
[Policy](#) | [How To Change](#) | [Generators](#) | [Strength](#) | [Managers](#) | [Best Practice](#) | [Application Passwords](#) | [Encryption](#)

Welcome to the Password Policy Portal

A concise collection of modern password tips, tools, and resources for Riverview Health.

Riverview Policy

Although [PolicyTech](#) retains the complete and [official password policy](#), these guidelines will help you remain compliant.

Requirements

Domain passwords must meet these requirements.

- **8 characters** or more
- Change every **6 months**
- Contain **3 character types** or more:
 - **A-Z** uppercase
 - **a-z** lowercase
 - **0-9** numbers

Do

Good passwords are long, random, and unique for each service.

- Longer passwords are *much* stronger
- Use a unique password for every website and application
- Use a mix of letters, numbers, and symbols

Don't

Your password should be unique, known only to you.

- Don't share your password
- Don't accept passwords from others (e.g. do not login for someone else)
- Don't display or hide passwords near keyboards, monitors, mouse pads, unlocked desk drawers

- **!-?** punctuation
- May not include **your name**
- Securely store your passwords in a [password manager](#)
- Refrain from using your work passwords anywhere else

How to change your password

As you might expect, there's more than one way to change your password.

Ctrl + Alt + Delete

From within Windows (virtual or physical)

- Press Ctrl + Alt + Delete
- Select Change a Password
- Select your account
- Enter your current and new passwords

Outlook Web App

From within Outlook Web App.

- Log into <https://owa.riverview.org/>
- Select Options > Change Your Password
- Enter your current and new passwords
- Log off and back into Windows

Other Devices

Don't forget to update other devices. They will also need to know your new password if they are configured to retrieve your email or calendar.

- Your mobile phone
- Your tablet
- [iOS](#) and [Android](#) how to

Password Generators

Use these tools to help you create complex and random passwords.

Passed.pw

Example: **uuxvVSEM44:}%>#**

- Best option, but hard to remember
- Mobile keyboard friendly
- Avoids ambiguous characters

VISIT PASSED.PW

MX Toolbox

Example: **Exm!yzyz96**

- Good option, mixed complexity
- Easy, Stronger, and Very Strong
- 8, 10, and 14 characters

VISIT MXTOLBOX.COM

Diceware Wordlist

Example: **sown-cuff-chill-suey-&9**

- Reasonable, easy to remember
- Random words, several languages
- Add your capitalization or numbers

VISIT REMPE.US

Test Your Password's Strength

Use these tools to test the strength of your password. The best practice is to enter a test password that is similar to your real password (e.g. change a few characters, but keep the same length and character types). Make note that longer passwords are more difficult to crack.

HowSecureIsMy Password.net

Red background is bad; green is good.

Kaspersky Secure Password Check

Similar tool, different results.

- **91849217** cracked in 4 hours

GRC's Password Haystack

A security researcher's testing tool.

- **91849217** cracked in 0.025 seconds
- **QW2xTEQ-** cracked in 3 days
- **QW2xTEQ-ab** cracked in 58 years
- **QW2xTEQ-ab12** cracked in 344 thousand years
- **tea-hansel-serum-7** cracked in 43 trillion years

VISIT HSIMP TO TEST

- **QW2xTEQ-** cracked in 12 days
- **QW2xTEQ-ab** cracked in 58 years
- **QW2xTEQ-ab12** cracked in 4 centuries
- **tea-hansel-serum-7** cracked in 10,000 centuries

VISIT KASPERSKY TO TEST

- **91849217** cracked in 0.001 seconds
- **QW2xTEQ-** cracked in 19 hours
- **QW2xTEQ-ab** cracked in 58 years
- **QW2xTEQ-ab12** cracked in 1.7 thousand centuries
- **tea-hansel-serum-7** cracked in 4 trillion centuries

VISIT GRC.COM TO TEST

Password Managers

Password Managers help you securely store and access the unique and complex passwords you create for every website, applicaiton, and service.

LastPass

Our recommended solution, installed on every virtual desktop.

- Online, securtly stored in cloud
- \$0 for most features

Dashlane

Very similar to LastPass, though the premium service is more expensive.

- Online and offline modes
- \$0 for most features

KeePass

An offline Windows app, better suited for home and personal use.

- Open-source and free
- Not online, is an application

- \$12/year to sync to unlimited devices (like your smart phone)

[VISIT LASTPASS.COM](https://lastpass.com)

- \$40/year to sync to unlimited devices (like your smart phone)

[VISIT DASHLANE.COM](https://dashlane.com)

- Could be portable if installed on a USB stick

[VISIT KEEPASS.INFO](https://keepass.info)

Security Advice from Giants

Google, Microsoft, Apple, and many other companies manage many user accounts. Here's what they have to say about passwords and security, which is good advice for all.

Google

"Choosing the same password for each of your online accounts is like using the same key to lock your home, car and office – if a criminal gains access to one, all of them are compromised. So don't use the same password for an online newsletter as you do for your email or bank account. It may be less convenient, but picking multiple passwords keeps you safer."

Microsoft

"Passwords are the first line of defense against break-ins to your online accounts and computer, tablet, or phone. Strong passwords are phrases (or sentences) at least eight characters long (longer is better) that include at least three of the following: uppercase and lowercase letters, numerals, punctuation marks, and symbols."

[RE:PASSWORDS](#)[RE:SECURITY](#)

Apple

"Apple policy requires you use strong passwords with your Apple ID. Your password must have 8 or more characters and include upper and lowercase letters, and at least one number. You can also add extra characters and punctuation marks to make your password even stronger. Using a strong password is the most important thing you can do to help keep your account secure."

RE:PASSWORDS

RE:SECURITY

RE:PASSWORDS

RE:SECURITY

Application Passwords

Many of our applications are connected to Microsoft Active Directory and thus inherit the same username and password. Some applications, however, manage their credentials independently.

Apps synced with Active Directory

Same username and password.

- Allscripts Pro PM
- Citrix XenApp
- Cisco Finesse
- Kronos Workforce Central
- Microsoft Dynamics GP
- Microsoft Lync/Skype
- Microsoft Outlook

Apps not synced with Active Directory

Different username and password.

- Allscripts Pro EHR
- GE Muse
- McKesson Orsos
- Passport Health
- QuadraMed
- Soft Lab

App Password Change Process

How to change your password in some applications

Allscripts Pro EHR

- Log into Allscripts Pro EHR
- Click on your name in the top right corner
- Select Change Password

QuadraMed

- Optimum
- PolicyTech
- VMware Horizon View

- Launch QuadraMed CPR
- Type in your credentials on the Logon screen
- Select Change Password

Encryption

These tools are more for system administrators than for end users. Should you receive a link from IT to one of these services, it would be safe to click on it.

Out-of-Band

If you send the username via email; use IM or SMS to send the password.

- Don't send username and password via the same medium
- The second medium should just be a password (no username)
- Most mediums are unencrypted, like a postcard, which is why you use two

Temporal.pw or Dead-Drop.me

Securely send an encrypted password.

- Safer than sending an unencrypted password via email or instant message
- Link to password expires
- Link to password can be viewed only a few times

LastPass Premium

Lets premium users securely share passwords.

- Must be a premium (\$12/month) user
- Can share access to a site without revealing the password
- Best suited for friends and family

RE:LASTPASS SHARING

VISIT TEMPORAL.PW

VISIT DEAD-DROP.ME