OpenSourceMatters

Secure Data Management Corporate Policy

Version 1.0

Article 1. *Introduction*. Open Source Matters operates several websites and services and has access to third-party software and services. Identities, login details, passwords, server information, software licenses, product keys and other information that are crucial to the operations of the corporation shall be managed centrally, securely and through proper access rights.

Article 2. *Purpose of this Policy***.** This Corporate Policy aims to provide the foundational guidelines and rules on how to manage sensitive corporate data.

Article 3. *Scope of the Policy*. This policy applies to all the sensitive access data, like website master accounts, FTP credentials, VPN connection information, extension website login details, SSH keys, product keys, software licenses and any other credentials.

Article 4. *Credential Vault*. The Full Board of Open Source Matters shall identify a software or a service to be used as a central repository for credentials. This centralized repository shall be defined as the Credential Vault and shall satisfy all the requirements in terms of security, uptime, access control and logs.

Article 5. *Requirements*. Every member of the Corporation who has been authorized to manage sensitive access data shall act according to this Policy.

Article 6. *Principles & Responsibilities*.

a) Each Department Coordinator shall be accountable and responsible for the usage of the Credential Vault by all teams and members within their respective Departments.
b) Each Department Coordinator shall lead by example, using the Credential Vault in an appropriate manner and storing all the sensitive information in the system.
c) Each Department Coordinator shall be responsible for the enforcement of this Corporate Policy within their respective Departments.
d) Each Department Coordinator shall be responsible to periodically review and update the access of the Team Members and Leaders within their respective Departments.
e) Each Team Leader and Assistant Team Leader shall be responsible for their own team specific Credential Vault (if applicable / available), using it in accordance with this Policy and ensuring that only relevant people from their teams have the appropriate access to the Credential Vault.
f) Each Team Leader and Assistant Team Leader shall report any irregularities or confidentiality breaches to their Department Coordinator in a timely manner and copying the Secretary of Open Source Matters.
g) Each Team Member shall use their access to the Credential Vault in accordance with this Policy and in a professional manner.
h) Each Member of the Corporation shall store organizational reserved data only in the Credential Vault.
i) All the information stored in the Credential Vault shall be under a Non-Disclosure Agreement (NDA) and shall be considered as confidential property of Open Source Matters, Inc.

Article 7. *Order of Precedence*. In case of conflict between the 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 #2020-37 on March12, 2020 and is published under the Policies section of the organization's website.