RISE RACING

Harnessweb — Password Security Update

User Guide for State Bodies & Participants

Purpose of this guide

This guide explains the password security improvements recently made to Harnessweb, what they mean for users, and practical tips to help participants create and manage strong passwords with ease. Please share this guide with participants who may have questions.

1. New Password Policy

Harnessweb now enforces a strengthened password policy across all account flows. These changes ensure every account is protected by a genuinely secure password.

What has changed

All new and reset passwords must now meet the following requirements:

- Minimum 16 characters in length
- At least one uppercase letter (A–Z)
- At least one lowercase letter (a–z)
- At least one number (0–9)
- At least one special character (e.g. !, @, #, $, %)

Passwords will be rejected if they

- Contain the user's first name, surname, username, or email address
- Include obvious sequences such as 123456 or abcdef
- Use simple repeating patterns such as AAAAAA or 111111
- Are the same as the previous password
- Appear on Rise Racing's internal blacklist of known weak or compromised passwords

Where these rules apply

- New account registration
- Forgot Password / password reset flow
- Change Password (via Account Details while logged in)

2. Mandatory Password Reset & Expiry

To bring all existing accounts up to the new standard, a mandatory password reset and ongoing expiry framework has been introduced.

How the expiry process works

1	**7-day notice**	When a password is approaching its expiry date, users will see a Password Expiry Notice each time they log in during the final 7 days. This notification is presented as a pop-up banner displayed in Harnessweb upon login.
2	**User choice**	The notice explains the expiry timeframe and prompting the user Change Password.
3	**Expiry enforced**	If the password is not updated before the expiry date, login is blocked. The user must set a new compliant password to regain access.
4	**Resolved**	Once a valid new password is saved, the expiry notice disappears.

What this means for participants

Users will receive advance notice before their account is locked. Encouraging participants to act on the 7-day notice promptly will avoid any disruption to their access.

3. Screen Improvements

Several improvements have been made to the password entry screens to make the experience clearer and reduce errors.

Real-time inline validation

On all password entry screens (Registration, Forgot Password, and Change Password), users now see live feedback as they type. This means:

- Password strength is shown in real time
- Any unmet rules are flagged immediately
- Clear error messages explain exactly what needs to be fixed

Password visibility toggle (eye icon)

A show/hide password button has been added to the Password and Confirm Password fields on all key screens. Users can tap the eye icon to toggle between masked (••••••) and visible text, reducing the chance of typing mistakes on long passwords.

Clearer error messages for shared email accounts

If an email address is linked to more than one username, Harnessweb will not allow the users to login with their email address and now show a specific message directing the user to log in with their username (e.g. FirstNameLastName) or to contact their SCB. This reduces confusion for participants who share an email address across accounts.

4. Tips for Participants: Creating & Saving a Strong Password

The new 16-character minimum can feel demanding at first. The good news is that modern browsers make it easy to create, save, and auto-fill strong passwords without having to remember them. Below are practical tips to share with participants.

Option A — Use your browser's built-in password generator

Most modern browsers (Chrome, Edge, Safari, Firefox) include a free, built-in password generator and manager. Here's how to use it:

Google Chrome & Microsoft Edge

- Click into the Password field on the Registration or Change Password screen.
- A small key icon or 'Suggest strong password' prompt will appear in or beside the field.
- Click it to have the browser generate a strong, random password that meets all requirements.
- Accept the suggestion — Chrome/Edge will automatically save it to your Google or Microsoft account.
- On your next visit, the password will be auto-filled when you click into the Password field.

Apple Safari (iPhone, iPad, Mac)

- Tap or click the Password field.
- Safari will suggest a strong password automatically — look for the 'Use Strong Password' prompt.
- Accepting saves the password to your iCloud Keychain, available across all your Apple devices.
- Safari will auto-fill the password on future logins.

Mozilla Firefox

- Click into the Password field.
- Click the key icon that appears, then select 'Use a Securely Generated Password'.
- Firefox will save the password to its built-in Firefox Passwords manager.
- You can view saved passwords at any time via Settings > Privacy & Security > Saved Logins.

Tip: Make sure your browser is signed in

To access saved passwords across multiple devices (e.g. home computer and mobile), make sure you are signed into your browser with your Google, Microsoft, Apple ID, or Firefox account. Passwords sync automatically across devices when signed in.

Option B — Create a memorable passphrase

If a participant prefers not to use a browser manager, a passphrase is a great alternative. A passphrase uses four or more random words joined together, optionally with numbers and symbols added. For example:

> **`Example passphrase:  Purple!Rain42HorseBoots`**
>
> Four random words + a number + a symbol = 22 characters, easy to remember, very hard to guess.

Option C — Use a dedicated password manager

Password manager apps provide the most comprehensive solution, especially for users who manage multiple accounts. Popular, trusted options include:

- 1Password — highly recommended for ease of use
- Bitwarden — free, open-source, available across all platforms
- LastPass — widely used with a free tier available

These apps generate, store, and auto-fill passwords across any device or browser. They also alert users if a saved password has been compromised in a data breach.

NOTE: Participants are free to choose a password manager of their preference and should do so at their own discretion.

General password safety tips

- **Never reuse passwords.** Using the same password on multiple sites means one breach can compromise all your accounts.
- **Never share your password.** Rise Racing staff will never ask for your password.
- **Act on expiry notices promptly.** When you see the 7-day expiry warning, update your password that day to avoid being locked out.

- **Keep your email address current.** Password reset links are sent by email, so make sure your registered email is active and accessible.

5. Scope & Known Items

Harnessweb only

These changes apply exclusively to Harnessweb. Ontrack is not affected and its login behaviour remains unchanged.

Locked account recovery

An enhanced one-time password (OTP) verification flow for accounts locked after five incorrect password attempts is part of the broader security initiative and will be delivered in a subsequent release. Further guidance will be provided when this feature becomes available.

6. Frequently Asked Questions

Q: My current password is strong — do I still need to change it?

A: Yes. As part of the security overhaul, all existing accounts are required to reset to a password that meets the new rules. You will be notified 7 days before your current password expires, giving you time to update it before any access is affected.

Q: I missed the 7-day notice and my account is now locked. What do I do?

A: Use the Forgot Password link on the Harnessweb login page. You will receive a password reset email to set a new compliant password and immediately regain access to your account.

Q: I keep getting a message that my password is on a blacklist. What does that mean?

A: Harnessweb checks new passwords against a list of commonly used and previously compromised passwords. Even if your chosen password meets all the complexity rules, it may still be rejected if it appears on this list. Simply choose a different password — try a passphrase (see Section 4) or use your browser's built-in password generator for something that will always pass.

Q: I use the same email address for multiple Harnessweb accounts and I can't log in.

A: Where an email address is shared across accounts, Harnessweb will display a message instructing you to log in using your username instead (e.g. FirstNameLastName). If you are unsure of your username, contact your State Controlling Body (SCB) for assistance.

Q: Is it safe to let my browser save my Harnessweb password?

A: Yes. Built-in password managers in Chrome, Edge, Safari, and Firefox encrypt saved passwords and are considered secure for everyday use. For added protection, ensure your browser account (Google, Microsoft, Apple ID, or Firefox account) is protected with a strong password and, ideally, two-factor authentication.

Q: I'm not receiving the password reset email. What should I check?

A: Check the following before contacting support:

- Check your spam or junk mail folder.
- Confirm the email address registered to your account is current and accessible.
- Wait a few minutes and try again, as email delivery can occasionally be delayed.
- If none of the above resolve the issue, contact your SCB who can assist with account details.

Q: Will I need to change my password again in the future?

A: The password expiry framework is an ongoing behaviour. Once your password is updated to a compliant one, you will receive the same 7-day advance notice before it expires again in future. Keeping your password saved in a browser or password manager makes these periodic updates quick and easy.

7. Support & Contact

If participants have questions that cannot be resolved using this guide, they should contact their State Controlling Body (SCB). SCBs can escalate to Rise Racing support if required.

Need help?

Participants experiencing login issues or questions about their account should contact their State Controlling Body in the first instance. SCBs can refer to this guide or escalate to Rise Racing if needed.