password, when terminate activity;
- Log-off from application, when no longer needed;
- Log-off from network services, when no longer needed;
- Secure devices (PCs, mobile devices,…) with passwords or any other security mechanism in order to prevent unauthorized uses.

6.6 Clear desk and clear screen policy

MSA develops this policy tacking into account its information classification, the legal and contractual requirements, and in order to protect information from unauthorized accesses, loss or damages.

1. Employees are required to ensure that all sensitive/confidential information in paper or electronic format is secure in their work area at the end of the day and when they are expected to be gone for an extended period;
2. Computer workstations must be locked when workspace is unoccupied;
3. Computer workstations must be shut down at the end of the work day;
4. Any sensitive or confidential information must be removed from desks and locked in cabinets, when workspace is unoccupied;
5. Keys used to access cabinet containing sensitive/confidential information must not be left at an unattended desk;
6. Printouts containing sensitive/confidential information should be immediately removed from printers;
7. Laptops must be either locked with a locking cable or locked away in a drawer;
8. Upon disposal sensitive/confidential documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins

6.7 Working off-site

It is accepted that laptops and mobile devices are taken off-site. The following controls must be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car;
- Laptops must be carried as hand luggage when travelling;
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN.

6.8 Authentication and use of secret authentication information

Each user is provided with an account to access MSA's infrastructure. This account will be deleted in case of termination of work. The account is composed by:

- Identification code (ID)
- Password

Account credentials are provided by IT department. Account privileges are assigned based on user's role.

Account credentials are personal and not-transferable. Passwords are strictly personals; to guarantee their confidentiality, the following directives must be followed:

- Passwords must be kept with care;
- Passwords must not be communicated to others.

Passwords must not be written on easily accessible media (post-it, clipboard, etc.) and must be changed frequently, especially when their confidentiality is considered undermined.

When choosing password, the following rules must be followed:

- Use a password compliant with MSA's Password Policy;
- Don't use the ID as password;
- Don't use any information that is simple to retrieve (name, surname, date of birth, telephone number etc..);
- Don't use simple dictionary word;
- Don't insert password when other people could see it.

6.9 Restrictions on software installation

Software installed on company equipment is only for professional use.
Self-software installation is not permitted; any software installation must be authorized and performed by IT department. To verify this, MSA puts in place specific controls mechanisms.

In any case, in order to prevent such installations that can introduce vulnerabilities in the information systems, the most part of the users have a limited set of privileges regarding systems customization.

The following rules apply to all MSA's employees:

- Employees can't download software from the Internet or bring software from home without authorization.
- When an employee detects the need for use of a particular software, a request needs to be transmitted to the IT department.
- The IT department shall determine if the organization has license of the software requested.

- If there is license, the IT department notifies the employee and will proceed to install the software on the computer of the user who requested it.
- If there is no license, a responsible party must assess whether the requested software is really necessary.
- Top management should participate in the decision on the acquisition of new software.
- Once the decision has been made, the IT department will proceed to include the software in their inventory and will install the software.

6.10 Protection of Intellectual Property Rights

All staff and all third parties under contract to us are required to comply with laws on intellectual property rights and legal use of software and information product.

6.11 Security of network services

The use of network and network services must comply with MSA security requirements. MSA protects its infrastructure with a set of technical measures that include use of firewall, VPNs and internal network segregation. Network service levels are addressed in the agreements with network providers.

The following rules apply to any subject who use or manage MSA’s networks:

- Any device connected to MSA network is a corporate tool necessary for the performance of one's work activity;
- Access to the company network is protected; access must be based on your personal profile;
- It’s forbidden to use company network for purposes not expressly authorised;
- It’s forbidden to monitor network if not specifically authorized;
- It’s forbidden to use Internet for reasons other than those strictly linked to the work activity itself;
- It’s forbidden to provide network access to non-authorized personnel;
- Create or transmit defamatory contents is not allowed;
- It’s forbidden to use company network for unlawful purposes (transmission or storage of contents under copyright, pornographic material, defamatory messages etc…);
- Registration to websites whose contents are not linked to work activity with company accounts is not allowed;
- It’s not allowed to join groups like forums
- Don’t use network to join forums and/or newsgroup not linked to work activities;
- It’s forbidden any activity that can damage, destroy or try to access without authorization to others’ data;
- Each user must preserve the confidentiality of other users (it’s forbidden to intercept or to disseminate confidential information);
- Download of contents not related to working activity is not allowed.

6.12 Electronic messaging

A company email is provided for each new employee. This email must only be used for business purposes.
MSA implemented technical measures to protect use and content of the emails. Anyway, users must pay attention when using this kind of electronic communication. In particular:

- Email from unknown senders or unusual messages must be handled with care;
- Suspicious attachments (e.g. file wit .exe extension) must not be opened;
- When sending heavy attachments, the use of compressed format (*.zip file) is suggested;

- Documentation sent outside MSA should be protected using non-modifiable format (*.pdf);
- Mailboxes must be kept in order, deleting unnecessary documents and, above all, bulky attachments.
- Don’t use company email for personal registration on forums and/or newsgroup;
- Don’t use company email to join chain letters or other kinds of spam;
- Don’t send or store messages that insult and/or discriminate sex, language, religion, race, ethnic origin, opinion and union and/or political membership;
- Don’t use company email for unlawful purposes (contents under copyright, pornographic material, defamatory messages etc…).

MSA advises employees to take care of the password used to access company mail and to not communicate it to others.