http://security.bsd.uchicago.edu


## In this issue of the BSD ISO Cybersecurity Newsletter…

- **Securing Your Devices –** The BSD Information Security Office wants to help protect you from any accidental confidential information disclosure and, in collaboration with the BSD Security Liaisons Group, developed the Securing Devices Guidelines. The enclosed Securing Devices Top 10 list provides a snapshot of the Securing Devices Guidelines with instructions on how to ensure greater security for your personal device(s). **(*Page 1-2*)**

- **What's New**

  - **Security Standards** – The BSD Security Liaisons Group published the BSD Security Standards for Web Applications. This standard ensures that web applications used by the Biological Sciences Division are properly and safely developed. See the Standards section for more information. **(*Page 3*)**

## Securing Your Devices

Personal computing devices are becoming more and more portable and securing the sensitive information stored on those devices is more important than ever. Don't ever say "It won't happen to me". We are all at risk and the stakes are high - to your personal and financial well-being, and to the Biological Sciences Division's standing and reputation. Can you check off any of the following Top 10 securing devices guidelines that protect your devices and information?

**Securing Devices Top 10 List**

| | |
|---|---|
| #1 | **Use a Password and Screensaver** |
| #2 | **Install and Use Anti-Virus Software** |
| #3 | **Enable Built-In Firewall** |
| #4 | **Encrypt Your Hard Drive** |
| #5 | **Install UChicago VPN (Virtual Private Network)** |
| #6 | **Keep your Operating System and Applications Software Up to Date** |
| #7 | **Enable Web Browser Security Settings** |
| #8 | **Be Aware of the Treatment of Confidential Information** |
| #9 | **Backup your Data** |
| #10 | **Report Security Incidents** |

The following table provides general instructions on how to implement the Top 10 securing devices guidelines. For detailed securing devices guidelines instructions, click the icon for your specific device below or visit the BSD ISO website at **http://security.bsd.uchicago.edu/Security-Policies**.

| OSX | Windows | IOS | Android |
|---|---|---|---|

# Securing Devices Top 10 List Instructions

## #1 Use a Password and Screensaver

Choose a strong password to access your device. Require the password when your device sleeps or the screen saver is activated. Do not allow automatic login. Set your screen saver and require your password to unlock it.

## #2 Install and Use Anti-Virus Software

Download Symantec Endpoint Protection. Log in using your CNetID and password and download the file. Extract the zip file, open the extracted file(s), and follow the instructions.

## #3 Enable Built-In Firewall

Macintosh, Windows, iOS and Android devices have built-in firewalls as part of their operating systems. When set up properly, these firewalls protect your computer files from being scanned.

## #4 Encrypt your Hard Drive

Visit the BSD ISO Website at http://security.bsd.uchicago.edu/encryption/ for more information on encrypting your devices.

## #5 Install UChicago VPN (Virtual Private Network)

Install cVPN software if you expect to use untrusted networks (such as guest wireless in a hotel or coffee shop). UChicago students, researchers, faculty, and staff can download and install cVPN by visiting cvpn.uchicago.edu.

## #6 Keep your Operating System and Applications Software Up to Date

Turn on automatic updating to keep your operating system and applications updated to the latest version of the release. This provides you with security updates and other improvements.

## #7 Enable Web Browser Security Settings

Choose web browser security settings that protect your privacy and enhance security. Learn more about security features in Internet Explorer, Firefox, Safari, and Chrome.

## #8 Be Aware of the Treatment of Confidential Information

Be aware that the University is bound by law or contract to protect some types of confidential information and in other instances the University requires protection of confidential information beyond legal or contractual requirements as an additional safeguard. Refer to HR Policy 601 - Treatment of Confidential Information.

## #9 Backup your Data

Backing up your machine regularly can protect you from the unexpected. Always keep a backup copy of files you do not wish to lose.

## #10 Report Security Incidents

**If you use your computer to maintain or access sensitive institutional data and it is lost or stolen, inform your Manager, IT custodian and send an email to the BSD Information Security Office at security@bsd.uchicago.edu.**

## Cyber Security Policies

We are please to announce that BSD Dean, Kenneth Polonsky and UCMC President, Sharon O'Keefe have approved the following new cyber security policies:

| Policy | Purpose | Target Audience |
|---|---|---|
| **Responsibilities and Oversight** | Defines responsibilities of management, administrators, faculty and staff for safeguarding information systems and information (e.g. Protect Health Information, private research data etc.) | • Administrators, Faculty, Staff<br>• Departmental Unit Leaders,<br>• Executive Management |
| **Awareness and Training** | Sets requirements and scope for cyber security awareness campaigns and trainings. | • Administrators, Faculty, Staff,<br>• Departmental Unit Leaders |
| **Access Control** | Sets requirements for establishing, activating, modifying, reviewing, disabling, and removing user accounts. | • Information System Owners and IT Staff |
| **Media Protection** | Sets requirements for safeguarding Electronic Media (e.g. hard drives, usb etc.). | • Information System Owners and IT Staff |
| **Personally Owned Devices** | Defines minimum expectations for the use of personally owned devices used to access, store and transmit BSD/UCM information. | • Administrators, Faculty, Staff<br>• Information System Owners and IT Staff<br>• Departmental Unit Leaders |

The BSD, UCM and University Information Security Offices collaboratively developed this first set of policies to guide our organizations through the new landscape of cyber security threats and regulations. These policies will supersede the existing Information Security Policies, which were last published in 2006. This new set of robust Policies will enable the organization to:

- Compete for new research opportunities and grants
- Safeguard patient, student and staff information
- Support critical business processes

It's important that you read the policies. We've developed a policy summary document for each policy that you can read through in less than a minute. You can access the new policies and summaries directly from our website BSD Information Security Office Policies.

## Information Security Standards

The BSD Security Liaisons Group has published a new standard the STA-07 BSD Security Standards for Web Applications. This standard ensures that web applications used by the Biological Sciences Division are properly and safely developed. For more standards to secure your devices, visit our site at BSD Information Security Office Policies webpage.

## What to do if you become aware of an information security incident?

Contact the BSD ISO Team via email at security@bsd.uchicago.edu.

## Information Security Office Team

| | | |
|---|---|---|
| Plamen Martinov, Chief Information Security Officer | O: 773-834-1714 | pmartinov@bsd.uchicago.edu |
| Kim Cooke, IT Security and Compliance Analyst | O: 773-834-7897 | kcooke3@bsd.uchicago.edu |