HOW-TO – MANAGE YOUR PASSWORDS

This How-to applies to all CartONG's staff, interns, service civiques, board and individual consultants.

General
1/ The use of Bitwarden as a password management system is mandatory
2/ Shared accounts are prohibited.

I. What is a secured password?

To be secured, a password should be difficult for a computer program to hack. Passwords have:

- To be **long enough** (min. of 12 characters)
- To be **complex** (i.e. using special characters, figures, upper and lower cases, etc.)
- To NOT be **easily identifiable** (e.g. not based on a date such as birthday)
- The same password shouldn't be used **twice** and passwords need to be **changed** regularly

To test the strength of your passwords you can use: http://www.passfault.com/

⚠ In case of a password provided or managed by a partner is not following the above rules, the partner need to be inform at least once in writing by the PM.

To generate highly complexed passwords, different solutions exist such as:

- **Every time that is possible: use a non-human-generated password.** The web application, mobile app and browser extension of Bitwarden are offering such a service.
- **Use passphrases** such as "Myst!fyFrostlike07DisorderChessReverse15Portal", **use the first letters of each word in a given sentence** (W@yft%10lra? for "Where are you found these ten lovely red apples?"), use a **schema on your keyboard,** etc.

II. Other general password management rules

All staff have to use Bitwarden as the password management system to store **ALL their professional passwords** (individual ones, shared ones, passwords shared by partners, etc.).

⚠ Password systems offered by browsers such as Chrome, other password managers, storing passwords on Google Sheets, or written them on notebook etc. are therefore prohibited.

It's requested of CartONG's staff to check the quality of their passwords at least once a year:

- **Check that your professional email address(es**) have not been **comprised in a data breach** with https://haveibeenpwned.com/ or https://monitor.firefox.com/.
- **Check that the passwords that you are using have not been exposed**. To do so, go to your Bitwarden Vault > Tools > Reports > Exposed password reports.
- **Check that you're not using weak passwords** (through Bitwarden same as above)
- **Check that you're not using the same password twice** (through Bitwarden)

III. Shared accounts

Shared accounts and shared passwords are generally prohibited. Excepted when:

- **The system / application for which the account has been created** doesn't contain "data to protect' (e.g. platforms used to submit a proposal, watch news, access to a map portal containing only base maps, platform used for CartONG purchase etc.)

- **The system / application doesn't allow the creation of individual accounts to access the same information or perform the same actions** (e.g. some MDC tools for instance) **or the partner refuse to use such account**. Such a situation should be described AND justified in the data controller / processor register by the PM.

IV. Email to create account

When needing to create a new account, you are required to use your CartONG professional email address (or the one provided by the partner).

⚠ It's not allowed to use an address outside of the cartong.org domain (Gmail, Yahoo, etc.).

V. Sharing a password

You may be required to share a password; i) either exceptionally when a shared account is used or ii) when you have to send a password following the encryption of data / documents

V.1. Within CartONG or with a "close" partner (who has Bitwarden account)

All passwords have to be shared within CartONG with Bitwarden without exception.

V.2. Outside of CartONG

Sharing passwords outside of CartONG should follow three rules:

1. **Only if necessary** (i.e. there is no other way for the partner to access the tool/data, such as creating a new dedicated account)
2. **Through a secured i.e. encrypted channel and with caution**

⚠ Sharing a password by email is therefore fully prohibited. SMS should also be avoided.

3. To always be done through **a different channel that with which the ID / link or the protected dataset has been shared**. *You can for example share the ID of the account by Skype and the password by a mobile app such as Whats app or more ideally Signal.*

To do so the following tools are recommended:

- **Framabin -** https://framabin.org/p/. You have to select the following options **"burn after reading"** and expires date should be maximum "a day" for a password (if possible select one hour). The generated link could then be shared ideally by using an encrypted message application (see below), or, if not possible, by email.
- **Using a messaging application**: ideally use Signal: https://www.signal.org/

⚠ You must ensure that you systematically delete the message that you sent, once it has been received (and read) by your recipient.

⚠ If you had no other choice that sending the password by email or by using WhatsApp or Skype, **please refer to the Policy – Password management.**

VI. Receiving a password

The same solutions/advice than detailed above could be suggested/requested from a partner who needs to share a password with CartONG.

💡 If you've received a password by email or by any other unsecured channels, it's your responsibility to alert the partner that such a practice is not recommended, and that more secured solutions exist. After having stored the password in Bitwarden, destroy the email and clean your trash folder.