SCM Group SpA

IT Security Policy

SUMMARY

1. SCOPE AND OBJECTIVES

This policy provides guidance to all SCM Group personnel and any third parties on their responsibilities regarding the management and use of IT resources and responsibility for their ownership. Furthermore, this policy provides guidance on identity management, the security of IT and network systems, the controls of IT structures and the maintenance of the level of security in the process of evolution of the systems themselves. This policy has three objectives:

- **Confidentiality** – Protection against unauthorized access, theft or disclosure of SCM Group information, whether accidental or intentional.
- **Integrity** – Safeguards against unauthorized modification, destruction, or creation of electronic information or communications.
- **Availability** – Protection to ensure service is not denied to authorized users.

2. TERMS AND DEFINITIONS

All terms and definitions are contained in the body of the policy itself when necessary.

3. INTRODUCTION

This IT Security policy applies to all SCM Group stake holders in the use of SCM Group data, systems and IT infrastructures.

The protection of the information produced by SCM Group and the systems supporting SCM Group operations is the responsibility of all SCM Group stakeholders. The systems supporting SCM Group's operations and the data processed, stored or transmitted on them are assets of vital importance for SCM Group. SCM Group's policy is to take all reasonable and appropriate measures necessary to identify and protect all forms of non-public information originating or owned by the company or entrusted to it by others. Furthermore, all reasonable and appropriate measures necessary to protect the computer systems that support SCM Group's operations and the data processed, stored or transmitted on such systems must be taken.

The protection of electronic communications in support of SCM Group operations is the responsibility of all SCM Group stakeholders. Electronic communications using SCM Group communication tools are the property of SCM Group. SCM Group's IT security policy provides for the adoption of all reasonable and appropriate measures necessary to protect data processed, stored or transmitted electronically in support of SCM Group's operations. The content of electronic messages must not be monitored unless warranted by operational, maintenance, control, security or investigative requirements.

All stakeholders accessing the systems that support SCM Group operations must be identified, authenticated and authorized before access is granted. It is the responsibility of all SCM Group stakeholders to ensure that this occurs as defined in the following policy.

REFERENCES

Policy Sponsor: IT Security Committee

Effective date: January 2023

Version number: 1.0

POLICY REVIEW AND UPDATE PROCESS

The IT Security Committee must annually review SCM Group's IT Security policy for potential changes and will publish approved updates.

4. INTERNAL ORGANIZATION OF IT SECURITY

ROLES

The IT Security Committee has responsibility for the overall security and compliance program and is composed of the Director of Systems (group information technology director) and the IT security manager (IT Infrastructure & Security Manager). It is governed by the Company Management Committee whose members are the CEO, general manager, group human resources and organization director, group chief financial officer , group information technology director , group communications director and the various division directors.

IT Infrastructure & Security team has overall responsibility for the implementation and ongoing support of security and event monitoring, patch management, incident response and user provisioning . This group works closely with the rest of the IT organization to execute the operational part.

RESPONSIBILITY FOR ENFORCEMENT OF THE POLICY

Managers and Directors are responsible for:

- Communicate and ensure compliance with this policy and support the guidelines.
- Provide guidance and decisions regarding granting and removing access to SCM Group information and systems.

All SCM Group stakeholders (i.e. employees, service providers, suppliers, contractors, consultants, business, channel and joint venture partners, subsidiaries and affiliates) who generate, possess, control information or use information technology equipment covered by the this policy are responsible for protecting them in accordance with this policy and supporting guidelines.

5. ASSET MANAGEMENT

DELIVERY AND RETURN OF ASSET

When hiring an employee who requires an electronic device (asset) that accesses company data processed by the SCM Group, the company IT department assigns the asset to the employee, recording its delivery as well as the employee's identification data.

Likewise, upon termination of the employment relationship, the employee who had the asset must return it, after verification and issuing a declaration of absence in the asset of personal data even if involuntarily stored although prohibited, relieving the company from any liability in case of accidental treatment of the same. The IT department will record the return and verify the operating and conservation status of the asset .

ASSET LIABILITY

Company management is responsible for the security of SCM Group devices, however, this responsibility is further delegated to managers, managers, employees and contractors who are entrusted with the custody of these systems.

THEFT AND LOSS OF ASSET

In the event of theft or loss of a company information work tool, the worker/collaborator to whom it was delivered is required to promptly notify the IT department of the incident so that the latter can, within the limits of its possibilities, block any access to the information contained therein. In the event of theft, the employee must also immediately report it to the competent authorities.

A similar report must be made by the worker/collaborator in the event of theft or loss of data on any medium (e.g. in the case of theft and/or loss of external USB disks or USB sticks whose use has been previously authorised; loss of paper documents etc.)

PROPERTIES OF THE SOFTWARE DEVELOPED FOR SCM GROUP

All computer software developed by employees, contract personnel or vendors on behalf of SCM Group is the property of SCM Group and may not be distributed outside of SCM Group without specific authorization. IT resources under development must be considered the property of SCM Group and must be protected.

COMPLIANCE WITH LICENSE/COPYRIGHT AGREEMENTS

All developers must comply with third-party software license agreements and copyright laws. Third-party software products may be distributed internally only in accordance with their respective license agreements.

PERMITTED USES

SCM Group provides systems, services and structures to conduct business activities. All employees are required to respect the values that represent SCM Group in their use.

Inappropriate, unethical or abusive use of SCM Group structures or systems by any user will not be tolerated and will be reported to HR and Managers to evaluate any disciplinary actions.

Examples of inappropriate employee use include, but are not limited to:

- Downloading or installing commercial software in violation of its license agreements
- Using any software or electronic file downloaded from the Internet without virus scanning for detection of possible threats, virus scanning is automatically performed on equipment configured as per SCM Group standards.
- Removal or compromise of any standard corporate security component (e.g. Antivirus, etc.).
- Intentionally interfering with the normal functioning of any communications infrastructure (internet, LAN, etc).
- Use SCM Group systems to support political or religious beliefs
- Sending offensive, slanderous or harmful messages to the company or to SCM Group employees.
- Accessing or downloading pornographic material
- Excessive use of the Internet for personal use (e.g. Video Streaming, etc).
- Carrying out illegal activities, including gambling

PERSONAL TOOLS FOR WORK USE

It is forbidden to use personal tools (for example: PCs, tablets and smartphones) to process company data. Should such use become necessary, a written request must be made to the System Manager/Administrator who will evaluate the real need on a case-by-case basis and suggest technical measures to be adopted on such authorized devices. In any case, the data - specifically identified - must remain on such personal devices for a specific time and, in any case, no longer than the time necessary for their use.

Each employee is assigned a workstation, through which all work activities can be carried out. However, it is also possible to use other stations if necessary, logging in with the assigned authentication credentials.

It is forbidden to save personal documents or documents containing data relating to relatives, friends or acquaintances on the company PC.

In the case of remote access to the data contained in the systems, maximum attention must be paid to ensure that copies are not saved on personal PCs which must, in any case, be deleted and also eliminated from the "recycle bin".

Furthermore, the electronic devices that access must necessarily be equipped with active and updated protection systems (such as access passwords, antivirus) for the entire duration of the connection.

6. PHYSICAL AND ENVIRONMENTAL SAFETY

6.1 SAFE AREAS

IT STRUCTURES

CONTROL OF ACCESS TO COMPUTER STRUCTURES

Access to facilities dedicated to IT processing (e.g. data centers and server rooms) must be physically limited. Authorizations to access IT facilities must be granted to those who have legitimate business responsibilities within the facility and who have a frequent need to access the aforementioned areas. The relevant IT manager must approve all access requests. Where possible, electronic access control systems should be implemented to prevent unauthorized access. The system must record all receipts and must be able to produce a report if required.

The access cards or badges of authorized personnel who no longer require access must be collected before they leave the company.

VISITORS CONTROL

Personnel who do not require continuous access to the IT facilities ("visitors") must be escorted by an authorized person.

PLANNING OF MAINTENANCE ACTIVITIES

Maintenance activities must be scheduled only with the prior knowledge and consent of the IT manager of the specific IT structure.

6 .2 EQUIPMENT SAFETY

SECURITY OF TELECOMMUNICATIONS, NETWORKS AND SERVERS EQUIPMENT

All telecommunications, networking and server equipment must be located in a secure facility. If possible, it should be hosted in a dedicated server room or data center. If this is not possible, such equipment must be kept in locked rooms. They must not be located in office areas.

HANDLING OF EQUIPMENT OFF SITE

Unauthorized removal of company computers will be considered theft. Non-portable computers may be removed from company premises only in the presence of specific authorization from the headquarters management and the IT manager for that location.

- **Portable device security:** Logical access controls should be implemented so that unauthorized users cannot access information stored on the device. Portable devices should not be left unattended or unsecured
- **Use of Encryption:** File or disk encryption should be used on laptop computers to protect SCM Group's confidential or sensitive information in the event of equipment theft.

7. INSTALLATION, CONFIGURATION AND UPDATE OF COMPUTER SYSTEMS

7.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES

ACCEPTANCE OF THE SOFTWARE

System security features should be reviewed with the system owner or vendor prior to installation and use of the system. Before actual use, the system administrator must carry out all security checks. User access for production purposes should not be allowed until security settings are fully up and running.

CONFIGURATION UPDATE MANAGEMENT

USE OF FORMAL PROCEDURES FOR CHANGE CONTROL

All systems used for SCM Group production processing must use the " *4SCM - Change Management Procedure" procedure* to regulate the activities necessary to correctly manage the software life cycle.

Program updates should not be downloaded from the Internet, from unverified sources, directly to a production server. All downloaded software must be scanned for viruses, examined for authenticity, and thoroughly tested before being put into production (updates from trusted vendors, such as virus definitions and signature updates, are exempt from this requirement).

SEGREGATION OF DUTIES IN THE USE, DEVELOPMENT AND ADMINISTRATION OF THE SYSTEM

The management or execution of certain tasks or areas of responsibility must be separated to the extent that the risk of unauthorized modification or misuse of data/services is acceptable.

Critical Functions to Segregate: The following functions should not be performed by the same employees in a production environment:

- Enterprise System Usage: A typical user performing normal business operations
- Data Entry: A user dedicated to mass data entry
- IT Operations: A technical user who manages daily operational tasks and may have high access to the system
- Network Management: A technical user who manages network devices and may have high access to network devices
- System Administration: Technical user who installs and manages operating systems and has high access to the system
- System Maintenance: A technical user who is responsible for maintaining the hardware and may have high access to the system
- Change Management: A technical user who is responsible for migrating changes to production and who may have high access to the system

In general, people with access rights to implement or migrate changes to production systems should be separated from people with responsibilities for developing and using the systems.

7.2 MANAGEMENT OF THE PROVISION OF THIRD PARTY SERVICES

HOSTED ENVIRONMENTS

Shared hosting providers must protect SCM Group's hosted environment and data by ensuring that only authorized individuals have access to SCM Group's environment; ensuring logging and audits are enabled and unique to SCM Group's environment and consistent with all relevant regulatory or industry requirements. They must also enable the

provision of timely forensic investigations in the event of a compromise to the environment or data of SCM Group or any other entity.

Resource usage must be monitored and projections made about future capacity requirements to ensure the required operation and performance of the system.

7.3 PROTECTION AGAINST MALICIOUS SOFTWARE/CODE

VIRUS PROTECTION SOFTWARE

To timely detect and prevent the spread of computer viruses, all SCM Group workstations, servers, portable computers, laptops and notebooks must be configured to automatically load and run virus detection software, where applicable. Only standard, management-approved antivirus protection products obtained from authorized vendors will be installed on systems.

CREATION OR INTRODUCTION OF MALICIOUS SOFTWARE

Users must not create or introduce malicious software onto any SCM Group system.

7.4 BACKUP

Computer data should always be saved in areas of company systems that are backed up. If you do not know these areas in the information system, you should contact the company IT department or the System Administrator.

All systems used for SCM Group production processing must use the " *3SCM - Backup Procedure* " procedure where the processes and methods adopted by SCM Group SpA for carrying out system backup and restore activities are described.

7.5 NETWORK SECURITY MANAGEMENT

CONFIDENTIALITY OF NETWORK ADDRESSES

Information relating to internal addresses, configurations and related designs of SCM Group networks and systems must be protected in order to maintain confidentiality and consequent integrity.

BLOCK OF NON-ESSENTIAL NETWORK SERVICES

All non-essential network or system services should be blocked and removed from production environments.

7.6 EXCHANGE OF INFORMATION

USE OF ELECTRONIC MAIL

The employee may be assigned one or more email addresses. These must all be used exclusively for work purposes, since - if necessary - the Company (owner of the domain and, in any case, data controller) will be able to access them, in compliance with legal requirements, even in the absence of the employee or the termination of the employment relationship.

The use of e-mail must take place in compliance with this regulation and the following principles and rules:

a) The email boxes provided by the Company are made available to employees for exclusively work purposes and are therefore to be considered, for all intents and purposes, intangible assets of the company and work tools also pursuant to art. 4 of the law. 300/1970.

email attachment files before using them (do not download executable files or documents from unknown websites or FTP servers).

c) It is necessary to pay due attention to the content of outgoing emails as, through them, the User represents the Company towards the recipients.

d) It is necessary to keep the email inbox tidy, deleting useless documents and bulky attachments;

e) It is necessary to archive the documents received and the information contained in the emails according to company rules.

f) Access to personal email inboxes is permitted exclusively via browser (e.g. Google Chrome , Microsoft Edge) without saving documents or files of any nature on the company information system and during breaks.

g) It is forbidden to use the assigned electronic mailbox: (i) to send personal messages; (ii) for sending messages and unrelated to the employment relationship or working relationships between colleagues; (iii) to send and download attachments containing videos/musical tracks that are not functional to the work activity; (iv) for participation in debates, forums, mailing lists; (v) for any other purpose not connected to work performance.

email file attachments if the sender is unknown or the relevance of the communication to work is doubtful.

i) The use of email software (for example Outlook, etc.) and the transit of any personal file on company emails and IT work tools or on the company information system in general as well as any transit of company emails or data is prohibited. on personal mail (it is therefore prohibited, by way of example and without limitation, to send or download attachments, forward - individually or automatically - work emails to private addresses and vice versa, etc.). In cases of proven emergency, it will be possible to use personal email addresses even during working hours, taking care to communicate the circumstance to the System Manager/Administrator.

j) In the event of prolonged absence, the user of the company email account must directly set up an automatic response notice which warns of his/her unavailability and, if necessary, indicates another alternative address to which emails should be sent.

The information relating to access to the various company mailboxes, such as the location of the IP address of the user accessing the email service, as well as the date and time of access, are recorded for reasons of security of the IT system and the data processed therein. The above information can be consulted by the System Administrator. The data (header and body of the email) may also be present in backup copies managed directly by the email service provider. The supplier guarantees the compliance of its email system with European regulatory requirements, in particular it has opted for the information conservation function within the EU territory.

Some email addresses, particularly non-personal ones, may be shared between multiple parties. In this case each user must scrupulously comply with the rules established by this procedure.

In case of necessity, for example due to temporary absence - even unplanned - of an employee/consultant if the same has not activated the automatic response function and upon written request from an Office manager and with authorization from the Management and also upon communication to the interested user, the Company, through the System Manager/Administrator, may activate this functionality and redirect the emails to another email address. In this case the password will be deleted and a new one will be entered. Changing the password by the System Manager/Administrator is a guarantee for the user that authorized access has been carried out by a third party.

The Company will be able to access the company email in the event of the employee's absence or at the end of the employment relationship, if circumstances arise that make this necessary to safeguard the company's interests (for example: in case of urgency requiring to guarantee operational continuity; for proven organizational and production needs; for the safety of the workplace and for the protection of company assets, including IT assets; to verify the integrity and security of the systems; to the company IT system, data and programs; violation of material subject to the Company's intellectual property rights; in the event of serious suspicion of the commission of possible crimes, including criminal/administrative ones, to the detriment of the Company or third parties) .

Access to the email inbox will take place in compliance with the principles established by law, however, according to: the principle of proportionality (access and control will take place for the time necessary to pursue the above purposes); the principle of transparency (this Regulation in fact has the objective of informing employees about the rights and duties of the parties); the principle of relevance and non-excess (modalities that guarantee security and confidentiality for the interested party will be used, and the control will not have a constant and indiscriminate nature).

Upon termination of the employment relationship, the company email account assigned to the worker will be denied access on the same day and deactivated within 15 working days.

After the termination of the employment/collaboration relationship, the content of the email and the related data will be retained for a period of 6 months. For e-mail messages with legal and commercial content and relevance, storage will take place in compliance with the terms established by law. To protect its rights in court in the event of ongoing disputes or pre-disputes, the Company may retain e-mail messages for a period longer than those indicated above and until the aforementioned legitimate interest persists.

METHOD OF TRANSFER OF COMPANY DOCUMENTS

The use of removable devices (for example, external USB disks or USB sticks) or even cloud spaces not provided by the company in which to transfer company data, even temporarily, is absolutely prohibited. If, exceptionally, such devices are used, the employee will be considered, for all intents and purposes, custodian of the same and of the data contained therein and will be responsible accordingly also from a disciplinary point of view.

Any protected documents and/or information, with respect to which the Company is bound by specific agreements (so-called NDA, Non- Disclosure Agreement) cannot under any circumstances be saved on mobile devices, unless this is expressly authorized in writing by your manager. The IT Department will indicate the data protection methods

7.7 MONITORING

All systems that process, transmit or store SCM Group information must generate LOGs. Procedures must be implemented to monitor system usage on a regular basis to ensure that users only perform processes that have been explicitly authorized by them. The record must be in the form of a chronological record of activities that permits reconstruction, review and examination of any chosen sequence of activities.

LOGGING

ACTIVITIES TO BE LOGGED

The activities to be recorded must include, but are not limited to, relevant attributes (user, date/time, resources, etc.) of the following:

- Activities performed
- Denied connections and rejected attempts
- Access successes and failures
- Error messages and warnings
- Account creation and modification activities
- Assignment and use of accounts with privileged access capabilities
- Other IT security administration tasks

USE OF TOOLS FOR LOG COLLECTION

Logs must be forwarded to a central logging system (SIEM) to ensure data integrity and facilitate monitoring and alerts. The logs of system administrators (AdS) must be maintained and not modifiable as requested by the data controllers carried out with electronic tools in relation to the attribution of system administrator functions in 2008 by the Guarantor for the protection of personal data (D . legislative decree 196/2003).

MINIMUM STORAGE REQUIREMENTS

Logs must be kept for **one year** .

LOG DATA PROTECTION

The Logs must be treated as confidential data of SCM Group and cannot be modified or deleted by anyone during the retention period.

SECURITY MONITORING MANAGEMENT

PURPOSE OF MONITORING

Critical systems and networks and their activities must be monitored to ensure compliance with all IT security policies and guidelines.

USE OF TOOLS FOR LOG COLLECTION

Automated tools should be used on an ongoing basis to facilitate review of Log data (e.g. firewall, Internet Browsing, etc.)

PERIODIC VERIFICATION OF THE INTEGRITY OF THE FIREWALLS

The integrity of all firewall systems must be verified in real time using the latest methods and techniques.

MONITORING OF THE USE OF THE SYSTEMS

Procedures for monitoring system use must be established to ensure that users only perform processes that have been explicitly authorized. The level of monitoring required for individual systems should be determined based on the sensitivity of the data handled by the system. The implementation of security policies and guidelines within the distributed environment must be monitored centrally. The areas to consider are:

- Attempts and failures to access the operating system and applications
- Monitoring of selected critical transactions
- The use of company resources
- Firewall activity
- IT security administration activities
- WWW pages visited
- FTP sessions (where permitted)
- SSH sessions
- Sudo activity
- Remote access by suppliers for maintenance or diagnostics
- Remote access via VPN

REAL TIME SECURITY MONITORING

Intrusion detection systems should be used for incoming Internet connections to detect attack attempts by performing real-time analysis of network traffic. The same detection is also required on third-party connections.

RIGHT TO MONITORING AND CONTROL

Users should have no expectation of privacy when using SCM Group electronic communications systems. At any time and without prior notice, SCM Group management reserves the right to examine information stored on SCM Group systems (e.g. e-mail messages, personal file lists) and may also disclose such data to law enforcement agencies .

SCM Group policy does NOT include monitoring of electronic messages unless warranted by operational, maintenance, audit, security or investigative requirements. Unless specifically authorized by management, interception or disclosure of electronic communications is prohibited.

FALSE IDENTITY AND ANONYMITY

SCM Group users must not, directly or implicitly, use a false identity (the name or electronic identification of another). A user of SCM Group may use a pseudonym (an alternative name or electronic identification for himself) for privacy or other reasons, provided that the pseudonym does not clearly constitute a false identity.

8. ACCESS CONTROL

8.1 CORPORATE REQUIREMENTS FOR ACCESS CONTROL

KNOW" PRINCIPLE

To reduce the risk of compromise or negative operational impact, access to SCM Group information is based on the " Need -to-Know" principle. Access should be limited to the information a person needs to fulfill assigned responsibilities.

ACCESS FROM EXTERNAL NETWORKS

All systems and applications must implement strong authentication (MFA) and encryption where possible for all non-public access from an external network, including the Internet. Any system or application exposed to the Internet that hosts or provides access to SCM Group information must run an appropriately secured operating system.

SCM GROUP'S RIGHT TO REVIEW IT SECURITY CONTROLS

SCM Group, in its discretion, shall have the right to review a third party's security controls to determine whether they are adequate to protect SCM Group's creative assets and may, in its discretion, directly enhance such security controls to prevent access harmful or inappropriate to SCM Group systems.

MINIMIZE RISKS FROM VIRUSES AND DATA CORRUPTIONS BY THIRD PARTIES

Third parties accessing SCM Group systems must agree to make every reasonable effort to scan any material intended for electronic transmission in any electronic format (e.g., email, file transfer, flash drive, etc.) for viruses and/or other malicious computer programs before its transfer to SCM Group.

EXTRANET OR INTERNET ACCESS CONTROL

Extranet or internet connections must be protected by an approved firewall device that limits access to only necessary components such as web servers, email systems or others down to the IP address and port level. Additionally, application gateways should be provided where technically feasible to further limit access to necessary functions and transactions.

DIRECT CONNECTIONS WITH EXTERNAL NETWORKS (TUNNERS)

The SCM Group security team (*IT Infrastructure & Security team*) must approve the creation of direct connections between SCM Group systems and the systems of external organizations, via the Internet or any other public/private network before their implementation.

OUTBOUND INTERNET ACCESS

All outbound Internet access must be approved by the IT *Infrastructure & Security Team* .

INTERNET-BASED REMOTE ACCESS

All Internet-based inbound remote access methods to SCM Group internal networks and/or multi-user computer systems must be approved by the *IT Infrastructure & Security Team* . The application of a specific authentication mechanism must be based on criteria established by the I *T Infrastructure & Security Team* to include:

- The criticality of the target information system resource
- User type: Employee, Former employees, Contractor , Supplier partner or Commercial partner
- The SCM Group classification of the information to be accessed
- Remote access by non-SCM Group employees will follow least privilege access, assigning access to SCM Group systems based on need and segregation of duties.

PROTOCOLS

All devices on the network must use only encrypted authentication mechanisms, unless otherwise authorized by the *IT Infrastructure & Security Team* . Services that use unencrypted authentication (such as, for example, Telnet) must be replaced by their encrypted equivalents or implemented in a secure manner such as traveling through an end-to-end secure tunnel or operating on a completely private network.

Any business requirements for using protocols that use an unencrypted authentication mechanism must be documented and approved by the *IT Infrastructure & Security* Team .

EMAIL

All Internet mail must be delivered via an SCM Group approved mail server. All files must be scanned for viruses before being introduced into the SCM Group's IT and communications infrastructure.

SECURITY PRIVILEGES FOR USING THE INTERNET

To manage the cost of Internet services and their continued availability to support business activities, SCM Group reserves the right to limit or revoke employee Internet privileges where usage levels or activities are deemed inappropriate or inconsistent with policies, the guidelines or fundamental principles of SCM Group and the values. SCM Group reserves the right to limit or revoke Internet privileges at its discretion.

INTERNET NAVIGATION

SCM Group blocks connections to certain non-company websites. Unintentional links to sites containing, for example, sexually explicit, racist, violent or other offensive material must be discontinued immediately. Connectivity to websites does not in itself imply that users of SCM Group systems are authorized to visit such sites.

8.2 USER ACCESS MANAGEMENT

GENERAL

PROHIBITIONS ON USER ACCOUNTS

Shared User Accounts must not be created or issued without the approval of the *IT Infrastructure & Security Team* . Shared User Accounts must have a designated SCM group owner and must be recertified annually. Process User Accounts, User Accounts used for the sole purpose of batch processing, automated processes or other non-interactive functions, must not be created or issued without the approval of the *IT Infrastructure & Security Team* . Process User Accounts must have valid designated SCM group owners and must also be recertified annually. The default accounts (user and administrator) provided with the software should be removed, disabled or renamed where technically feasible. Where not technically feasible (e.g. root , sysdba), controls approved by the *IT Infrastructure & Security Team* must be implemented to mitigate risk, including, but not limited to, changing default passwords.

USER GROUPS

Access to resources should by definition be at the group level and should be tied to job function, business area and need to know/minimum privilege.

ACCESS GRANT AND REVOCATION PROCESS

ACCESS REQUESTS

Unless specifically identified as a default resource granted as part of your employment with the company, your manager and the owner of the requested resources (where such an owner exists) must review and approve all requests for access. When assigning a new account, the new user must acknowledge that they understand their responsibilities as a user of SCM Group information assets.

NOTIFICATION IN THE EVENT OF USER TRANSFER OR TERMINATION

The Human Resources Department or the Company Management must immediately communicate to the IT Management the resignation, termination or transfer of personnel, or the termination of their business relationship with SCM Group. The transferred or terminated employee's current supervisor is responsible for directly coordinating the removal of the user's access rights. This also applies to all consultants, contractors and temporary staff. If notified of personnel transfer or termination by Human Resources or management, access must be removed within one business day.

NOTIFICATION OF ACCESS PRIVILEGE ANOMALIES

The employee is invited to promptly report any discrepancies between access privileges and tasks performed that occur during the natural evolution of the employment relationship (for example, change of tasks linked to operational needs or modification of the department, department, or area company).

Any operating anomaly must be immediately reported to the System Administrator or other IT manager, who will carry out the appropriate checks and assessments.

REVIEW OF PRIVILEGED ACCOUNT ACCESS

Annual access reviews of privileged user accounts should be conducted to ensure unauthorized user accounts are removed.

ADS REVIEW (SYSTEM ADMINISTRATORS).

Annual reviews of the list of ADSs, internal and external to the organization, must be conducted by the *IT Infrastructure & Security Team* to verify their compliance with the organizational, technical and security measures with respect to the processing of personal data required by current European legislation.

STANDARDIZED AUTHENTICATION (SSO)

All systems must integrate with and where possible rely on the company's standard authentication (SSO) system approved by the *IT Infrastructure & Security team* .

IDENTIFICATION CHECKS

USER ID ISSUANCE

User IDs must be unique and assigned to an individual regardless of computing platform. For all issued User IDs, SCM Group must maintain records of your full name, relationship to SCM Group, and contact information.

SCM GROUP USER ID COMPOSITION

User IDs must consist of the first character of the first and last name and, if required for uniqueness, use the first character of the middle name (if available) or the second/third character of the first name. Below is an example; the fields in brackets are optional for uniqueness purposes:

<first name initial >(<second character>)(<third character>)<surname>

NON-SCM PERSONAL DESIGNATION

Non-SCM Group personnel, such as consultants, contractors and temporary employees, must be easily identifiable as non-SCM Group users to anyone within the company. Any email sent must be clearly marked as not belonging to SCM Group or the respective company.

BUILT-IN CREDENTIALS

User IDs and/or related passwords should not be embedded in batch files or scripts that automate authentication sequences.

INACTIVE ACCOUNTS AND ACCOUNT EXPIRATION

Where technically feasible, SCM Group user accounts that have been inactive for more than 90 days and non-SCM Group user accounts that have been inactive for more than 60 days must be disabled. An account must remain disabled until the specified user requests the helpdesk for the account to be re-enabled and provides proof of identity, including proof that their business relationship with SCM Group has not changed. For non-SCM Group users, there must be a system-set account expiration date that coincides with the end of the project or **6 months** , whichever is less.

PRIVILEGED ACCOUNTS

Users with privileged access (root , administrator, etc.) must use a different account name than a normal user. These IDs must be revalidated **every 1 year.**

SYSTEM ACCOUNT SUSPENSION FOR UNSUCCESSFUL LOGIN ATTEMPTS

Where possible. After 10 consecutive failed login attempts, a user account must be locked out for 15 minutes or until manually reinstated by the information security administrator.

MISUSE OF IDENTITY

It is prohibited to misrepresent, obscure or suppress the identity of a user (anonymity) on any communications system.

8.3 ACCESS CREDENTIAL MANAGEMENT

Access to data is allowed only after passing an authentication procedure. It is advisable that the password chosen by the person in charge is such as to guarantee maximum protection as established by the " *2SCM - Password Policy* " procedure defined and approved by SCM Group.

PASSWORD STORAGE

Personal access credentials must be kept secret, therefore it is absolutely forbidden to save them in clear text (either on file or on paper) or communicate them to another employee or third parties in general.

PASSWORD COMPOSITION/COMPLEXITY

Passwords must be a **minimum of 16 characters.**

- Passwords must be constructed using at least 3 of the following character types:
  - Lowercase characters (including letters of the English alphabet);
  - Uppercase characters (including letters of the English alphabet);
  - Numeric characters;
  - Punctuation and special symbols available in commonly used keyboards;
- In cases where the use of special symbols is not possible, passwords must contain numeric and alphabetic characters that can be divided into a number between a minimum of 3 and a maximum of 5, without prejudice to the minimum overall length set at 16 characters;

- Passwords must contain no more than three consecutive identical characters;
- Passwords must not contain whitespace characters anywhere;
- Passwords are not allowed:
    - Equal to the corresponding user identification;
    - Containing the name or surname of the owner;
    - Containing the company number of the owner.

USER'S ABILITY TO CHANGE PASSWORDS

Users must be provided with the ability to change their password after logging in.

ONE-TIME USE OF THE INITIAL PASSWORD

If a user is provided with an initial password by SCM Group, this **must be changed the first time a user accesses a service.** Where possible, the system should apply the initial change until the early expiration. Temporary passwords must be transmitted to users in a secure and reliable manner.

MINIMUM PASSWORD AGE

Passwords must be **at least 1 day old** where technically feasible.

PASSWORD EXPIRATION

Passwords for users **must expire after 90 days.** Systems must notify the user daily, starting at least 15 days in advance, when their password will expire. An account with an expired password must be forced to change the password the next time you log in.

RESET PASSWORD

Only restore requests from the individual account holder or a delegate approved by the *IT Infrastructure & Security Team will be accepted.*

PASSWORD HISTORY

Users should not be allowed to select a password that matches any of the user's **previous 5 passwords** .

EXCEPTIONS

SCM Group recognizes that, at times, certain authorization, identification or password controls may not apply to all users. Approval from the *IT Infrastructure & Security team* is required and must be documented for all such cases.

8.4 NETWORK ACCESS CONTROL

SERVER CONNECTION

Servers should not be configured for network access without approval from the *IT Infrastructure & Security team* .

SYSTEMS ACCESS TO THE NETWORK

All hosts that store or process SCM Group data must be isolated behind a firewall from external public networks (e.g., the Internet). System administrators must restrict access to and from the relevant ports and IP addresses.

REVIEW OF ACCESS TO SERVERS FROM OUTSIDE

Firewall and router rule sets should be reviewed on an annual basis to detect unauthorized changes.

NETWORK TRAFFIC FILTERING

Network traffic should be filtered as determined by the *IT Infrastructure & Security team* . The traffic to be prohibited must include all traffic not justified by the activity and everything that is prohibited by SCM Group policies.

INVENTORY OF CONNECTIONS EXTERNAL TO THE NETWORK

An inventory of all external connections to the network must be maintained by the SCM Group IT department and must be reviewed regularly.

CONNECTIVITY TO AND BETWEEN NETWORKS

IT Infrastructure & Security Team must authorize all new connections to wireless and wired networks that could allow users to access SCM Group systems and information.

If the new connection is an addition to a previously certified internal or external connection and the connection is made using the same configuration, no prior approval is required. All connections between internal networks and the Internet (or any other publicly accessible computer network) must incorporate an approved firewall device and related access controls.

SYSTEMS ADMINISTRATION WITH REMOTE ACCESS

All systems administration not carried out from a console should be conducted using secure methods that have been approved by the *IT Infrastructure & Security team* and should where possible use two-factor authentication (MFA) whenever possible.

WIRELESS NETWORK MANAGEMENT

All wireless networks must be planned, deployed and managed in an organized and centralized manner to ensure functionality, maximum bandwidth, interference management and security. Therefore, the *IT Infrastructure & Security* team is solely responsible for implementing wireless access intended for use on the SCM Group corporate network. Wireless access to non-corporate networks (e.g. Guest access) must also be reviewed and approved by the *IT Infrastructure & Security team.*

Wireless transmissions must use strong encryption for authentication and transmission of SCM Group data.

All wireless deployments on the SCM Group network must be approved by the *IT Infrastructure & Security team.*

MODEM WIFI POLICIES

WiFi modems should not be purchased or installed in computers without approval from the *IT Infrastructure & Security team*

WiFi modem connections must be configured for outbound access only, unless written authorization is obtained from the *IT Infrastructure & Security team* .

Approval for the installation of remote control communications software (software that allows a remote user to connect to a PC connected to the network and issue commands from it as if it were connected to the network itself) must be approved in advance by the *IT Infrastructure & Security* team .

8.5 OPERATING SYSTEM ACCESS CONTROL

ACCESS CONTROL

File and directory permissions must be reviewed and reduced to the minimum necessary, according to the " Need - to-Know" principle, in order to provide the functionality of the relevant service.

CONFIGURATION AND STANDARD OPERATING SYSTEM

All systems must be configured according to configuration standards approved by the *IT Infrastructure & Security team*

SINGLE USE

All systems should be implemented to perform a primary function.

SYSTEM WARNING MESSAGE AND ACCESS BANNER

Where technically feasible, a message should be displayed at all network connections advising potential users that unauthorized use is prohibited. Login banners or greeting screens must not reveal any system information.

8.6 CONTROL ACCESS TO COMPANY APPLICATIONS

Depending on the role in the company, the employee is assigned access and credentials to company applications that may contain information regarding employees' personal data or confidential company documentation.

If, during the course of his professional life, the employee realizes that he has access to information which for the role currently held is no longer his responsibility or which over time no longer is, he must immediately report this situation to the company IT department, so that this should be remedied as soon as possible.

9. SECURITY OF COMPUTER SYSTEMS FOR ACQUISITION, DEVELOPMENT AND MAINTENANCE OF COMPANY INFORMATION

9.1 SECURITY REQUIREMENTS FOR INFORMATION SYSTEMS

SECURITY BY DESIGN

SCM Group systems, standards and platforms must be implemented with security in mind by design. Business Analysts and Business Processes Owners have joint responsibility for ensuring that security guidelines are an integral part of the system design, testing, installation and deployment process. Safety issues and impacts must be addressed and documented.

DESIGN

INFORMATION SECURITY CONTROLS IDENTIFICATION/DOCUMENTATION

All safety features must be identified and documented before installation and use. The final product documentation must include an explanation of the software's security features so they can be used effectively.

9.2 CORRECT PROCESSING IN APPLICATIONS

DEVELOPMENT

Appropriate controls must be designed into applications, including user-developed applications to ensure correct processing. These controls should include validation of input data, internal processing, output data and logging.

TESTING OF SAFETY FEATURES

Testing of security features should be performed as part of system testing. Security features documented in the security requirements and security design must be fully tested using scenarios developed during the design phase. Test results must be fully documented and retained for the life of the system.

9.3 SOFTWARE SECURITY

SECURITY SOFTWARE

SCM Group employees and users of SCM Group systems and resources must only use software authorized by the IT Department. Copyrighted software must be used in accordance with the requirements specified in the license agreement or any agreement signed with SCM Group. Users must not copy or modify the purchased software unless expressly provided in the software license. Products licensed to run on a particular computer or at a particular site

must not be copied to another computer or used at another site without the written permission of the vendor. Software copied or downloaded illegally from an unauthorized source cannot be loaded onto equipment owned by SCM Group. If you need public domain or mass-distributed programs (for example, printer drivers) for a valid business need, you should obtain them from a trusted source such as a vendor site.

PROPRIETARY SOFTWARE

Before distributing software owned by SCM Group to third parties, it is necessary to obtain authorization from the legal department and the software vendor .

9.4 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

SEPARATION OF TEST AND QA ENVIRONMENTS FROM THE PRODUCTION ENVIRONMENT

Testing and QA functions must be kept physically or logically separate from production environments.

10. SECURITY INCIDENT RESPONSE MANAGEMENT

INCIDENT RESPONSE

Refer to the document " *SCM Group - Incident Response Plan* " for all details and procedures.

INCIDENT ISOLATION

System administrators must take the necessary actions to limit the effects of a security incident by immediately isolating the problem.

1 1. BUSINESS CONTINUITY MANAGEMENT

Refer to the document " *Disaster Recovery Strategy SCM Group* " for more information.

12. TRAINING

SCM Group periodically organizes training courses on IT security for all employees (and in any case when hiring new employees) to better understand how to use IT tools, the security measures adopted and to be adopted, the procedures or security measures to be implemented .

The IT department will be responsible for all course contents and, depending on the topic, they will be organized through the company training platform or in the classroom.

The training must include a verification of the actual understanding of the contents presented (the evaluation phase must be included); the participation certification, with the results of the verification, must be documented and kept for any future verifications.