KEEPER®

Password Security for Public Sector Organizations

Researchers found 723 breaches containing .gov emails in 2023, an increase from 695 in 2022 and 611 in 2021. Password reuse rates for .gov users also increased in the last year, from 61 percent in 2022 to 67 percent in 2023.

Everyone knows "123456" is a bad password, and so are "admin" and "password." For a variety of reasons, you shouldn't use the same password for more than one account. When the screen pops up - "it's time to change your password" - many users don't have the energy to think of yet another password that's easy to remember. Because of this, they type in one that they've been using forever - and maybe it's even the same as the one used for their email or bank account.

This scenario doesn't just play out in homes, but also in offices – especially in government offices. A 2023 report released by cyber crime analytics company SpyCloud reported that password hygiene might actually be going down for people with .gov email addresses.

Weak passwords and reusing passwords are a security issue because if one account is compromised, the stolen credentials can potentially be used to access other accounts.

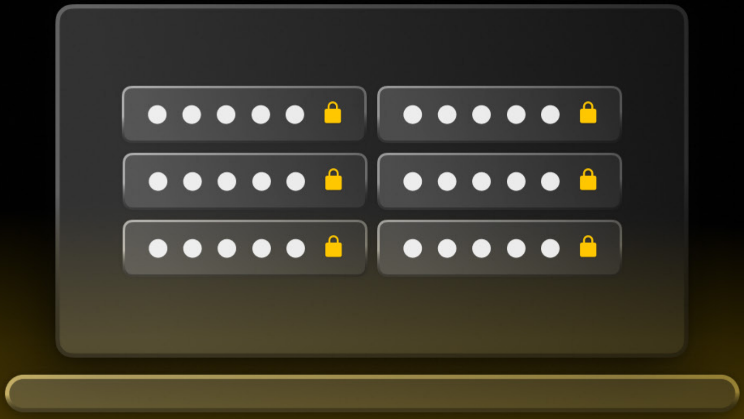
Cybercriminals search the dark web for breached account credentials and use techniques like credential stuffing and brute-force attacks to guess multiple passwords to gain access to accounts. Password reuse can lead to lateral movement within an organization's network. If an attacker is able to get in, they might start exploring other systems with higher privileges, attempting to access sensitive data, compromise accounts, install malware or launch additional attacks within the network.

Even large federal agencies are not immune from weak passwords.

> ***A 2023 audit published by the The Office of Inspector General found that over 20% of user passwords at the Department of Interior were able to be cracked using standard methods.***

Many of the passwords that were cracked included accounts with escalated privileges or belonging to senior government officials. Even though many passwords met the department's complexity requirements, they were still extremely easy to crack. So called "strong" passwords can still be compromised – especially when based on single dictionary words.

How to securely manage passwords

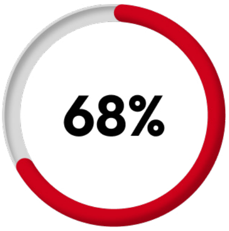


Passwords are often stored using insecure methods at all levels of government. Though it may seem harmless to keep passwords in a notepad file, Excel spreadsheet, email or even stored in a browser, none of these methods are secure. Passwords protect confidential records, network access and sensitive accounts – and password security is critical for every government employee.

This means that the password used for each and every account should be unique and complex. System administrators should have access to view the password health of the organization, without seeing the actual passwords. A password manager should provide an enterprise-level risk assessment showing which employees are using weak or reused passwords. Administrators should also have the ability to enforce complex password requirements.

Password security doesn't have to come at the expense of adoption. A password manager eliminates the need to remember dozens of passwords by providing a secure vault for each user to generate and store all their passwords. Users can autofill login credentials on websites and applications, on any device.

Some common ways credentials get stolen are through phishing attacks and public data breaches. Though all employees should be trained on phishing email scams, phishing emails are becoming more sophisticated all the time. Even if an employee clicks a malicious link, a password manager can differentiate between a fake website and a real one, mitigating the risk that employees reveal their login credentials. Some password managers can also send IT administrators notifications if an employee's login credentials appear in a data breach so they can prompt the employee to change their passwords.



of breaches involve the human element - with the majority due to stolen or weak passwords, credentials and secrets.

Secure password and file sharing

Employees at government organizations often need to share passwords and files. Without a secure sharing solution in place, they may be sharing sensitive information through spreadsheets, instant messaging or email. Email is generally not encrypted, making it possible for cybercriminals to intercept emails and attachments in transit. Sending sensitive information over email also risks the information being forwarded, saved or printed without the sender's permission.

Government employees may need to share the password for certain systems and accounts with other employees. For example, there may be one administrative password for an account that is used by several members of the finance team. Finance teams, in particular, log in to systems that contain sensitive information and any compromised credentials could lead to serious consequences, such as data theft and breaches.

Another example where there might be shared passwords within a team are collaboration systems that multiple people have access to. While these systems are especially helpful in today's distributed, hybrid workforce, these passwords should never be written down, nor should they be stored in spreadsheets, devices or emails.

The safest way to share passwords and files is via a secure password manager that offers multiple layers of encryption.

Password and file-sharing security becomes even more important when sharing information with third parties. One example of third-party file sharing in government is within court systems. A judge may need to share certain case information with an outside party, such as a defense attorney. With a secure file sharing system, a link is created that allows users to choose the amount of time that they wish to make a record available. The link is locked to one device, meaning a recipient can not forward the link or even open it on a separate machine.

Finance teams within government offices often need to share credit card information on a one-time basis to a vendor. A secure and time-limited one-time share option can be used in lieu of calling them with the number or sending it in an email.

A secure password manager with file-sharing capabilities gives system administrators complete control and visibility over employee usage and credential sharing. The entire organization benefits from each employee having an encrypted vault to store and share their work-related passwords, passkeys, files and more. They can share individual records, folders or share a time-limited secure record with anyone outside of the organization.

At the same time, administrators can restrict permissions, as necessary, and set up instant alerts when shared records are accessed or changed, allowing for on-demand visibility of access permissions on records and credentials across the entire organization.

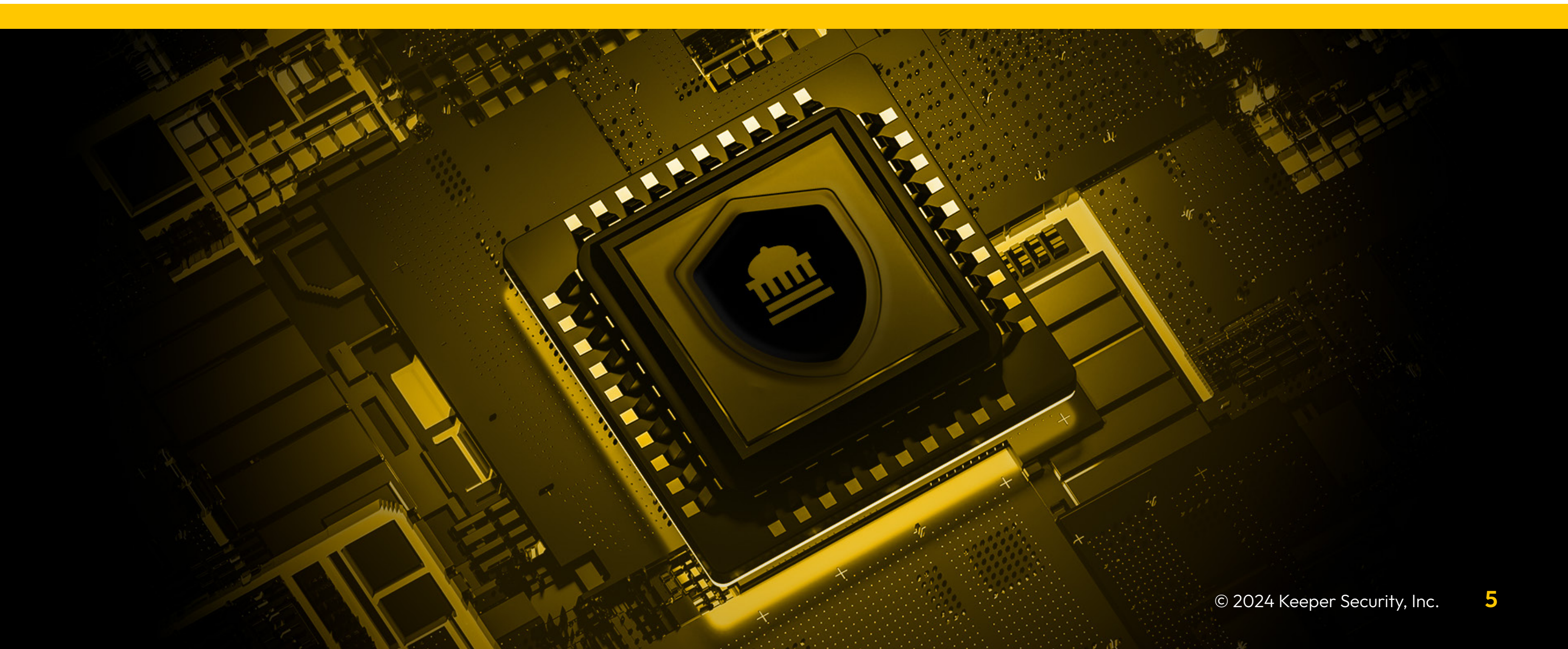
Government compliance and reporting

Government agencies must be in compliance with several security frameworks, including ITAR, SOC2, GDPR and ISO 27001. On the state level, cloud computing solutions must be StateRAMP Authorized. And on the federal level, in addition to utilizing FedRAMP Authorized cloud computing providers, agencies are mandated to adopt a zero-trust security architecture by September 2024.

With today's distributed, remote workforce, auditing access control policies is more important than ever. A password manager can streamline compliance monitoring and reporting by giving IT administrators full visibility and control over employee password usage and role-based, zero-trust network access throughout their data environments. Additional reporting features may include delegated administration, enforcement policies, event tracking and monitoring with customizable audit logs and event reporting.

Keep your organization compliant

- Get an overview of weak passwords, password reuse and Multi-Factor Authentication (MFA) usage
- Enforce least-privilege policies with granular role-based access controls
- Delegate administration by department or team leader
- Automatically revoke access when an employee exits the organization



Keeper Security Government Cloud for the Public Sector

Keeper Security Government Cloud (KSGC) password manager and privileged access manager is FedRAMP Authorized and StateRAMP Authorized. KSGC maintains the Keeper Security zero-trust security framework alongside a zero-knowledge security architecture, so users have complete knowledge, management and control over credentials and encryption keys.

- **Safeguard against ransomware attacks**
  Mitigate risks that lead to breaches by providing real-time protection and access to applications, systems, secrets and IT resources.
- **Save money and time with quick set-up**
  Easy, fast and affordable to integrate and deploy for organizations, departments and agencies of any size.
- **Powerful security insights**
  Provide analytics into credential security and hygiene across all endpoints and systems with native SIEM integrations.
- **Robust compliance and reporting**
  Simplify and strengthen auditing and compliance with support for RBAC, 2FA, FIPS 140-2 encryption, HIPAA, FINRA, SOC, ITAR and more.

Public sector organizations need a way to protect privileged accounts that is highly secure, easy to deploy and cost effective. Keeper's zero-trust and zero-knowledge Privileged Access Management (PAM) solution protects organizations of all sizes - from small municipalities and institutions to large state agencies and college campuses.

Ready to learn more? **Contact us.**

KEEPER®

Thank you for downloading this Keeper Security datasheet! Carahsoft is the distributor for Keeper Security solutions.

To learn how to take the next step toward acquiring Keeper Security solutions, please check out the following resources and information:

For additional resources:
carah.io/keeperresources

For additional Keeper Security solutions:
carah.io/keepersolutions

To set up a meeting:
KeeperSecurity@carahsoft.com
(703) 871-8548

For upcoming events:
carah.io/keeperevents

For additional Cybersecurity certified solutions:
carah.io/cybersolutions

To purchase, check out Keeper Security's contract vehicles available for procurement:
carah.io/keepercontracts