Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Guideline on Password Security

Published: 2025-10-20

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT48-58/2025E-PDF
ISBN: 978-0-660-79022-0

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Ligne directrice sur la sécurité des mots de passe

Guideline on Password Security

On this page

1. Introduction

▶ In this section

1.1 Context

As the Government of Canada (GC) increasingly relies on digital technologies, it must continue to strengthen its defences against unauthorized access to sensitive data and information technology (IT) systems. Weak and compromised passwords are a leading cause of security breaches, and even strong passwords can be undermined by tactics such as keystroke logging and social engineering.

Research on breached passwords has provided valuable insights into user-generated passwords and informed new best practices in something you know or password-based authentication. Historically, passwords have been the primary form of authentication, but they should no longer serve as the sole mechanism. Users have often been compelled to create complex passwords, which has led to insecure practices. Poorly secured user accounts pose significant vulnerabilities, giving attackers potential footholds to compromise entire systems through methods such as phishing and social engineering. Although good password practices are vital, they are just one component of a comprehensive IT security strategy. To effectively protect GC assets, the GC requires an approach that ensures robust authentication measures while alleviating the burden on users.

1.2 Purpose and scope

The purpose of this guidance is to:

- establish best practices to securely manage passwords in the GC
- set out advice and direction for GC system owners to consider when implementing password-based authentication systems, whether they are used as the sole authentication method (not recommended) or in conjunction with a multi-factor solution

The scope of this guidance focuses on passwords for human users and does not apply to non-human entities, such as service accounts, which are not constrained by human memory or behaviour. For accounts that are administered digitally, automated systems should be used to frequently change long and complex passwords when appropriate.

1.3 Intended audience

This document is primarily for GC system owners and contains guidance for users within the GC.

2. Help users help you

▶ In this section

2.1 Favour length over complexity

Forcing users to create complex passwords that include lower-case and upper-case characters, a digit, and special characters was intended to lead to stronger passwords. It has, in fact, done the opposite. Struggling to remember a growing number of complex and expiring passwords, users often do the bare minimum to meet the GC's complexity requirements. For instance, one of the most common passwords is "password". To meet complexity requirements, an alarming number of users use "Password1" or "Password1!".

To help users create better passwords, GC system owners are encouraged to:

- disable or reduce complexity policies (for example, allow passwords to be in all lower-case characters and also allow upper-case letters and other characters to be used)

- require a minimum number of characters (at least 12) and encourage users to make their passwords as lengthy as they want, within reason (for example, 64 characters or fewer) [1]
- permit passphrases that use at least four or five random words to meet the minimum 12-character length requirement
- in Windows environments, consider having a 15-character minimum [2] to prevent weak local area network (LAN) manager password storage

Refer to Appendix B for recommended minimum password length for situations where some degree of password complexity is still required (for example, in legacy systems or because of technological limitations).

2.2 Eliminate password expiry dates

Forcing users to change their passwords regularly puts a significant burden on users and has little effect on security. Typical password validity periods do little to prevent password cracking and, once a password is cracked, an attacker still has ample time to exploit the system. Also, users tend to select weak passwords that differ only slightly and predictably.

GC system owners are therefore encouraged to require users to change passwords only when there is a good reason to do so, such when there has been a known or suspected compromise or a change in password policy requirements. Before enforcing password changes, system owners should consider how doing so affects users. If someone’s account is secure and meets all policy requirements, they shouldn’t be asked to change their password unnecessarily. Also, if there is a security concern, users must not reuse their old passwords.

2.3 Block-list certain passwords

Past breaches have revealed that an astonishing number of users use passwords such as “password” or “123456”. Block-listing (or blocking) passwords that are common or obvious, including Canadian-themed ones that use the name of a local hockey team or that appear in word lists from previous password breaches, can reduce the likelihood of a successful word-list attack.

When GC system owners use block-listing, they should make sure that systems tell users why a password is being denied when users try to select a block-listed password.

2.4 Provide a password manager

Password managers are applications that, at a minimum, store passwords securely. They can also, for example:

- generate strong, random passwords
- automate authentication by directly interacting with login prompts
- support populating common fields in forms such as name and address

Password managers are an excellent tool for helping users cope with password overload. They also promote the use of strong, complex passwords and discourage password reuse.

Although password managers offer many benefits, they also present many risks. The greatest risk is that, if they are compromised, all the accounts associated with the passwords stored in them are potentially compromised as well. In a sense, a password manager holds the “keys to the kingdom” for a user.

Refer to Appendix D for additional information.

2.5 Avoid or manage the use of shared accounts

Shared accounts are strongly discouraged due to the significant risks and operational challenges they pose. The primary issue is a lack of accountability: when a group shares the same credentials, it becomes difficult to determine which individual performed a specific action. This makes it challenging to investigate security incidents, as audit logs may not clearly identify the user responsible for particular activities.

If the use of shared accounts is unavoidable, and there is a compelling business justification for their use, stringent security measures must be implemented to mitigate the associated risks. For example, passwords should be rotated regularly or immediately whenever a member leaves the group. This ensures that former users no longer have access and reduces the risk of unauthorized access.

The frequency of password rotation should be determined by specific factors, including:

- the sensitivity of the asset being accessed
- the likelihood of former members attempting to access the authentication interface
- the turnover rate of group members

As an additional mitigating measure, consider using a security vault or password manager that can track and audit access to passwords after they are used.

3. Implement measures to counter online attacks

▶ In this section

Online password attacks happen when an attacker interacts with a system's login screen and inputs password guesses for one or more accounts. These attacks may be automated and may originate from multiple, distributed sources (for example, a botnet).

Measures to defend against online guessing attacks include the following:

- throttling
- lockout
- monitoring and risk-based authentication
- multi-factor authentication
- procedures do securely reset passwords

3.1 Throttling

Throttling limits the number of attempts that can be made to log into a given account in a given period of time. The Communication Security Establishment Canada's User Authentication Guidance for Information Technology Systems: ITSP.30.031 recommends a maximum of 100 attempts or fewer within any 30-day period.

When used with block-listing, throttling can render online password attacks largely ineffective.

3.2 Lockout

Lockout blocks access to an account after a predetermined number of incorrect password guesses. For example, a system might lock an account after 10 failed attempts.

A balance must be struck between the need to prevent an online guessing attack and the need to address the reality that legitimate users will, from time to time, type their password incorrectly.

3.3 Monitoring and risk-based authentication

Monitoring login attempts (for example, based on an Internet Protocol (IP) address and time of day) to detect anomalies is another way to prevent online guessing attacks.

Monitoring mechanisms should be able to detect the following:

- large numbers of failed logins on an individual account
- large numbers of failed logins across many accounts

Risk-based authentication can provide an adaptable response to monitoring by computing a risk score and applying authentication controls based on the score. Risk-based authentication can analyze an authentication attempt from an unusual IP address or at an unusual time, or both, and either apply additional controls such as asking a security question or simply deny access.

3.4 Multi-factor authentication

Multi-factor authentication (MFA) enhances account security by requiring at least two distinct authentication factors during the login process.

As computational power increases and offensive tools (including password-cracking software driven by artificial intelligence) become more sophisticated, MFA will be essential to maintaining strong security. Without MFA, passwords would need to be increasingly lengthy, creating a burden for users. Therefore, implementing MFA for all users across all authentication processes within the GC is strongly recommended to reduce the risk of account takeover and strengthen the overall security posture of the GC.

For more details, refer to Government of Canada (GC) Guideline on Multi-Factor Authentication (MFA): Technical Recommendations for Authenticators to Support MFA Within the GC Enterprise Domain.

3.5 Procedures to securely reset passwords

A procedure to securely reset passwords is critical to safeguarding user accounts and preventing unauthorized access. Any password recovery process, including SSPR (self-service password reset) must be at least as secure as the method(s) used to register the user if the password is the only authenticator used.

The following outlines considerations for resetting passwords via links sent by email versus procedures for security questions:

- email reset links:
  - emails reset links must be sent only to pre-registered and verified email addresses controlled by the GC
  - links should be time-sensitive and expire after a certain period to limit the window of possible misuse (5 to 10 minutes)
  - tokens generated must be unique, random and valid for only one use; a token should be securely stored and associated with the user's account
- security questions:
  - also known as knowledge-based authentication (KBA), security questions are no longer considered an acceptable method of authentication, and they should not be used; attackers can discover the answers to many questions, combined with the limited number of possible choices for those questions, resulting in an unacceptably high risk of successful exploitation by unauthorized individuals

4. Implement measures to counter offline attacks

▶ In this section

An offline attack happens when an attacker obtains the password database for a system and conducts an attack against stored passwords.

Because this approach circumvents the online attack countermeasures outlined above and gives an attacker access to greater computation power that permits, for example, many billions of guesses per second, an offline attack can rapidly expose numerous system passwords if system owners have not taken specific countermeasures.

Measures to protect against offline attacks include:

- hashing
- salting
- keyed hashing

Password length is of particular importance in protecting against offline attacks.

4.1 Hashing

“Hashing” is a way to turn information, such as a password, into a scrambled mix of characters that can’t be changed back. Passwords must never be stored as plain text. Systems must hash passwords using modern and approved hashing algorithms set out in the Canadian Centre for Cyber Security’s Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information: ITSP.40.111 (for example, Password-Based Key Derivation Function 2 (PBKDF2)).

Hashing is a one-way process, meaning it cannot be reversed to retrieve the original password. This characteristic makes it ideal for validating passwords because even if an attacker obtains the hashed password, they cannot use it to log in as the user.

However, attackers may attempt to crack or reverse-engineer passwords by:

- using lists obtained from previous security breaches
- using lists of words in dictionaries
- trying brute force attacks

Although the number of permutations can be vast, the low cost of high-speed hardware, the tendency of people to select common passwords, and cloud computing makes password cracking increasingly feasible.

To counteract this risk, systems should implement hash iteration to increase the computational cost for attackers per guess. A minimum of 10,000 iterations is recommended.

4.2 Salting

“Salting” makes a password more secure by adding extra random information to it before hashing it. The extra data is different for every user and helps stop hackers from using pre-made lists (called rainbow tables) to crack passwords. Because each salt is unique to each user (for example, by being based on usernames) and are randomly generated, it is significantly more difficult to crack large numbers of hashes, as the time needed increases directly with the number of hashes. If salting is not possible, it is even more important to use other countermeasures to keep passwords safe.

4.3 Keyed hashing

A further password storage protection measure is to combine the password with a secret key before hashing. A secret value (sometimes called “pepper”) can be used for all users alongside salting to provide an extra layer of security, making it more difficult for attackers to crack hashes in the event of a database breach. Unlike salts, which are stored in the database with the hashed passwords, the secret value is kept in a secure location, such as within the application itself or ideally in a secret vault or hardware security module.

In the event of a database breach, attackers may gain access to the salts and hashes but will not have access to the pepper. This added layer of protection significantly increases the difficulty of reverse engineering the hashes, as attackers would need to guess or discover the pepper. Consequently, this approach enhances security against offline attacks.

Keyed hashing is a technique where passwords are hashed using a cryptographic key that can be unique for each user or a group of users.

Although this measure is not available for all systems, it provides the highest level of password protection that is practically available.

5. References

1. Communications Security Establishment Canada, User authentication guidance for information technology systems (ITSP.30.031 v3), April 2018.
2. United Kingdom National Cyber Security Centre, Password administration for system owners.
3. United States, National Institute of Standards and Technology Special Publication 800-63-3, Digital Identity Guidelines: Authentication and

Lifecycle Management, June 2017.
4. Australian Cyber Security Centre, Passphrases, November 2017.
5. Robyn Hicock, Microsoft Identity Protection Team, Microsoft Password Guidance.
6. J. Bonneau, C. Herley, P.C. van Oorschot, and F. Stajano. Passwords and the Evolution of Imperfect Authentication. *Communications of the ACM*, Vol. 58, No. 7, July 2015), pages 78 to 87.
7. D. Florêncio, C. Herley, and P.C. van Oorschot. An Administrator's Guide to Internet Password Research, USENIX LISA, November 2014.
8. Open Worldwide Application Security Project, Password Storage Cheat Sheet. [Accessed: November 19, 2024]

6. Enquiries

For more information or for clarification of this guidance, contact ZZTBSCYBERS@tbs-sct.gc.ca.

Appendix A: Glossary

botnet

A collection of compromised computers or devices (bots) that run malicious applications without the user's knowledge by means of a command and control infrastructure.

hashing

A function that maps a bit string of arbitrary length to a bit string of fixed length.

phishing

An attempt by a third party to solicit confidential information from an individual, group or organization by mimicking or spoofing a specific, usually well-known brand, usually for financial gain. Phishers attempt to

trick users into disclosing personal data, such as credit card numbers or online banking credentials, which they may then use to commit fraudulent acts.

keyed hashing

A type of hashing that involves a secret key in the computation of hash value. Unlike standard hashing, which is deterministic and public, keyed hashing (example: HMAC – Hash-based Message Authentication Code) ensures both integrity and authenticity. It verifies that a message has not been altered and originates from a trusted source.

rainbow table

A precomputed table for reversing cryptographic hash functions, usually for cracking password hashes.

salting

A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.

spear phishing

Using spoof emails to persuade people in an organization to reveal their usernames or passwords. Unlike phishing, which involves mass mailing, spear phishing is done on a small scale and is targeted.

Appendix B: Password Complexity Equivalency

Although the preferred approach is to eliminate password complexity requirements in favour of enforcing a minimum password length of 12 characters, this is not always possible, particularly in legacy systems or

where there are technical constraints. In such cases, increasing password complexity can help improve entropy, a measure of how unpredictable and resistant a password is to guessing or brute force attacks.

Entropy increases when passwords include a diverse set of characters, such as upper-case and lower-case letters, numbers, and special symbols. However, complexity alone is not sufficient if the password follows common or predictable patterns. For example, “Password123!” appears to be complex but is easily guessed, offering low effective entropy.

To ensure strong password security, especially for passwords shorter than 12 characters, it is strongly recommended that they be randomly generated, ideally using a reputable password manager capable of creating high-entropy passwords that are both complex and difficult to guess.

Table B1 shows the minimum recommended password length for situations where some degree of password complexity is still required.

Complexity	Minimum password length
Upper-case and lower-case letters	10 characters
Alphanumeric characters	9 characters
Alphanumeric characters and special characters	8 characters

Appendix C: Password Guidance for Government of Canada Users

▶ In this section

Password length and complexity

Longer and simpler passwords are better than shorter and more complex ones.

“Password complexity” refers to the mixture of characters in a password. A password that contains only lower-case letters is not complex, but one that contains lower-case and upper-case letters, numbers, and special characters is complex.

On the surface, requiring users to use complex passwords strengthens passwords; however, because complex passwords are more difficult to remember, users often reuse passwords, which actually reduces overall security.

In addition, analyses of users’ passwords from past breaches show that users choose predictable patterns when they have to make a password more complex. For example, they will upper-case the first letter and use an exclamation mark as the last character.

Longer and less complex passwords, such as those composed of four or five random words, are therefore better. The extra length makes up for the reduced complexity, and the reduced complexity means that users can create passwords that are easier to remember.

When a simple, all-lower-case password is used, it should have at least 12 letters.

Password reuse

Past system breaches have given attackers access to over 3 billion passwords. These compromised passwords are a good starting point for password-guessing attacks. Users should therefore avoid reusing

passwords. A compromised password obtained from the breach of one system may open the door to breaching other systems.

Ideally, passwords should be unique to each system. At a minimum, users should not use the same passwords for their personal accounts and their GC accounts. Users should also consider using unique passwords for their most important accounts, particularly for accounts that are used to recover passwords.

Multi-factor authentication

Many systems now offer users optional MFA by, for example, sending a one-time code or a prompt to the user by text message or through an app. Using MFA can help prevent accounts from being compromised. Users are encouraged to use MFA, particularly when using untrusted networks such as the Internet. They should also consider using MFA for their personal accounts, such as Google, Apple, Facebook, LinkedIn and Twitter accounts, to help prevent their personal accounts from being used to devise spear phishing attacks against GC user accounts.

Password tips

The following tips can help users create and manage secure passwords:

- Use a passphrase. Passphrases are easier to remember and can be just as secure as shorter, more complex passwords.
    - Choose four or five randomly selected words (for example, “correct horse battery staple”).
    - Include words from another language (for example, “correct cheval battery staple”).
    - Try the Schneier scheme (for example, “I like to eat pizza every Thursday for dinner” becomes something like “IltepzevThfd”).

    - Don’t use common expressions, song titles or lyrics, movie titles, well-known quotations and so on.
- Give a possible password the “20-guess test”: would someone who knows the user well or has access to the user’s social media content be able to guess their password in 20 attempts? Don’t include personal details in passwords such as a birth date, wedding date or names of family members; such information can be easy to guess.
- Add complexity to a password as long as it is still memorable. In general, every additional character or word strengthens a password or passphrase.
- Use a password manager to generate a strong password (refer to Appendix D for guidance on password managers).
- Don’t use predictable techniques such as transposing “E” to “3” or “a” to “@”. Such techniques provide a false sense of security and are highly susceptible to automated guessing attacks.
- If complexity is required, don’t simply capitalize the first letter and use a punctuation mark (especially an exclamation mark) as the last character (for example, “password” becomes “Password!”). Passwords like this are easy to guess.
- Don’t use a season combined with the year as a password (for example, “Summer2018”). This a common password strategy, so such passwords are easily guessed.
- Don’t store passwords in plain text or as unencrypted text (for example, in a text document or notes app).
- Don’t use any of the password examples given above.

Appendix D: Guidance on Password Managers for Government of Canada

Users

Password managers are applications that, at a minimum, store passwords securely. They can also, for example:

- generate strong, random passwords
- automate authentication by directly interacting with login prompts
- support populating common fields in forms such as name and address

Password managers are an excellent tool for helping users cope with password overload. They also promote the use of strong, complex passwords and discourage reusing passwords.

Although password managers offer many benefits, they also present many risks. The greatest risk is that, if they are compromised, all the accounts associated with the passwords stored in them are potentially compromised as well. In a sense, a password manager holds the “keys to the kingdom” for a user.

Tips for using password managers:

- Don’t store GC passwords on personal devices.
- Only use password managers from reputable vendors.
- Use a password manager with MFA capability, if possible.
- Consider omitting your most important passwords.
- Never store passwords for privileged accounts.
- Select a master password for the password manager that is at least as strong as the strongest password stored in it.
- Be diligent in installing updates for the password manager.

Additional guidance is available on the GC Cyber Security Community GCxchange Site (accessible only on the Government of Canada network).

Footnotes

1 The use of “something you know” (such as a password or personal identification number (PIN)) as an activation factor for multi-factor authentication (MFA) is not covered in this guidance. Activation factor passwords are generally less reliant on length, meaning they may not require a minimum of 12 characters. However, they must still be protected against brute force attacks given that passwords are stored locally.

2 The recommendation of 15 characters is based on recommendations in Microsoft’s Passwords Technical Overview.

ISBN: 978-0-660-79022-0

Date modified: 2025-12-08

xx
yy