Cestaro Rossi & C. S.p.a. cyber security policy

Policy brief & purpose

Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure. The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation. For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks.

Scope

This policy applies to all our employees, suppliers and anyone who has permanent or temporary access to our systems and hardware.

Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data.

Company PCs are supplied already password protected and blocked from installing apps except with the direct intervention of the IT Manager via the "Administrator" user, with antivirus and automatic updating of company apps and the operating system.
We aks to our employees to keep both their personal and company-issued computer, tablet and cell phone secure.
You can protect your personal devices if:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave the devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

We also ask to our employees:

- to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others
- to access company accounts and systems only through secure, private networks.

When new employees receive company-issued equipment, they will be given instructions on how to handle it properly and ensure the security of company data.
If you have any questions, please contact the IT Manager.
Keep emails safe
Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we ask to our employees to:

- Check email and names of people they received a message from to ensure they are legitimate.
- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, must absolutely not open it and can contact our IT Manager

Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we ask to our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Do not exchange credentials with other persons
- Change their passwords every six months.

Transfer data securely

Transferring data introduces security risk. Employees must:

- Do not use USB flash drives to transfer data
- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our IT Manager for help.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

Our IT Manager need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we ask to our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our IT Manager must investigate promptly, resolve the issue and send a companywide alert when necessary.
Our IT Manager is responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to him with any questions or concerns.

Internet Browsing

The device enabled for Internet browsing is a company tool necessary for carrying out the assigned work activity. Browsing the Internet for reasons other than those strictly related to work activity is therefore absolutely prohibited. Our employees are not permitted to:

- access INTERNET sites by avoiding or overcoming or in any case attempting to overtake or disable the systems adopted by the company to block access to some sites and in any case use sites or other tools (e.g. CRACKING PROGRAMS) that achieve this purpose
- access INTERNET sites that have content contrary to the law and to rules for the protection of public order, relevant for the purposes of the commission of a crime, or that are in any way discriminatory on the basis of race, ethnic origin, skin color, religious faith, age, sex, citizenship, marital status, handicaps.

The company internet connection service must not be used to commit punishable or reprehensible actions such as infringing intellectual property rights and visiting pornographic sites. In this sense, by way of example, the user may not use the internet to:

- upload or download freeware and shareware software, as well as the use of documents, including films and music, from websites or http, unless strictly related to work activities and after checking the reliability of the sites in question (in case of doubt, the IT Manager must be contacted for this purpose)
- carry out any type of financial transaction including remote banking, online purchases and the like, except in cases directly authorised by the General Management (or possibly by the Office Manager and/or the IT Manager) and in any case in compliance with the normal purchasing procedures
- any form of registration on sites whose contents are not strictly related to work activities
- participation in non-professional forums, use of chat lines (excluding authorised tools), electronic bulletin boards and registrations in guest books, even using pseudonyms (or nicknames) unless expressly authorised by the Office Manager
- access, via the internet, to personal webmail boxes
- access to Social Media (ex. Linkedin, Facebook, Instagram, X, TikTok etc.) unless expressly authorised by the Office Manager

Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to IT Manager
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.

- Avoid accessing suspicious websites.

Our IT Manager:

- Install firewalls, anti malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.

Our company will have all physical and digital shields to protect information.

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches will face disciplinary actions.

Suppliers

Our Supplier guarantees that its IT systems, including the systems used to provide the services/products that are the subject of our contractual relationships, comply with the Cyber Security requirements requested by our Company and the End Customer, and that they are in line with the international reference standards (e.g.: NIST, ISO/IEC 27000 information security management systems, etc.). In particular, our Supplier, with reference to the above systems, guarantees:

- to have adopted and to adopt all the measures necessary to guarantee timely compliance with the provisions of the law regarding the processing of personal data and compliance with standards and regulations regarding cyber security;
- to have obtained any security certifications necessary to comply with obligations of compliance with standards and regulations;
- that such systems are free from security vulnerabilities and malicious code such as, by way of example and not limited to, viruses, Trojans, and backdoors, capable of compromising the confidentiality, availability and integrity of data or in any case jeopardizing the security of our Company's IT systems

If situations arise such as, by way of example and not limited to, non-compliance and/or security vulnerabilities detected in the auditing/monitoring activities conducted by our Company, directly and/or through third parties, cyber risk factors related to our relationship and reported by our Company, our Supplier is required to formulate a plan containing the operational actions for the resolution or, alternatively, the mitigation, of such critical issues,

which must be submitted for approval by our Company. All activities related to such plan are the responsibility of our Supplier, without any cost to our Company and will be monitored by our Company. If during the course of our relationship there are regulatory changes (national, EU or international) or industry practices (for example standardizations) that require the adoption of Cyber Security, organizational and/or technical measures, additional and/or different to those previously defined, our Supplier must ensure the integration and updating of the Cyber Security requirements relating to our relationship in order to comply with compliance obligations. In the event of Cyber Incidents and/or Data Breaches that directly affect the applications and/or IT systems, products and data covered by our relationship or, indirectly, the IT systems and information from our Company and/or the End Customer, our Supplier is required to alert us promptly, communicating which data and/or systems are involved and ensuring a prompt response and restoration without any cost to our Company and will be monitored by us.

Take security seriously

Everyone, from our customers and partners to our employees and suppliers, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Firmato digitalmente da Fabio Dalla Serra
ND: cn=Fabio Dalla Serra, o=Cestaro Rossi &c. S.p.A., ou=Presidente, email=f.dallaserra@cestarorossi.com, c=IT
Data: 2024.11.12 13:00:48 +01'00'