IT Services

VetPoint Web Security Information

The new VetPoint Web allows easy access to all of the VTH electronic medical records from many different devices and many different locations. Because of this easy access to sensitive information, it is imperative to client data privacy that you take steps to secure your device. By following the steps below, you can limit the possibility of exposure of this sensitive data in the event your device is lost or stolen.

1.) Set a passcode or password on your device.
2.) Set a timeout period on your device that locks the screen if it is left idle.
3.) Utilize tracking and remote-wiping software solutions in the event your device is lost or stolen.
4.) Never leave your device unattended.
5.) Delete any attachments containing sensitive information from your device that are no longer needed.
6.) Do not leave your device logged into Vetpoint when not in use.
7.) Install an anti-virus program and keep it up to date.
8.) Always keep the operating system and other applications on your device up to date.

Recommended software and hardware specifications for VetPoint Web

The following instructions are meant for devices running the following operating systems:

- iOS: iPad running iOS7 or higher.
- Android: Android 4.0 or higher.
- Windows: Windows 7 Services Pack 1.
- Apple: Mac OSX 10.6 or higher.

1.) Set a Passcode or Password on your device.

You can use a passcode or password on your device to protect your data. Each time you turn on or wake up the device, it will ask you for the passcode or password before you can access the device.

- **iPad or iPhone:** Go to Settings and select Passcode Lock, select Turn Passcode On
- **Android Device:** Go to Settings, select Security, and select Screen Lock.
- **Windows:** Open Control Panel and select User Accounts. Click the Create a Password option.
- **Apple:** Open System Preferences, select Users & Groups, click the Change Password button.

2.) Set a timeout period on your device that locks the screen if it is left idle.

If you device is left idle, you can enable a feature that will lock your device and require your password to unlock it again.

- **iPad or iPhone:** Go to Settings, select Passcode, Select Require Passcode and select your time frame.
- **Android Device:** Go to Settings, select Security, select Automatically Lock and select your time frame.
- **Windows:** Open Control Panel, select Personalization, select Screen Saver, check the box "On resume, display logon screen and select your time frame.
- **Apple:** Open System Preferences, select Security & Privacy, check the box "Require password" and select your time frame.

3.) Utilize tracking and remote-wiping software solutions in the event your device is lost or stolen.

If your device goes missing, there are applications and services available to help recovery them or wipe the information from them remotely. Neither CVMBS nor CSU are liable for lost or stolen devices.

- **iPad or iPhone:** Go to Settings, select iCloud, slide the Find My iPad or iPhone option to the "On" position.
  If the device goes missing, go to any internet connected computer, navigate to iCloud.com, sign into your iCloud account and select Find my iPad or iPhone. Choose your missing device from the All Devices dropdown menu. You can now track your device's location or remotely erase your device.

- **Android Device:** Go to Google Settings on your device and select Android Device Manager. Enable both Remotely locate this device and Allow remote lock and erase options.
  If the device goes missing, go to any internet connected computer, navigate to Google.com/android/devicemanager, and sign into your Google account. You can now track your device's location or remotely erase your device.

- **Windows:** Most windows computers do not have a built in tracking function and will require a 3rd party application to track missing devices. Software such as LoJack for Laptops or Prey Pro can be installed and used to tracking missing devices. Please contact the IT Services Helpdesk for more information.

- **Apple:** On your device, Open System Preferences, select iCloud and check the Find my Mac Option.
  If the device goes missing, go to any internet connected computer, navigate to iCloud.com, sign into your iCloud account and select Find my iPad or iPhone. Choose your missing device from the All Devices dropdown menu. You can now track your device's location or remotely erase your device.

The College of Veterinary Medicine and Biomedical Sciences is not liable for lost or stolen devices and can only provide information regarding applications or services that can assist in the recovery of your device.

4.) Never leave your device unattended.

Computers are most vulnerable when the user is logged in and then leaves it unattended. It is possible for unauthorized access to applications to result in modification of data, fraudulent use of CVMBS

resources or theft. When leaving a workstation unattended, even if only for a few minutes, users should log off or lock their workstation with a password or lock their device.

The College of Veterinary Medicine and Biomedical Sciences is not liable for lost or stolen devices.

5.) Delete any attachments containing sensitive information from your device that are no longer needed.

VetPoint allows you to save documents and other sensitive information locally to your computer or other device. These documents may contain private client information, so if you no longer require these documents to do your work, we recommend deleting them immediately. Because VetPoint information also remains in your devices' temporary internet folders, we recommend you clear these locations as well.

- **iPad or iPhone:** Open the Chrome App, select the settings option, select Privacy, and choose Clear All
- **Android Device:** Open the Chrome App, select the settings option, Select Content Settings, Select Website Settings, select any CVMBS and Vetpoint related sites and select Clear stored data
- **Windows:** Open Chrome, click the settings option, select Tools, Select Clear browsing Data, check Download History, Cached images and files and click Clear browsing data.
- **Apple:** Open Chrome, click the settings option, select Tools, Select Clear browsing Data, check Download History, Cached images and files and click Clear browsing data.

6.) Do not leave your device logged into Vetpoint when not in use.

When you are not actively using Vetpoint, we recommend you log out of the application to prevent unauthorized access in the event your device is misplaced or stolen. To log out of VetPoint, simply close the Google Chrome browser window.

7.) Install an anti-virus program and keep it up to date.

An antivirus program helps prevent a virus or other malware from damaging the computer's operating system, other functions of your computer or any network to which your computer is attached. Updating the antivirus application with up-to-date virus definitions is also extremely important to protect your critical data, information, files, documents, photos, presentations and other material stored on your computer from virus attacks.

- **iPad or iPhone:** There are no Antivirus apps available for the iPad or iPhone.
- **Android:** Lookout Security & Antivirus is available from the Google Play store and provides App and file scanning, device tracking and remote wiping services.
- **Windows and Apple:** Symantec AntiVirus for Windows and Apple is free for home use for faculty, staff and student personal computers and can be downloaded from Academic Computing and Networking Services at www.acns.colostate.edu/downloads.

8.) Always keep the operating system and other applications on your device up to date.

Keeping your computer—including its operating system and all the installed 3rd party software—up to date is extremely important. Having an up-to-date system reduces the likelihood of being exploited by malicious software. On top of operating system updates, you will also need to check 3rd party applications for updates individually such as Adobe Reader, Adobe Flash and Java.

- **iPad or iPhone:** Open Settings, select General, select Software Update and install all available updates. Open the iTunes App Store, select updates, and select Update All to update all available apps.
- **Android Device:** Open Settings, select About and Select System Updates and install any system updates that are available. Open the Google Play Store select the Play Store icon, select My Apps, and update all available apps.
- **Windows:** Open the Control Panel and select Windows Update. Select Check for Updates and install all available updates.
- **Apple:** From the Apple menu, select Software Update and install all available updates.

The College of Veterinary Medicine and Biomedical Sciences is not liable for damage to hardware or software caused by 3rd party applications such as Symantec Anti-virus, Java, Junos Pulse VPN, Adobe Reader, Adobe Flash, or Google Chrome.

If you have any questions regarding these recommendations, please contact the CVMBS IT Services Helpdesk at 970-297-HELP(4357) or CVMBSComputerHelp@Colostate.edu.