Mindbridge Virtual Asset Usage Policy

V.1.0
Last revised: 2 November 2020

I. Introduction

The Mindbridge Foundation (“Mindbridge”) establishes this policy to lay out management, and acceptable usage of virtual assets and platforms under its, or a project’s, possession.

This policy shall be administered by the Mindbridge IT Administrator (“Chief IT Administrator”), as appointed by the Mindbridge Board. In their absence, the Mindbridge Board of Directors (“Board”) or any person(s) designated by the Board (“Designee”) shall act as the enforcing body. For the remainder of this document, Chief IT Administrator refers to the appointed individual, Board, or Designee as appropriate.

Each project with an online presence will have an appointed IT Administrator. Multiple roles will be administered by an individual project’s IT Administrator (“Project IT Admin”).

II. Project Expectations of Virtual Assets

All virtual assets (eg. social media accounts, cloud storage repositories, websites, etc.) must have a maintained virtual keyholder vault. Maintenance of this virtual keyholder vault is the responsibility of the Project IT Admin, and access will also be granted to the Chief IT Administrator. The Project IT Admin is expected to maintain the virtual keyholder vault in such a manner that it can be easily transferable to future project executives or leads.

For shared accounts of each project, the virtual keholder vault will contain the following:

- Platform for account usage.
- Purpose of account.
- Credentials (Username & Password).
- User(s) who have been issued credentials and date received.
- Dates of audit approval (for accounts issued for more than one consecutive year).
- Contact information for the authorized user(s)

For personal accounts of each project, the virtual keyholder vault will contain the following:

- Account Platform.
- Username.
- Date issued.
- Contact information for authorized user.

All passwords for shared accounts must be reset on a regular timeframe by the Project IT Admin, as designated by the project executives or lead. At the time of password reset, all authorized individuals must be contacted and given the new credentials.

If Project IT Admin is unavailable, the Chief IT Administrator may be contacted by a pre-authorized user, but the Chief IT Administrator may not issue passwords to any users not already authorized by the Project IT Admin.

For financial accounts, the virtual keyholder vault can contain the username and contact information for password holders, but passwords MUST NOT be stored within the vaults. These passwords are the responsibility of the appropriate treasurer.

An individual project's executives or lead, as well as its Project IT Admin may create additional rules and bylaws dictating the usage and expectations of project virtual assets, so long as they do not conflict with those directed in this document. A copy of those additional rules and bylaws should be sent to the Chief IT Administrator.

III. Audit

The Project IT Admin is responsible for performing an audit of all shared account authorizations at the time of password resets. Any authorizations that were issued more than one calendar year prior must be approved by the current project executives or lead.

The Chief IT Administrator is responsible for a regular audit of each project's virtual keyholder vault, to ensure that proper maintenance and usage is being practiced. Activity to be performed when improper maintenance or usage is found are defined below under Enforcement.

Prior to the beginning of each fiscal year, the Chief IT Administrator is responsible for issuing a current state of each project's virtual keyholder vault to the Board.

IV. Enforcement

The Chief IT Administrator shall be responsible for executing and enforcing this policy, in coordination with the Project IT Admins. Should there be a security breach or violation in the policy, it is left to the Project IT Admins to act appropriately and in a timely fashion first. If the Project IT Admin is unable to respond in a timely fashion, then the Chief IT Administrator may step in to secure any breach or prevent any further violations in the policy.

Should a Project IT Administrator fail in their duty to communicate to the Chief IT Administrator regarding the state of the virtual keyholder vaults, or otherwise fail to carry out their tasks, then the Chief IT Administrator shall inform the Mindbridge Board of these issues, with the Board directing the appropriate project executives or leads on a recommended course of action. Should the Project IT Administrator be in serious dereliction of their duty, then the Board shall

be empowered to remove that Project IT Administrator and direct the Chief IT Administrator and the project executives or leads to find a new Project IT Administrator.

V. Appropriate Usage of Virtual Assets

Any usage of Mindbridge Virtual Assets in any illegal, inappropriate or defamatory manner is strictly prohibited, activity in this manner will result in immediate removal of authorized access, and possibly further sanctions as determined by the appropriate bodies.

None other than the Chief IT Administrator or Project IT Admin shall change the passwords on any mindbridge virtual asset, unless otherwise authorized by the Board or project executives or lead. Exception to this is for personal accounts, which may be changed at the discretion of the individual holder of said account.

Additionally, no Mindbridge Virtual Asset may be used in a manner to generate personal profit unless specifically authorized by the Board and Treasurer. Exceptions to this can be made for cases of charitable giving, with authorization from the appropriate project executives or lead.

Other usage guidelines for virtual assets shall be defined in each individual project’s rules and bylaws.