IDEXX Cornerstone*
Practice Management Software

Password Policy

Document Purpose	This document provides general recommendations for creation of strong passwords, the protection of those passwords, the frequency of change, and how to change passwords. The information in this document is intended for all staff members. Passwords are an important aspect of computer security. Security requires a multi-layered strategy and choosing a strong password is a crucial step in preventing unauthorized access, compromised or lost data, downtime, and other negative consequences. 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	• Each time you purchase a new computer, device, or software application, set up a new password. Do not continue using the default password supplied by the vendor. • Create a policy that all passwords are required to be changed regularly. A typical requirement would be to change passwords every 30 to 90 days and after any suspected security event. • All passwords (e.g., Windows® Administrator, network equipment, software administration accounts, email, web, desktop computer, etc.) should be considered when creating a password policy. • If a workstation is shared by multiple people, users should not store any personal or sensitive information on that workstation. • Use individual user names for IDEXX Cornerstone* rather than sharing a username between multiple people and follow the password creation guidelines below. • It is the responsibility of the practice to maintain their passwords and it may be necessary to present passwords to IDEXX and other IT professionals to perform troubleshooting tasks. Any time a password is given out to someone other than the user, that user should immediately change that 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:
	  o Lowercase characters
	  o Uppercase characters
	  o Numbers
	  o Punctuation and “special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.)
	• 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)
	• A common usage word such as:
	  o Your name, names of family, pets, friends, co-workers, etc.
	  o Computer terms and names, commands, sites, companies, hardware, software, etc.
	  o The practice name or any abbreviation for the name of the practice.
	  o Birthdays and other personal information such as addresses, phone numbers, social security numbers, driver's license numbers, bank account, or credit card numbers.
	  o Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321.
	  o Any of the above spelled backwards.
	  o Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
	
	For additional guidance on creating a strong password, please refer to the following article from Microsoft® http://www.microsoft.com/security/online-privacy/passwords-create.aspx.

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 need to be safeguarded by the practice. IDEXX will not store and will not have access to your passwords. • In the event that a password is forgotten, IDEXX may not be able to restore access to your computer or device, which may lead to a reload or reconfiguration. This process may be time-consuming for your practice and may be subject to our current billable rate. • Always use different passwords for workplace/business accounts versus other non-workplace/business access (e.g., personal financing, email, benefits, etc.). • Always use different passwords for various access needs whenever possible. For example, select one password for user-level Windows® access, a different password for administrator-level access, and a third password for logging into Cornerstone. • Do not reveal a password in email, chat, or other electronic communication. • Do not speak about a password in front of others. • Do not hint at the format of a password (e.g., "my family name"). • Do not 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, Outlook®).
How to Change Passwords	**Networking devices, peripherals and software** To change passwords and/or keys for these 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 • Accounting software **Local user accounts** Use the following link to change the password of a local user account: • http://windows.microsoft.com/en-us/windows/change-windows-password **Note:** Workgroup computers should have a shared username and password. **Domain user accounts** Follow the appropriate link to change the password of a domain user account. • To change the password of a user account from the server: http://technet.microsoft.com/en-us/library/cc754395.aspx • To change the password of a user account from a workstation: See the “How do I change my password when my PC is connected to a domain” section • http://windows.microsoft.com/en-us/windows/change-windows-password

IDEXX LABORATORIES

idexx.com/cornerstone