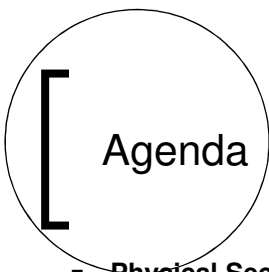


CVM Computer Security Training



Responsible Computing Practices

Veterinary Information Systems
March 2008

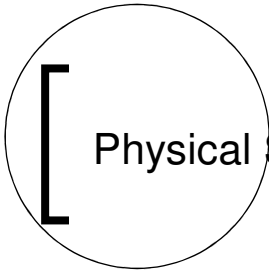


Agenda



- **Physical Security**
- **Responsible Behavior**
- **Minimum Computer Security Standards (MCSS)**
 - Data Definitions and Examples
 - Passwords
 - Patching & Updates
 - Protection
- **Backing up Data / Responsible Storage**
- **Application Security**
- **Summary**
- **Q&A / Discussion**

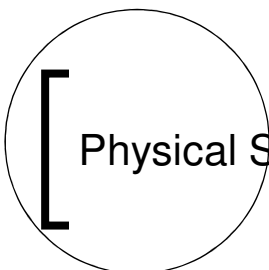




Physical Security



- **Physical Locks**
 - Use a laptop lock if/when possible
- **Responsible Behavior**
 - Never leave your laptop in your car (even if it's locked)
 - Do not walk away from your laptop in a public setting
 - Be aware of your surroundings
 - Inventory your portable system



Physical Security (What if your device is stolen?)



- **BEFORE:** Record your MAC (Media Access Control) address and serial number; keep them in a safe place
 - MAC address is a 12-digit alphanumeric code
 - Looks like 00-13-72-77-A1-E2
 - Don't know how to find it? Just ask VIS
- **AFTER:** Immediately notify the police and file a police report
 - If it is university owned, notify the Director of IT (Don Krueger, Don.Krueger@cvm.osu.edu, 7-4346)
 - VIS may have to notify CIO Security



Responsible Behavior

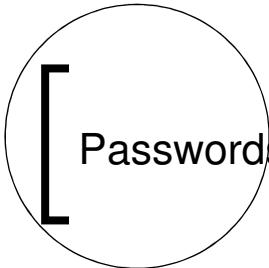
- **Know what restricted data is**
 - Take the required Institutional Data Training Policy
- **Follow best computing practices**
 - 3 P's: Passwords, Patching, Protection
- **Use screensavers with password protection**
 - Lock your computer when you leave
- **Be careful when web surfing or downloading**
 - Know what you are looking at and what you are getting



Data Definitions and Examples

- **Public Data**
 - Examples: Data intended for broad distribution; freely available to anyone
- **Limited Access Data**
 - Examples: Requires specific authorization to access – Date of birth; ethnicity; non-personal research data
- **Restricted Data**
 - Examples: Data protected or regulated by law – SSNs, Student academic records, credit card #s, and so forth
- **Take the required Institutional Data Policy Training**

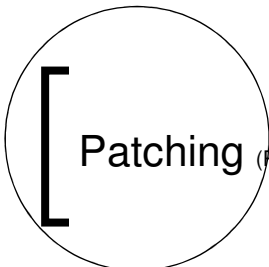




Passwords (NEVER share them with anyone)



- **Required MCSS standard**
- **Strong and robust passwords**
- **CVM Password Criteria**
 - Change every 120 days
 - 8 or more characters in length
 - Must contain 3 of 4 of the following - Upper Case letters, Lower Case letters, numbers, and/or special characters
 - Cannot contain part of your username
- **Do not write your password down and store it in obvious places**
 - Under the keyboard, in your desk drawer, a post-it on your monitor

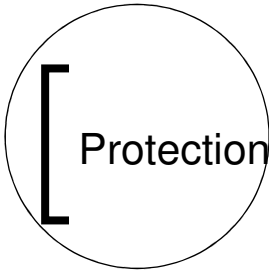


Patching (Perform Frequently and Automatically)



- **Required MCSS standard**
- **Acts as preventative maintenance to software and operating systems**
- **Acts as a defense mechanism against attacks**
- **Many operating systems and software packages offer auto updates**

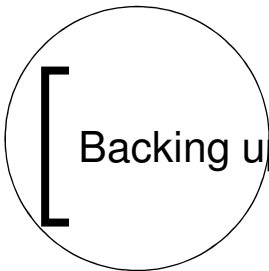




Protection (FREE to any OSU affiliated faculty or staff member)



- **Required MCSS standard**
- **Antivirus protection**
 - FREE DOWNLOADS to any Faculty, Staff, or Student
 - McAfee VirusScan 8.5 and McAfee VirusScan AntiSpyware module for PC
 - Virex 7.7 or VirusScan 8.6 for MAC
- **Spyware/Adware protection**
 - Spybot Search & Destroy
 - Ad-Aware
- **Firewall** - Current versions of Windows and MAC operating systems have integrated firewalls



Backing up your Data



- **You are responsible for backing up your data**
- **Back it up regularly** – Rule of Thumb: Once a week




Responsible Storage

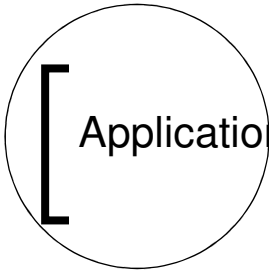
- **Recommended: store data on CVM network**
- **No restricted data on personally-owned devices**
- **No restricted data on portable devices, for example:**
 - Maxtor
 - USB jump drives (flash drives)
 - PDA's
 - CD's/DVD's



Application Security (Internet)

- **Utilize best practices when web surfing**
 - Do not store passwords
 - Double check the URL and ensure you are using a secure connection when performing online transactions
 - Check for "HTTPS" in the URL hyperlink when performing online transactions
 - Look for the "lock" icon in your browser, looks like: 
 - Keep your history clear by deleting your cache, cookies, and downloaded info cleared regularly (select delete all)

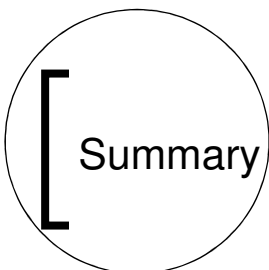




Application Security (Email)



- **Utilize best practices when downloading emails**
 - Do not open emails – especially attachments from people you don't know
 - Do not open emails with misspellings or that “advertise”
 - Do not use the “remove” option from anything suspected to be spam



Summary



- **What can you do?**
 - Take the Institutional Data Policy Training
 - Ensure your computer and software are patched and up to date
 - Change your passwords regularly
 - Do not store university data on a non-university owned computers or other devices
 - Contact VIS at 292-4146 or vishelpdesk@cvm.osu.edu with any questions or concerns you may have

