6 BASIC RULES FOR A GOOD PASSWORD POLICY

aka *How to setup a safer organization by IT departments*

01.

DEFINE THE POLICY IN AN EASY-TO-UNDERSTAND FORM

Document the password policy so that it includes all the important information – such as length of the password, complexity as well as acceptable unsuccessful login attempts.

02.

FORCE RESPECTING THE POLICY ON ALL LEVELS

All employees are to follow the company password policy. This includes the owners as well as top management and board members, without exception.

03.

BLACKLISTING BAD PASSWORDS

Create a "blacklist" of the most commonly used and/or previously compromised passwords and reject all attempts to use them.

04.

STORAGE OF USER PASSWORDS

Store the user passwords as salted hashes, and use a hashing algorithm specifically designed for password storage.

05.

CHANGING PASSWORDS NOT TOO OFTEN

Periodic password expiration is no longer an advised security practice. NIST as well as the UK National Cyber Security Centre (NCSC) now recommend changing passwords only in case the subscriber requests it or there is evidence of a compromise. Users forced to change their passwords too often will resort to using simpler and easy-to-remember passwords, or to adopting a trivial strategy such as adding a number or letter to the end of their password and then incrementing that at each change. Both approaches result in weaker protection of the company system.

06.

APPLY POLICY TO THE WHOLE NETWORK INCLUDING IOT

Password security policy should also encompass all passwords protecting the organization's devices and systems, especially IoT devices, such as security cameras, smart hubs and routers. If these are mismanaged or are used with default credentials, there is an ever-growing risk that attackers will find and try to exploit this vulnerability.