



SOCIAL MEDIA & INTERNET USAGE POLICY

1. **POLICY BRIEF**

This policy provides a framework for using social media and internet. Social media is a place where people exchange information, opinions, and experiences to learn, develop and have fun. Whether you're handling a corporate account or using one of your own, you should remain productive and avoid damaging our organization in any way. This policy provides practical advice to avoid issues that might arise by careless use of social media in the workplace. This policy also outlines our guidelines for using our company's internet connection. We want to avoid inappropriate or illegal internet use that creates risks for our company's legality and reputation.

2. **SCOPE**

This policy applies to all our employees, Directors, Officers, employees of subsidiaries and affiliates, contractors and anyone who has permanent or temporary access to our systems and hardware.

3. **POLICY ELEMENTS**

A. **Social media usage policy**

By "social media", we refer to a variety of online platforms such as blogs, social networks, chat rooms and forums – not only platforms like Facebook or Twitter.

a) *Using personal social media*

We ask you to be careful when posting on social media. We can't restrict what you post, but we expect you to refrain from sharing confidential or private information about the company's business operations. We also caution you to avoid posting something that might make your collaboration with your colleagues more difficult (e.g. hate speech, discriminatory comments, etc.).

Overall, we advise our employees to:

- **Ensure others know that your personal account or statements don't represent our company.** You shouldn't state or imply that your personal opinions and content are authorized or endorsed by

our company. We advise using a disclaimer such as “opinions are my own” to avoid misunderstandings.

- **Avoid sharing intellectual property.** Employees should get appropriate permission to use a third party's copyrights, trademarks, service marks or other intellectual property.
- **Avoid any defamatory, offensive or derogatory content.** All employees are to maintain appropriate practices and refrain from activity that can be interpreted as disrespectful, or discriminatory based on race, sex, disability, religion or any other status protected by law. Although not an exclusive list, some specific examples of prohibited social media conduct, while employed at the company include posting commentary, content, or images that are defamatory, obscene, harassing, slanderous, or that can create a hostile work environment.

b) Representing our company

Some employees represent our company by handling corporate social media accounts or speak on our company's behalf. When you're sitting behind a corporate social media account, we expect you to act carefully and responsibly to protect our company's image and reputation. You should:

- **Be respectful, polite and patient**, when engaging in conversations on our company's behalf. You should be extra careful when making declarations or promises towards stakeholders (e.g. employees, local population, the public, politicians, etc.).
- **Avoid speaking on matters outside your field of expertise** when possible. Everyone should be careful not to answer questions or make statements that fall under somebody else's responsibility.
- **Observe laws on copyright, trademarks, plagiarism**, and get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- **Avoid deleting or ignoring comments** for no reason. Listen and reply to criticism.
- **Never post discriminatory, offensive or libelous** content and commentary.
- **Correct or remove** any misleading or false content as quickly as possible.

c) Disciplinary Consequences

We will monitor all social media postings on our corporate accounts.

We may take disciplinary action leading up to and including termination if employees do not follow this policy's guidelines. Examples of non-conformity with the employee social media policy include but are not limited to:

- Disregarding job responsibilities and limits to use social media at work.
- Disclosing confidential information through personal or corporate accounts.
- Directing offensive comments towards other members of the online community.

If you violate this policy inadvertently, you may receive a reprimand. In case of recidivism stricter disciplinary actions will apply.

B. Internet usage policy

a) *What is appropriate employee internet usage?*

Our employees are advised to use our company's internet connection for the following purpose:

- To complete their job duties.
- To seek out information that they can use to improve their work.

We don't want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgement and remain productive at work while using the internet.

Any use of our network and connection must follow our cybersecurity policy.

b) *What is inappropriate employee internet usage?*

Our employees must not use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

We also advise our employees to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask our IT service provider.

Our company may install anti-virus and disk encryption software on our company computers. Employees may not deactivate or configure settings and firewalls without managerial approval.

We won't assume any responsibility if employee devices are infected by malicious software, or if their personal data are compromised resulting from inappropriate employee use.

c) *Email*

Our employees should use their corporate email account for work-related purposes only in compliance this policy's rules. Employees shouldn't use their corporate email to:

- Register to illegal, unsafe, disreputable or suspect websites and services.
- Send obscene, offensive or discriminatory messages and content.
- Send unauthorized advertisements or solicitation emails.

Our company has the right to monitor corporate emails. We also have the right to monitor websites employees visit on our computers and networks.

d) *Disciplinary Action*

Employees who don't conform to this employee internet usage policy will face disciplinary action. Serious and/or repeat violations will be cause for termination of employment, or legal action when appropriate. Examples of serious violations are:

- Using our internet connection to steal or engage in other illegal activities.
- Causing our computers to be infected by viruses, worms or other malicious software.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.