

## Cyber Security Awareness Day



October is Cyber Security Awareness Month. The Governor encourages all citizens to learn about cyber security and put that knowledge into practice in their homes, schools, workplaces, and businesses.

The Governor's Office of  
Administration

Office for Information  
Technology

Information Security Division

**Email:**  
[ra-ciso@state.pa.us](mailto:ra-ciso@state.pa.us)

**Web:**  
<http://cybersecurity.state.pa.us>



## Commonwealth of Pennsylvania



Cyber Security Tips  
for Pennsylvania  
Businesses



**Aiming to keep the  
Commonwealth Safe  
On-line**

<http://cybersecurity.state.pa.us>

## Cyber Security Tips for Pennsylvania Businesses



The topic of Cyber Security covers many actions that together help to deter against hackers, viruses and other potential risks to the networked enterprise. Everyone has a role to play including:

- Management
- Information Technology Staff
- End Users

The key to effectively managing Cyber Security is to demonstrate top-level executive support. Some of the key recommendations include:

- Create security policies to match the size and culture of your business. Policies must be written, enforced, and kept updated.
- Create and deliver a comprehensive security awareness program that addresses cyber security at all levels of the organization.
- Establish a computer software and hardware asset inventory list and create a lifecycle plan for each device.

- Classify data by its usage and sensitivity. Establish owners of all data assets. Identify data covered by specific regulations and requirements. (Federal laws, credit card information)

- Create and test cyber incident response policies and procedures so you are prepared to react quickly in a real situation.

- Make sure you involve other entities in your testing and planning, such as your local law enforcement agencies, to ensure that they are aware of your needs and requirements. This will also develop lines of communication in advance of any real incident.

- Follow best practice cyber security guidelines at all levels of your organization, including application development, server installation, user provisioning and infrastructure management.

- Subscribe to security mailing lists and regularly monitor IT security web sites in order to keep abreast of current issues and threats

- Ensure physical security of systems and facilities. Limit access to authorized personnel.

- Create and test business contingency and continuity plans for your critical systems, data and personnel.

### **Security Related Internet Sites**

- *Commonwealth of PA Chief Information Security Officer Page* - <http://www.cybersecurity.state.pa.us>
- *United States Computer Emergency Readiness Team (US-CERT)* - <http://www.us-cert.gov/>
- *National Cyber Security Alliance – Stay Safe Online* - <http://www.staysafeonline.info/>
- *Federal Trade Commission’s OnGuard Online* - <http://onguardonline.gov/>
- *Carnegie Mellon Computer Emergency Response Team (CERT)* - <http://www.cert.org/>
- *National Strategy to Secure Cyberspace* - <http://www.whitehouse.gov/pcipb/>
- *NIST Computer Security Resource Center* - <http://csrc.nist.gov/>
- *SANS Institute – Security Policy Project* - <http://www.sans.org/resources/policies/>
- *AntiSpyware Coalition* - <http://www.antispywarecoalition.org/>
- *Availability.com* - <http://www.availability.com/>
- *Microsoft Technet Security Center* - <http://www.microsoft.com/technet/security/default.msp>