Systems Security Policy

Distribution list

Directly interested

Internal KO2

Sommario

Indice

Indice Tabelle

1 Revisioni

Revision	Date	Description
A	03/10/2019	First revision of the document

Tabella 1: Revision.

2 Introduction and general overview

2.1 Policy Objectives

The main objectives of this Policy are:

- To define the general security policy for KO2 Information Systems and the information stored, processed and transmitted by them, including outsourced services.
- To define a uniform approach, ensuring a high degree of information systems security throughout KO2
- To define responsibilities with regards to information systems security;

This document defines the general framework deriving to specific security policies and system specific security standards, as well as departmental/local procedures. All derived security policies, standards, guidelines and procedures shall be consistent with the present policy document.

2.2 Scope of the Policy

This policy applies to all KO2 staff, assignees and contractors that provide services to KO2 and is an integral part of the KO2 Business Code of Conduct.

This policy covers the security of information systems and data networks owned or used by KO2 as well as the information that is stored, transmitted or processed by those systems.

This policy does not cover issues related to general physical and building security. It covers, however, physical security aspects of buildings or parts of buildings that directly affect the security of information owned by KO2

3 Policy

This policy is intended to help you make the best use of the computer resources at your disposal, while minimizing the cyber security risks. You should understand the following:

- You are individually responsible for protecting the equipment, software and information in your hands. Security is everyone’s responsibility.
- Identify which data is non-public, which includes company confidential data, client data and personal data as further described below. If you do not know or are not sure, ask. Even though you cannot touch it, information is an asset, sometimes a priceless asset.
- Use the resources at your disposal only for the benefit of KO2.
- Understand that you are accountable for what you do on the system.
- Protect equipment from loss & theft. Only store company data on encrypted devices.

- Do not bypass established network and internet access connection rules.
- Do not bypass or uninstall your virus checking or firewall software.
- Do not change or install any unauthorized software or browser 'plug-ins'
- Do not copy or store KO2 data on external devices or unauthorized external locations (including cloud-based services which are not company approved services). Contact IT for the best solution for secured file transfer when this is required.
- If you become aware of a potential or actual Security Incident, you must report the incident as soon as possible by sending and email to: IT_support@KO2.IT

The Policies and supporting Standards in this chapter must be read, understood, acknowledged and followed by all Staff. These set the ground rules under which KO2 operates and safeguards its data and information systems to both reduce risk and minimize the effect of potential incidents.

3.1 Data Protection

KO2 takes the protection of personal data seriously and the security measures set forth in this policy are essential to ensure the data protection standards supporting the KO2 Information Management Policy are met.

3.2 Human Resources security

3.2.1 Job definition and resourcing

Information security must be covered in the Group's Security Human Resources policy and standards. The HR policies should ensure, as a minimum, that security is adequately covered in job descriptions; that personnel are adequately screened, trained and that confidentiality agreements are signed by all new employees and contractors.

3.2.2 User training on Security Awareness

A training plan and training material must be in place to ensure that the right level of Security Awareness is created and maintained within the organization. Software developers and all other relevant personnel involved in the development of software for KO2 are required to undertake secure development training on a periodic basis

3.3 Asset Management

KO2 uses a variety of information assets, ranging from laptops and mobile phones to servers. An inventory needs to constantly be maintained and must include the following details for all significant information assets belonging to, or used by the company:

- Asset name and characteristics

- The information owner
- The custodian of the information, and repository location (database etc.)
- The sensitivity of the asset, due to regulations, laws, customer expectations or other requirements
- Requirements for the asset regarding availability, uptime, business continuity, etc.

3.3.1 Hardware Management

At KO2 we take a hardware lifecycle approach to hardware management:

- Hardware should only be acquired from approved vendors.
- Only approved software configurations should be applied to new hardware
- End-users should take appropriate care with any hardware that has been issued to them;
- Lost/Stolen hardware should be reported immediately.
- End-of-Life hardware should be securely disposed

3.4 Information Management

3.4.1 Information Classification

The KO2 Information Security Policy focuses on the protection of the 3 components of information stored on KO2 systems: Confidentiality, Integrity & Availability, whilst ensuring Data Privacy.
All KO2 information must be classified based on these 3 categories in order to allow implementation of the appropriate levels of protection in line with its criticality and to ensure that the controls applied to it are sufficient, and do not impair the company's business.
Information classification requirements are detailed in the KO2 Information Management Policy

3.4.2 Information Handling

Information, in electronic and physical formats, should be handled in accordance with the sensitivity, risk and classification of the information:

- Ensure confidentiality agreements are in place before sharing data externally
- Check email addresses prior to sending any files.
- Files should only be copied to removable storage when necessary and the storage should be encrypted.
- Use restricted access storage areas whenever possible
- Data disposal should be done in accordance with the Information Asset Handling and Protection Standard for End User

3.5 System Access Policy

Access to information and systems in the possession of, or under the control of KO2 must be provided based on a least privilege, need to know basis.
All KO2 computers must be protected by approved password-based access control systems.
Multi-factor authentication for remote access to corporate and production networks by employees, administrators, and third parties shall be implemented where available.
The following rules must be maintained for managing user access rights:

- User registration: approving and granting access rights to users on a need-to-know basis.
- Privilege management. Clear hierarchies must be determined for each system, and each hierarchy must be formally approved.
- User management. As above, each system must have clear procedures for approval and method of granting access to that system. Procedures must exist for each system for both joiners, movers and leavers, with audit trails.
- User access rights are subject to periodic reviews.
- Inactive user accounts must be configured to automatically disable after 90 days

3.6 User Authentication Standard

Users must be forced to change their passwords during the first log on, and at 60 - day intervals.

Passwords shall not be displayed or transmitted in clear text and shall be suitably protected via approved cryptographic solutions.

Passwords shall be stored in an encrypted format. A history of passwords shall be maintained to prevent the re-use of passwords.

A maximum of five successive login failures shall result in account lockout until an administrator unlocks it.

Default accounts shall be disabled and/or default passwords associated with such accounts shall be changed.

3.7 Password Selection

In order to make it harder to guess or steal your passwords please keep in mind the following:

- All the passwords should be with a minimum of 8 characters
- Do not use dictionary words - All real words are easy to guess. Avoid using any words, words in foreign languages, swear words, slang, names, nicknames, etc.
- The names of family, friends and partners, anniversary dates, car registrations and telephone numbers are the first things tried when guessing your passwords.
- Instead try to use acronyms relevant to you only, mnemonics, random letters, etc., and insert nonalphabetic characters in the middle of the word
- Use a mixture of UPPER and lower case, numbers and special characters.
- When changing passwords, change more than just the number.
- However, choose something you can remember. It is no use having a strong password if you have it written on a Post-It Note on your desk! If you must have a reminder or

hint, use something cryptic that only you can understand.

- Never tell anyone else your password or allow them to log in as you.
- Try to avoid letting other people watch you key-in your password. Choose something that is not easy to guess from watching
- Be aware of 'social engineering'. These are practices used to obtain personal information such as passwords, account numbers etc. (via fake web pages, e-mails, phone calls).
- Phishing is an example of social engineering
- Phishing are e-mail messages that entice recipients to divulge passwords and other information (e.g., via clicking embedded links). These e-mails are disguised to appear as if coming from a trusted source. In such cases, do not respond and report this as a Security Incident.
- Use Multi-Factor Authentication, if available. This is a combination of something you know (e.g., password), something you have (e.g., a token, a smartphone) and / or something you are (e.g., biometric – fingerprint).

3.8 Acceptable Use Policy

IT resources may only be used for KO2 business related purposes.

3.8.1 Email Usage

E-mail is a business communication tool which all KO2 employees are requested to use in a responsible, effective and lawful manner.

3.8.2 Internet Usage

KO2 provides Internet access to all staff to assist them in carrying out their duties such as looking up details about suppliers, products, accessing governmental information and other work-related information.

Occasional and limited personal use of the Internet is permitted if such use does not:

- Interfere with work performance & productivity.
- Include downloading or distribution of large files.
- Have negative impact on the performance of KO2' IT systems.

When using Internet access facilities, you should comply with the following guidelines:

- Keep your personal use of Internet to a minimum.
- Check that any information you use from the Internet is accurate, complete and current.
- Respect the legal protections of data, software, copyright and licenses.
- Immediately inform the Security team of any unusual occurrence.
- Do not download or transmit text or images which contain any software, material of obscene, threatening, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
- Do not use the company's equipment to make unauthorized access to any other computer or network.
- Do not represent yourself as another person.

It is STRICTLY FORBIDDEN to upload Company non-public Information such as any of the following to external file transfer or storage sites, like Box, Dropbox or Google Drive:

- Source Code, object code, user documentation and all other software development details.

- Project related information.
- Personally Identifiable Information.
- Company strategy and business plans.
- IT infrastructure arrangements including any log files.
- Intellectual Property, such as: Copyrights, Patents and Trade Secrets.
- Employee personal information such as salaries, appraisals, medical records or health care details.
- Any information concerning our clients and prospects including details of our client projects, client proposals, contracts, fees or strategic plans.
- Information related to our clients' customers, including any details stored within KO2 software products, such as transaction or bank account details.
- Any other company non-public information.

3.8.3 Portable Media

The use of portable media is not permitted.
The intended purpose is to protect customer and company information from being transferred via unauthorized means.
KO2 reserve the right to inspect and erase portable media that is used on our network

3.9 Remote Access and Electronic Communication

Frequently users will be required to access the Group's Information systems from outside the office, for example travelling consultants and/or employees working in Sales / Business Solutions.

For remote access to the IT Infrastructure resources only the officially supported and approved facilities by the internal IT department are to be used (i.e., KO2 Secure Access Portal). The associated security policies must be applied.

Online Communication within KO2 offices to an external party may only use KO2 approved communication channels. Personal internet connections or connectivity devices (e.g., using personal data modems and Mobile Hotspot connections, remote access connections, personal VPNs etc.) are strictly prohibited.

3.10 System Changes and Configuration

KO2 recognizes that change is a necessary process in order that we can maintain, protect, and enhance services provided to Clients, however uncontrolled change can create significant security risks for KO2. KO2 also recognizes that there are different types of change, therefore, an efficient change management process must be implemented to handle these different types in the most appropriate manner.

All changes must be conducted in a controlled and approved way, in accordance with the IT Change Management Standard and IT System Configuration Standard.

System changes or re-configurations of standard IT components are not allowed. Only additions and/or changes of software components can be made by users on workstations based on customer project requirements.

The following system changes are strictly prohibited

- Installation of:
  - Unauthorized connectivity devices (e.g., data modems, router….);
  - Any component suitable to gain unauthorized access to restricted areas;
  - Any other non-standard software or hardware component.
- Merging of two networks by physically integrating them on a network node;
- Disabling virus protection;

3.11 Network and Communication Policy

3.11.1 Internet Usage

At KO2 a secure network is critical to the security of our business:

- External facing networks should be firewalled to an appropriate level
- Physical and logical network changes should only be made by approved users
- Networks should be segregated on a geographical and/or business line basis
- Appropriate controls should be in place at network interfaces
- WAN services should only be acquired through approved vendors
- Network event logging and monitoring should be implemented
- Third-party users shall not connect their computing devices to the wired or wireless network of KO2, unless authorized.
- KO2 computers and networks may be connected to third-party computers or networks only with explicit approval after determination that the combined systems will be in compliance with KO2 security requirements.

3.11.2 Wireless Networks

- Passwords for Guest wireless networks should be changed on a regular basis
- Only approved wireless access points should be used
- Wireless networks should always be encrypted

3.12 Incident Management Policy

3.12.1 Event Logging and Monitoring

Adequate monitoring controls to detect attacks and unauthorized access to its information processing systems must be implemented. The level of monitoring required shall be determined by risk assessment and any relevant or applicable legal requirements shall be identified to ensure that the monitoring activities comply with the requirements.

Monitoring may consist of activities such as the review of:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Help desk tickets
- Vulnerability Scanning
- Other log and error files

Any security issues discovered will be reported to the Information Security Department for investigation. Our detailed policy is set out in the Security Event Logging and

Monitoring Standard

3.12.2 User Monitoring

In order to maintain the security of the Group's IT systems (including to prevent cybersecurity threats) and to protect the Group's assets and data, KO2' monitors many aspects of user behavior including but not limited to:

- Monitoring Internet access usage;
- Reviewing material downloaded or uploaded via the Internet;
- Reviewing e-mails sent or received by users, if there is a well-founded suspicion about a breach of provisions of this Policy or of applicable laws, or if there is a legal or regulatory requirement in this respect;
- Reviewing installed software on user's computers;
- Logins to and use of KO2' network as well as use of PCs.

Any monitoring done by KO2 will be in accordance with applicable law.

3.13 Workstation Security

Workstations include laptops and desktops:

- All workstations should have corporate-approved antivirus software installed and enabled
- All workstations should have data loss protection software installed (where available)
- All laptops should be encrypted
- Only install software from trusted sources
- Do not allow unauthorized users to access your
- workstation
- Take appropriate steps to maintain the physical security of your workstation

3.14 Mobile Device Security

Every mobile device capable of accessing KO2 information shall be enrolled in the company MDM solution.

In the event of the loss of a mobile device or unauthorized
access to a mobile device, the user should contact the local IT team and report the Security Incident to Information Security Team

3.15 Bring Your Own Device

Only KO2 owned devices are considered trusted and can be connected directly to the KO2 Local Area Network (LAN). All non-KO2 owned devices are by default considered as untrusted. Untrusted devices must never be connected directly to KO2 Internal network, neither through a network cable connection in a KO2 office, nor through the KO2 Employee wireless network. Untrusted (non- KO2 owned) devices are only allowed to use Visitor network access while in a KO2 office.

Employees personal devices are not allowed to be connected to KO2 corporate network

3.16 Business Application Management Policy

At KO2 we have a high dependency on software to conduct our day-to-day business:

- Applications should comply with the Privacy By Design principle.
- A Data Privacy Impact Assessment (DPIA) should be completed for major software changes that involve personally-identifiable information (PII).
- Security requirements for software should bedocumented as part of the development process
- Software changes should be subject to change control procedures
- Only authorized users are permitted to deploy software changes

This policy only applies to software we develop for internal users e.g., VMWARE Tools, RedHat suite, Oracle E-Business, development of the KO2 Product Suite is outside the scope of this policy

3.17 Encryption

Encryption is required to be used to protect Company nonpublic Information from being disclosed to unauthorized parties. All personnel are responsible for assessing the confidentiality level of data being sent or residing on the devices they use. If data is non-public, all KO2 employees are responsible to comply with the Encryption Standard.

3.18 Backup

KO2 Business Continuity Management Policy provides a framework for ensuring that information in scope of this policy will not be lost during an incident affecting availability or integrity. Similarly, all media containing backups of KO2 data must be protected according to the data classification related to Data Confidentiality, Integrity & Availability, whilst ensuring data privacy.

Both data classification and backup requirements must be determined by the asset owner and communicated to IT for implementation. Asset / data owners are responsible to inform IT in writing of the specific backup requirements for each asset or data set and of the required backup retention period in line with Business Continuity Management Policy.

3.19 Malware Protection

A process must be maintained to ensure that malicious software cannot enter the secure IT environment. This will include regular anti-malware updates, schedule malware scans and monitoring of events and incidents related to malware.

3.20 Security Incident Management Standard

KO2 follows a consistent and effective process to address any actual or suspected security incidents relating to information systems and data. Security Incident Management Standard details the framework for early detection, reporting and responding to security incidents.

All security incidents whether actual or suspected, must be reported as soon as possible by sending an email to IT_support@ko2.it

Even if a Security Incident is not considered to be serious, it should always be reported as it may be part of a wider issue or trend. Additionally, first appearances of the severity of the Security Incident may be deceptive and not indicative of the severity of the underlying risk.

3.21 Responsabilities

Information Security is everyone’s responsibility, although the ultimate responsibility resides with the Board of Directors and Executive Management. This responsibility cascades down through a series of designated roles.

3.21.1 Managers

Managers shall be individually responsible for the security of their environments where information is processed or stored.

Furthermore, they are responsible with:

- Ensuring that all staff, permanent, temporary and/or contractors, are aware of the information security policies, procedures and user obligations applicable to their area of work and of their personal responsibilities for information security;
- Determining the level of access to be granted to specific individuals;
- Ensuring staff have appropriate training for the systems they use;
- Ensuring staff know how to access advice on information security matters.

3.21.2 All Staff

All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. In particular, all staff should understand:

What information they are using, how it should be used, stored and transferred in terms of data security;

- What procedures, standards and protocols exist for the sharing of information with other parties;
- How to report a suspected breach of information security within the organization;
- Their responsibility for raising any information security concerns

All KO2 users are responsible with adhering to the provisions of this Policy and all related policies, standards, guidelines and procedures and must report every incident of misuse or abuse of which they become aware as described in the KO2 Security Incident Management Policy.

3.21.3 External contractors

All contracts with external contractors that allow access to the organization's data or information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organization comply with all appropriate security policies.

4 Breach

Breach of this Policy will be taken seriously and may result in disciplinary actions in conformity with the legal and contractual framework, including termination of employment.
Any user disregarding the rules set out in this Policy or in applicable laws will be fully liable and KO2 will disassociate itself from the user as far as legally possible.
All breaches of this policy must be reported to the respective Manager/Director for appropriate action.
All security incidents whether actual or suspected, must be reported
as soon as possible by sending an email to IT_support@ko2.it

4.1 Physical Securty

All of the aspect of the physical security related to the KO2 Governance are described on the "DVR Document"

Rome 03 october 2019

L'Amministratore Unico

KO2 s.r.l.
Società Unipersonale
Via Marsala, 29/h 00185 Roma (RM)
C.F. e P. IVA IT14856901005
Iscrizione R.E.A. Roma n.1551093