Information and technology security

We use information technology to advance the business interests of company and our customers. We recognize that the use of information technology and associated systems such as email, software, networks, applications, internet and social media might all be subject to cyberattacks and other similar internal and external threats. We use our information technology responsibly, only for legitimate business purposes, consistent with company's interests and rights, and in accordance with company's rules, regarding our information technology systems.

What you should keep in knowledge

• Social media must be used responsibly. Inappropriate communication or unauthorized sharing of information (e.g. images, comments, links or other data) could cause legal or reputational damage to you, your colleagues, company, our customers, or others.
• Limited personal use of company's information technology assets is permissible in accordance with applicable policies, provided such use is not in conflict with company's interests
• Cyberattacks typically aim at stealing data or making systems unusable and can have many victims, including customers or employees. Compromised systems can severely interfere with our information technology and operational technology systems.
• Portable storage devices, such as USB sticks, may contain malicious software and pose a risk to our systems. They should only be used with the greatest care and to the extent authorized.
• Information produced and stored on company's information systems is a company asset. Company reserves the right to monitor the use of its information systems and to access, retrieve and disclose all such information except where limited by law or agreement.
• Emails and other forms of electronic and instant communication might be regarded as statements issued by company and should be written with care and attention. Failure to do so may bring company into disrepute or put company at a disadvantage in a commercial relation

Your responsibilities

• Never download, access or install software that you are not authorized or licensed to use or download on company information systems. Never download or store company information on personal or non-company equipment or networks. Only store appropriate content on your company-issued mobile phone, computer or other electronic devices.
• Protect your passwords. Do not write them down. Do not share them with others, including the support staff.
• Use company accounts, not personal accounts, for business communication and storing data.
• If you become aware of a possible cyberattack or other malicious behavior on company's systems or assets, you must immediately inform to the IT team.
• Act with caution with emails from unknown sources. Do not open suspicious attachments or links as they may put company's information systems at risk. Report such emails through the specific means provided in the email system or to the IT team.

We aim to Achieve Zero cases related to information & technology security breaches throughout our operations.

Intellectual property and confidential information

We take great pride in our spirit of innovation. Company has created an immensely valuable brand and continuously adds to its portfolio of intellectual property that is incorporated into patents, copyrights, trademarks, service marks, trade secrets, design rights, and other proprietary rights. We also possess vast amounts of expertise and other confidential information that give us a competitive edge in the marketplace. We vigorously protect our intellectual property and confidential information, and follow our internal policies on the proper use, safekeeping, marking and handling of such property and information. We respect the intellectual property and confidential information of others and expect the same from others in return.

What you should keep in knowledge

• Promptly disclose, prior to dissemination to others, ideas, inventions or developments to company's intellectual property counsel so that appropriate legal protections may be developed.

• It is likely that you handle company confidential or trade secret information every day – safeguard its contents from unauthorized disclosure to third parties, avoid discussions in public places, and use filter screens on laptops when working externally.

• Confidential information needs to be appropriately labelled and classified, and access should be limited to only those who have a specific need to know. Remember that an outside party must sign a proper non-disclosure agreement before disclosure of any confidential information

• When handling intellectual property, you need to ask: who owns this, am I authorized to use it, may I share it with others, and is the user's license or access rights still valid?

• Inappropriate use of others' intellectual property may expose company and you to possible criminal and civil fines and penalties.

• Your obligations regarding the confidentiality of company's proprietary information remain in place even after you have left company

Your responsibilities

• Use company's confidential information, and authorized confidential information of others, for business purposes only, and disclose it only to those who are authorized and have a need to know.

• Seek advice from company's intellectual property counsel before you solicit, negotiate, accept or use intellectual property not owned or managed by company and before letting a non-company entity use or have access to any of company's confidential information or intellectual property.

• Involve company's intellectual property counsel before dealing with any legal intellectual property matter, agreements concerning intellectual property rights (such as third-party licenses for instance), or another party's possible use of company's intellectual property

• Comply strictly with intellectual property licenses, obligations and term requirements, including third-party offerings, as in the case of software or images. Ensure company complies with the obligations in such licenses, whether for a limited use or for commercialization.

• Seek legal review from company's intellectual property counsel before externally publishing technical or company information that may contain intellectual property rights of company.

We aim to Achieve Zero cases related to loss of intellectual property and confidential information throughout our operations

Privacy and Personal data

We acknowledge the importance of personal data protection and believe that the principles behind data protection strengthen individual rights. We collect, use, store, handle, transfer and disclose personal data in accordance with applicable laws and expect our suppliers and business partners to do the same. Company's global standards for safeguarding personal data ensures that company provides a high level of protection regardless of where the data is collected and processed

What you should keep in knowledge

• Personal data means any information relating to an identified or identifiable natural person. This may include, for example, a person's home or office address, email address, phone number, photo, birthdate, banking or payroll information, IP address, mobile device ID, government-issued identification information and other similar information of that person.
• Company collects, uses, stores, handles, transfers and discloses personal data in accordance with applicable laws.
• Certain categories of personal data must be treated with greater care, including, for example, race, ethnicity, political affiliations, religion, and membership in a trade union, physical or mental health data, sexual orientation, criminal records and genetic and biometric data.
• Email and internet communications made through company workplaces, networks, devices and providers may be treated as company's business information and so may be accessed, retrieved, monitored and disclosed by company, subject to applicable legislation and contractual agreements.

Your responsibilities

• Only use personal data consistent with the business purpose for which it was collected and for only as long as necessary. Use the minimum personal data you need for your purpose; do not collect or use data that is not necessary or beyond document retention limits.
• If you transfer personal data, be aware of applicable local regulations. Be careful not to transfer personal data between countries without first understanding the data privacy standards in those countries.
• When collecting and using personal data, be careful to safeguard it against inadvertent disclosure, for example, by leaving data viewable in open spaces, electronic collaboration sites, at the printer, or in or on unsecured computers, devices, desks or cabinets.
• Report immediately security incidents involving personal data or any perceived weakness in company's privacy to the IT team.
• Be familiar and comply with the relevant privacy, security and data protection policies, including company's Corporate Regulation on data privacy

We aim to Achieve Zero cases related to loss/breach of privacy and Personal data throughout our operations.