Password recommendations

This document provides general recommendations for creating strong passwords, protecting passwords, changing passwords, and determining the frequency of password change. This information is intended for all staff members.

Choosing a strong password is a crucial step in preventing unauthorized access, compromised or lost data, downtime, and other negative events.

IMPORTANT: Although IDEXX has outlined the recommendations below, your practice is ultimately responsible for implementing a password policy and continuing to monitor the effectiveness of that policy.

General recommendations

- **Create a new password** for every new computer, device, or software application. Do not continue using the default password supplied by the vendor.
- **Create a policy** that all passwords must be changed regularly.
  - A typical requirement would be to change passwords every 30–90 days and after any suspected security event.
  - **Consider all passwords** when creating the policy (passwords for Windows* administrator, network equipment, software administration accounts, email, internet, desktop computer, etc.).
- **Do not store** any personal or sensitive information on your diagnostic imaging image-capture PC.
- **It is your practice's responsibility** to maintain all passwords. You may need to share passwords with IDEXX and other IT professionals to perform troubleshooting tasks. Any time you give a password to someone other than the user, the user should immediately change the password as soon as the troubleshooting task is complete.
- **All passwords should conform to the guidelines** described below.

Password creation guidelines

Strong passwords have the following characteristics:

- Contain at least **three of the four** following character classes:
  - Lowercase characters
  - Uppercase characters
  - Numbers
  - Punctuation and special characters (@#$%^&*()_+|~-=\`{}[]:";'<>/)
- Contain a **minimum of eight** alphanumeric characters, although **fifteen** is recommended.

Avoid the following characteristics when creating a password:

- Less than eight characters
- A word found in a dictionary (English or foreign)
- Commonly used words, such as:
  - Your name, names of family, pets, friends, coworkers, etc.
  - Computer terms and names, commands, sites, companies, hardware, software, etc.
  - The practice name or any abbreviation of the name
  - Birthdays and other personal information, such as addresses, phone numbers, social security numbers, driver's license numbers, bank accounts, or credit card numbers
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321
  - Any of the above spelled backwards
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

For additional guidance on creating a strong password, refer to the following article from Microsoft*:
support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb

Password protection standards

- If you suspect that your system is compromised in any way, you may need to report the incident to the authorities. Consult your local law enforcement agency because rules vary by state.
- Passwords must be safeguarded by your practice:
  - IDEXX will not store and will not have access to your passwords.
  - If a password is forgotten, IDEXX may not be able to restore access to your image-capture PC, which may lead to a service event and unexpected downtime for your diagnostic imaging system.
- Always use different passwords for workplace/business accounts versus nonworkplace/business access (e.g., personal financing, email, benefits).
- Always use different passwords for various access needs whenever possible. For example, select one password for user-level Windows* access and a different password for administrator-level access.
- Do not:
  - Reveal a password in email, chat, or other electronic communication.
  - Speak about a password in front of others.
  - Hint at the format of a password (e.g., "my family name").
  - Reveal a password on questionnaires or security forms.
- Always decline the use of the "Remember Password" feature of applications and websites (e.g., web-based email, ecommerce web sites, Microsoft* Outlook*).

Changing passwords

Networking devices, peripherals, and software

To change passwords and/or keys for the following devices or software, see the manufacturer's documentation. This documentation is typically included with the product or can be found on the manufacturer's website. Common examples include:

- Router
- Access point
- VetConnect* PLUS
- IDEXX-PACS* Imaging Software

Local Microsoft user accounts

Use the following link to learn how to change the password of a local user account:

windows.microsoft.com/en-us/windows/change-windows-password

Note: Workgroup computers should have a shared username and password.

Domain user accounts

Work with your IT professional or use the following link to learn how to change the password of a domain user account from the server: technet.microsoft.com/en-us/library/cc754395.aspx

Security resources

- Cybersecurity & Infrastructure Security Agency (CISA), Tips at: us-cert.cisa.gov/ncas/tips
- National Institute of Standards and Technology (NIST), Small Business Cybersecurity Corner at: nist.gov/itl/smallbusinesscyber
- Security.org, How secure is my password? at: security.org/how-secure-is-my-password