EMAPTA

Secure Use of social media Policy

PROTECTED

DOCUMENT CONTROL NO.: EVSI.ITD.25.00PM
EFFECTIVITY DATE: June 2024

TABLE OF CONTENTS

1. OVERVIEW

1.1. Emapta (the Company) recognizes employees' rights to use social media during non-working hours for personal reasons but acknowledges associated risks and responsibilities that may impact the workplace. This Secure Use of social media Policy aims to guide responsible social media use, ensuring that employee actions do not expose the Company to legal, security, or public relations issues. Employees violating this policy may face sanctions, including termination, and legal actions for illegal social media use.

1.2. This document is marked as PROTECTED by EMAPTA; access to this document is restricted only to Emapta Employees.

2. OBJECTIVE

2.1. The objective of this policy is to:

2.1.1. Ensure that employees use social media responsibly and in a manner that does not jeopardize the Company's interests.

2.1.2. Protect the Company's confidential and proprietary information.

2.1.3. Uphold the Company's reputation and prevent any public relations issues.

2.1.4. Ensure compliance with applicable laws and Company policies.

2.1.5. Define the guidelines for both personal and Company-sponsored social media use.

3. SCOPE

3.1. This policy applies to all Emapta employees and other individuals & entities granted use of Emapta information, including, but not limited to, contractors, temporary employees, partners, and vendors.

4. DEFINITION OF TERMS

4.1. **Social media:** Includes all forms of Internet communication and content posting, encompassing personal web pages, message boards, networks, communities, blogs, and social networking sites (e.g., Facebook, Twitter, LinkedIn, Tumblr, TikTok, YouTube, Instagram, and Google My Business). It also extends to platforms such as Glassdoor, indeed, and JobStreet.

4.2. **Company-Sponsored social media:** Social media accounts and platforms that the Company uses to communicate with current and prospective employees, customers, suppliers, and the general public. These accounts are owned by the Company and managed by authorized employees.

5. ROLES AND RESPONSIBILITIES

5.1. Employees:

5.1.1. Ensure compliance with this policy and all related Company policies.

5.1.2. Protect confidential and proprietary information.

5.1.3. Use social media responsibly and ethically.

5.1.4. Report any violations or concerns related to social media use to their manager or Customer Experience Management (CXM).

5.2. Managers:

5.2.1. Educate team members about this policy and ensure adherence.

5.2.2. Monitor employees' social media activities as needed and report violations.

5.2.3. Provide guidance to employees on appropriate social media use.

5.3. Customer Experience Management (CXM):

5.3.1. Oversee the implementation and compliance of this policy.

5.3.2. Address concerns and questions from employees regarding social media use.

5.3.3. Monitor Company-sponsored social media for compliance and effectiveness.

6. RESPONSIBLE USE OF SOCIAL MEDIA

6.1. Confidential Information

6.1.1. When engaging in social media, employees are responsible for protecting Company trade secrets, as well as proprietary and confidential information. Using or disclosing Company trade secrets, as well as proprietary and confidential information is prohibited. Some examples of confidential or proprietary information within the meaning of this policy include:

6.1.1.1. Non-public information regarding business strategies, costs, contract terms, and similar information which could be used by competitors to the Company’s disadvantage.

6.1.1.2. The names of the Company's Clients subject to non-disclosure to the public of their partnership with the Company that could, if disclosed without authorization, subject the Company or employees to liability.

6.1.1.3. Confidential or personal information regarding third parties doing business with the Company that could, if disclosed without authorization, subject the Company or employees to liability.

6.1.1.4. Private information about the Company's employees and third parties doing business with the Company that could, if disclosed without authorization, violate data protection and privacy laws or result in legal action against the Company or employees; and

6.2. Company Policy Compliance

6.2.1. Employees are responsible for ensuring their activities do not violate the Company's policies, including policies prohibiting harassment, discrimination, and retaliation.

6.2.2. Employees are prohibited from using social media to post or display comments about the Company's employees, customers, vendors, suppliers, or other third parties that are vulgar, political, obscene, physically threatening or intimidating, harassing, or otherwise constitute a violation of the Company's policies against discrimination or harassment on account of an individual's race, ethnicity, religion, age, sex, sexual orientation, disability, or other protected characteristic.

6.2.3. Additionally, when posting employees' personal point of view, employees are responsible for avoiding any statement or implication that the views employees express are those of the Company. Employees may not at any time make statements about the Company's services that cannot be substantiated.

6.3. Personal Information

6.3.1. Do not share personal information about any other employee, such as their name or other personal information, unless verified by or with the consent of the employee.

6.4. Applicable Laws

6.4.1. Employees are required to abide by all applicable laws when using social media, including but not limited to criminal, intellectual property, data protection, privacy, and libel/slander laws.

6.5. Policy Violation

6.5.1. Employees who violate the social media policy will be informed of the consequences facing their actions. Depending on the nature and severity of the violation, the Company will decide how to handle the matter. Before taking any grave actions such as termination of employment, the Company will consider the employee's past social media activity to determine the motives behind the committed violation.

7. SOCIAL MEDIA DO'S & DON'TS

7.1. Employees are encouraged to do the following on their social media accounts:

7.1.1. Do:

7.1.1.1. Maintain the highest levels of courtesy and professionalism.

7.1.1.2. Update their job title and employer.

7.1.1.3. Mention that the views expressed are their personal input and not those of the company.

7.1.1.4. Tag the Company's profile in the description of their work-related posts – such as on Facebook, Twitter, LinkedIn, and Instagram.

7.1.1.5. Report to the Company any sighted posts, groups, accounts, pages, or social media events that violate the Company's social media policy or that misrepresent the Company

7.1.1.6. Consult with their Manager or Customer Experience Management (CXM) before posting any information on social media about our Clients

7.1.2. Do Not:

7.1.2.1. Post content that can be interpreted as obscene, threatening, politically charged, intimidating, discriminating, harassing or bullying.

7.1.2.2. Allow any incorrect, confidential or non-public content about Emapta or our Clients to be posted on social media; don't disclose the names of our clients on social media unless they have given consent.

7.1.2.3. Respond to questions or negative comments on the official pages, unless they are officially authorised to respond on behalf of the Company.

7.1.2.4. Discuss details about employees, customers, partners and suppliers without their expressed consent.

7.1.2.5. Post content published by competitors.

7.1.2.6. Post specific technology details and software tools owned by the Company (e.g., security software, IT infrastructure components) on public profiles in order to limit any information that can be used by fraudsters to illegally access the company's systems.

7.1.2.7. Create or participate in social media channels/groups that bears the EMAPTA brand or trademark but are not administered by any authorized personnel from the Company.

7.1.2.8. Disclose the names of employees' colleagues on social media unless they have given consent

7.1.2.9. Disclose personal contact numbers on public social media platforms to represent Emapta unless employees have been given authorization to represent the company.

7.1.3. Employees should be responsible in reviewing their content before posting or engaging with others online.

7.1.4. Note: If employees have other concerns or questions regarding proper social media usage, they can reach out at social@emapta.com.

8. SOCIAL MEDIA MONITORING

8.1. The Company reserves the right to monitor social media activities related to its brand and employees to ensure compliance with this policy. Monitoring may include reviewing public posts, comments, and interactions that could impact the Company's reputation or security.

9. SOCIAL MEDIA USAGE DURING COMPANY EVENTS

9.1. During Company-sponsored events or conferences, employees are expected to adhere to this policy when posting about or representing the Company on social media platforms. Guidelines for appropriate content and disclosures apply to maintain consistency and professionalism.

10. DOCUMENTATION AND COMPLIANCE

10.1. Employees must adhere to all related Company policies, including those prohibiting harassment, discrimination, and retaliation. Any confidential information must be handled according to the Company's confidentiality agreements and data protection laws.

11. POLICY REVIEW

11.1. This policy will be reviewed annually or as necessary to ensure its relevance and effectiveness. Updates will be communicated to all employees and relevant parties.

12. EFFECTIVITY

12.1. This policy is effective immediately upon approval and will remain in effect until modified or rescinded by the Company.

POLICY/PROCESS OWNER:	**Information Security Manager**
DOCUMENT CONTROL NO.:	**EVSI.ITD.25.00PM**
EFFECTIVITY DATE:	**June 2024**

	NAME / DESIGNATION	DATE
AUTHOR	**Jappy Damaso – Information Security Manager**	**June 2024**
REVIEWED	**Luis Sicat III – Chief Information Security Officer (CISO)**	**June 2024**
APPROVED	**Henry Vassall Jones – Chief Information Officer (CIO)**	**June 2024**

REVIEW AND REVISION HISTORY

DATE:	ACTION	Control No. (for Revision)	DESCRIPTION / COMMENT
August 2021	*Created*	*1.0*	*Social media is created.* *-Justin Arrojado-*
June 2023	*Reviewed and updated* *Template updated*	*1.1*	*Transferred document to official template. Made minor adjustments within the policy to safeguard against vishing and smishing; focused on secure use of social media.* *-Justin Arrojado-*
June 2024	*Reviewed and updated* *Template updated*	*1.2*	*Reviewed and updated sections social media monitoring and social media usage during company events.* *-Shihani Punchihewage-*