IDEXX Cornerstone*
Practice Management Software

General Security Guidelines

Document Purpose

Network security is essential for protecting client, patient and business information. The information provided in this document provides basic guidelines, not an all-inclusive list, because security is ultimately the responsibility of the practice and every business is different. IDEXX is NOT responsible for the security of your practice's computers, network and/or data.

Your practice is responsible for developing a strategy and plan, implementing the items identified and monitoring their effectiveness. IDEXX highly recommends working with a security professional to determine the appropriate security measures and practices that best fit your business based on your needs, your environment and your risk assessment.

An effective approach to security requires a multi-layered strategy, including but not limited to, educating and training staff, network security, keeping up to date with software and operating system updates and data security. The section below includes basic guidelines that can be used as a starting point.

Guidelines

Educate and Train Staff

- Educate and train staff on security best practices and how to recognize and remediate against perceived cyber threats.
- Implement a safe Internet browsing policy for your staff to follow.
- Implement a password policy. An example password policy can be found here: http://www.idexx.com/passwordpolicy
- Design and implement physical security protocols (e.g., equipment access, room access, building access)

Network Security

- Ensure a hardware firewall is setup at a minimum. If desired, a software firewall can be configured as well. For firewall configuration details specific to Cornerstone* functionality, view the Firewall Configuration Guide at: https://www.idexx.com/files/small-animal-health/products-and-services/practice-information-management/cornerstone-software/firewall-configuration-guide.pdf
- Ensure that all unnecessary ports are closed and remote management features are disabled in the router/firewall.
- If the practice has a wireless network, make sure that WPA2 security is enabled.
- If the practice has a remote access solution, ensure that a hardware VPN or other solution that uses two-factor authentication is in use. This also makes the remote access solution PCI compliant.

Software and Operating Systems

- Install antivirus/antimalware software and stay current with definition updates.
- Only use manufacturer supported operating systems and stay up to date with service packs, security updates and other updates.
- Stay current with version updates and security updates for software.

Data Security

- Using a credit card processing solution requires you to be PCI compliant, see PCI guidelines at: https://www.pcisecuritystandards.org/security_standards/index.php
- Use caution if storing any sensitive data on your system. Do not store sensitive data within Cornerstone.
- Ensure data backups are current.

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.

IDEXX LABORATORIES

idexx.com/cornerstone