

Policy regarding organization tools

Version 1.0

Article 1. Introduction. Each volunteer classified as member of the organization pursuant the Section 4.01(C) of the Bylaws of Open Source Matters, Inc. might be granted an access to one or more tools provided and or operated by the organization to fulfill his/her responsibilities as Project member.

Article 2. Purpose of this Policy. This organization policy aims to reduce the security and business risks and to let users know how they are permitted to use organization tools.

Article 3. Scope of the Policy. This policy applies to all organization members pursuant Section 4.01(C) of the Bylaws and contributors. It applies no matter where that email use takes place. It applies to use of organization tools (as defined in the Article 4) on any device.

Article 4. Tools. The organization uses different tools and software, including, but not limited to, desktop software, web-based software, web applications, cloud-based services like mail, storage platform, real time communication services (i.e. Gmail, GSuite, Glip, Quickbooks, etc.).

Article 5. General tools guidelines. The organization encourages its members and contributors to use provided tools whenever appropriate. For instance allowed usage includes: communicate with other members/contributors (i.e. through email, instant messaging or videoconferences), work/collaborate with other members and stakeholders on project materials (i.e. team documents, project documents, collaborated folders).

Article 6. Unauthorized use. Any of the project tools (i.e. email account, software license, chat system) shall not be used for personal reasons and for non-project related activities. Any usage of the tools that is not related to the project may affect the services availability for the other project users and activities, so it shall be considered as unallowed and unauthorized.

Article 7. Tools Security. Used inappropriately, tools (especially online) can be source of security problems for the organization. Users shall not:

- 1) Open email/messaging attachments from unknown sources as they might contain a virus, trojan, spyware or any other kind of malware.
- 2) Disable eventual security or malware prevention software or feature as they are essential to protect from security issues, threats, frauds.
- 3) Send and or disclose confidential data of the organization.
- 4) Access another user's organization account (i.e. email account, service profile, messaging account, etc.).

Article 8. Inappropriate Contents/Usage. Any of the organization tools, including but not limited to communication systems (i.e. Email, Glip, Chat), must not be used to send or store inappropriate content or materials. It is important members and volunteers understand that viewing, storing or distributing inappropriate content via the organization tools is not acceptable under any circumstances. Users shall not:

- 1) Write or send emails or messages that might be defamatory or incur liability for the organization.

OpenSourceMatters

- 2) Create or distribute any inappropriate content or material through any of the provided tools. Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs. This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- 3) Use tools for any illegal or criminal activities.
- 4) Send offensive or harassing emails, messages or materials to others.
- 5) Create or distribute messages or materials that could damage the organization's image or reputation.

Any user who receives or detects messages or materials they consider to be inappropriate should report this to any of the Officers of the organization.

Article 9. Copyright. The organization respects and operates within copyright laws. Users may not use company email to share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.

Members and contributors must not use the organization's tools to perform any tasks that may involve breach of copyright law. Users should keep in mind that the copyright on letters, files and other documents attached to emails/messages may be owned by the email sender, or by a third party. Forwarding such materials on to other people may breach this copyright.

Article 10. Termination. Any access to organization tools (including email, chat and services accounts) shall be revoked or removed upon the membership termination or if the user is not anymore an active contributor to the project.

Article 11. Policy Enforcement. The company tools are provided for legitimate business use. The organization therefore reserves the right to investigate the usage of provided tools upon violation report or suspicious usage detection. Any such investigation will only be carried out by Department Coordinators or Officers of the organization.

Any breaches of this policy might result in a disciplinary action, up to the termination of membership or the deactivation of the user account in any of the organization tools.

Article 12. Order of Precedence. In case of conflict between provisions of this Policy, the order of precedence for conflict resolution in descending order shall be as follows: (i) Bylaws, including amendments; (ii) and (iii) the Policies.

This policy has been adopted by the Board of Directors of Open Source Matters, Inc. with the motion #2018-011 on February 01, 2018 and is published under the Policies section of the organization's website.