Approved by Chris Urbina, Executive Director and Chief Medical Officer, February 2013

SUMMARY

Colorado and federal statutes and regulations require privacy protection for citizens. Accordingly, employees of the Colorado Department of Public Health and Environment and the Office of Information Technology (OIT) shall follow this policy and its procedures for configuring department computers.

POLICY

To protect department information systems, data and applications, it is important to reduce the risk of importing viruses or other malicious software into the department's information technology environment. Some software may contain security flaws or weaknesses that could endanger other parts of the department network and information systems. For these reasons, employees shall have software approved, in accordance with the following procedure, before it is loaded onto a department computer.

PROCEDURE

1. All documents and data brought from home or received from an outside source shall be screened for viruses and malicious software before being imported or installed on a department computer. Employees shall contact an OIT technician if they are uncertain about how to screen for viruses or are unaware of which applications are automatically screened.
2. Prior to the final installation of software on a department computer, it shall be installed on a test computer to identify security issues or possible conflicts with existing operating systems. The employee shall have supervisor approval before any software is installed. Employees shall work with an OIT technician on test installations.
3. No personal software shall be downloaded or installed onto department computers. All software shall be either licensed to the department or, if free-ware, approved in advance.
4. No software may be installed for strictly personal, nondepartmental use.
5. In general, no sensitive information – including letters, data, spreadsheets, etc. – shall be stored on any laptop or other mobile computing device, home computer or shared computer in the department. If it absolutely necessary to store sensitive data on a mobile device, the employee's supervisor and OIT must approve the specific application and the security configuration of the device.
6. Each employee who works at home, either on a home computer or laptop, shall discuss appropriate encryption or password-protection techniques with OIT. Supervisors will decide whether an employee may access sensitive information when the employee is not at the department.

7. Passwords shall be kept confidential from colleagues, other family members, other laptop users, etc., who are not authorized to access the information. If a data application is involved that is already set up with unique user IDs and password protection, normal procedures for protecting the integrity of passwords shall be observed, and the supervisor shall not have access to the employee's unique password.
8. Employees working remotely shall consult with an OIT technician on the appropriate configuration for home computers, laptops and other remote computers. Any employee working with sensitive information from home or from an otherwise remote location shall implement three safeguards:
    a. Having a firewall installed on the remote computer
    b. Having the remote computer set up for automatic patch updates
    c. Monitoring intrusion attempts on the remote computer
9. OIT security personnel shall approve all wireless applications in advance of installation or use.
10. Any employee not complying with this policy and these procedures may be subject to progressive discipline, up to and including termination. Non-employees who do not comply with this policy and these procedures will be dealt with appropriately.

TOOL/GUIDANCE/STANDARDS

Policy 15.10 Acceptable Use
Workstation Security Guidelines
Wireless Security Guidelines
Wireless and Modem Use Guidelines
Laptop and Remote Access Computer Acceptable Use Guidelines

REFERENCE

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule §164.310, Physical Safeguards, Workstation Use (b) and Security (c).