

Passwords and Mobile Devices Protocol

Approval: Kfir Pravda **Approval Date:** 2025-09-25 **Protocol Type:** Public-Unlisted **Document Status:** Reviewed

PassWords and Mobile Devices Protocol

Responsibility:

As defined by the C.E.O of Pravda Media Group ("PMG").

Date of update:

18 Sep 2025 (Itzhak Wolkowicz)

5 May 2020 (Benny Akler)

Protocol

1. The purpose: To keep systems and mobile devices used in Pravda Media Group (PMG) safe from outside interventions and provide guidance to Password usage in and.

Definitions:

"Password": A string of characters used to verify the identity of a user during the authentication process. Passwords are typically used in conjunction with a username; they are designed to be known only to the user and allow that user to gain access to a device, application or website.

"IT Manager": An individual that is responsible for IT and IT security measures.

'Personal Data': Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

'DataBase': Any D.B. that contains 'Personal Data'.

"Breach": Any 'Personal Data' leaked by doings or by outside personal doings. Not all leaked data is a breach. Only personal data leaked will be considered as a breach.

"Authorised personnel": Personnel defined by the C.E.O of PMG to have access to personal data.

"Teamwork": Secured communication tool.

"Device": Any device that is by wire or wireless and using internet/ cloud to connect to systems used in PMG with any kind of access to a D.B..

"Personal receiving A D.B."": Any employee of PMG with contact with the client that gets a D.B. from the client ("receiving party").

"D.B. received form": Form sent to client to fill with details about the D.B..

"D.B. Documentation form": Form filled with details send to the "IT Manager" so he will be able to document and organize all stored D.Bs.

"1PassWord": "1Password" is a password manager. It provides a place for users to store various passwords, software licenses, and other sensitive information in a virtual vault that is locked with a guarded master password.

"2FA": 2FA (Two-Factor Authentication) is a security method that requires users to provide two different forms of identification to access an account or system, typically combining something a user knows (like a password) with additional authentication method a user possesses (like a smartphone app, SMS code, or hardware token).

Single Sign On (SSO): an authentication method that allows users to access multiple applications or systems with just one set of login credentials. Instead of remembering separate usernames and passwords for each system, users authenticate once and gain access to all authorized applications without needing to log in again. This streamlines the user experience by reducing password fatigue and improving productivity. SSO also enhances security by centralizing authentication control and reducing the risk of weak or reused passwords across multiple systems. PMG preferred method of authentication is using "Sign in with Google" SSO mechanism using the Google Workspace account. Passwords are only set as a preferred authentication method where SSO is unavailable.

General:

All systems used in PMG will be "guarded" by Passwords and also 2FA methods (where available).

All devices in PMG will be protected and locked.

The mobile devices will have encryption and remote locking capability

Passwords will be given by the IT Manager and on a "need to know" only.

All devices and systems will have password locks.

All devices and systems will be locked while not being used.

All devices and systems will have an automatic lock when not used. The time to activate the lock will be determined by the IT Manager.

This protocol will show the Pravda Media Group (PMG) employees the ways of handling Passwords and keeping all systems and devices safe from any security incidents.

PMG, As part of her regular work is using online systems and local devices.

These systems and devices should be used only by authorized personnel only.

Passwords are the most basic way for controlling access to online tools or for local devices and tools.

The use of strong passwords and their secrecy is therefore vital in order to protect the organisation's and individuals' security and identity.

All employees of PMG will use the "1Password" tool for generating passwords and keeping them on the relevant devices.

The method:

1. The IT Manager will have log of all passwords activities related to D.B's.
2. The IT Manager will follow the employee onboarding protocol
3. Once every half a year on a random date the IT Manager will change all passwords in PMG.
4. All devices with access to D.Bs will be "guarded" by a password.
5. The IT Manager will set a password to any system that is used by any employee is responsible to assure that his/her mobile device is updated to the latest OS and security updates.
6. 'Personal Data' will not be stored directly on PMG issued laptops (local, but only in the cloud). Locally processed personal data is permitted, upon need and approval from IT manager - up to 24 Hours on a local device, which is then deleted and reported to the IT manager.
7. Personal Mobile devices **will not** be used for any connection related to PII from client Databases.
8. Once every half a year, the IT Manager will have a meeting with all PMG personal explaining the security hazards and the Data security Breach protocol and the ways to prevent such hazards.
9. The IT Manager training will be about the ways to use passwords in the right way:
10. Choosing the Best Passwords:
 1. Do:
 1. Always use a password.
 2. To create a strong password, simply choose three random words. Numbers, symbols and combinations of upper and lower case can be used if you feel you need to create a stronger password, or the account you are creating a password for requires more than just letters.
 3. There are alternatives, with no hard and fast rules, but you could consider the following suggestions: Choose a password with at least eight characters (more if you can, as longer passwords are harder for criminals to guess or break), a combination of upper and

lower case letters, numbers and keyboard symbols such as @ # \$ % ^ & * () _ +. (for example SP1D3Rm@n – a variation of spiderman, with letters, numbers, upper and lower case). However, be aware that some of these punctuation marks may be difficult to enter on foreign keyboards. Also remember that changing letters to numbers (for example E to 3 and i to 1) are techniques well-known to criminals.

4. A line of a song that other people would not associate with you.
5. Someone else's mother's maiden name (not your own mother's maiden name).
6. Pick a phrase known to you, for example 'Tramps like us, baby we were born to run' and take the first character from each word to get 'tlu,bwwbtr'

Don't:

1. Don't Use the following as passwords:
2. Usernames, actual names or business name.
3. Family members' or pets' names.
4. Own or family birthdays.
5. Favourite football or F1 team or other words easy to work out with a little background knowledge.
6. The word 'password'.
7. Numerical sequences.
8. A single commonplace dictionary word, which could be cracked by common hacking programs.
9. When choosing numerical passwords or PINs, do not use ascending or descending numbers (for example 4321 or 12345), duplicated numbers (such as 1111) or easily recognisable keypad patterns (such as 14789 or 2580).

Looking After Your Passwords

1. Never disclose your passwords to anyone else. If you think that someone else knows your password, change it immediately.
2. Don't enter your password when others can see what you are typing.
3. Use a different password for every website. Don't recycle passwords (for example password2, password3).
4. The routine changing of passwords is not recommended, unless the accounts to which they apply have been compromised, in which case they should be changed immediately.
5. An alternative to writing down passwords is to use an online password vault or safe.
6. Do not send your passwords by email.