Wyoming Department of Health

Commit to your health.
visit www.health.wyo.gov

Thomas O. Forslund, Director **Governor Matthew H. Mead**

Policy Title:	Protection from Malicious Software
Policy Number:	S-005b
Effective Date:	July 1, 2013
Approval:	Thomas O Forslund — Thomas O. Forslund, Director; 6/20/13 — Date

Purpose:
This policy establishes security measures to prevent downloading/installation of malicious software; to enhance recognition and reporting of malicious software; and to ensure appropriate mitigation of malicious software attacks.

Scope:
In terms of resources, this policy applies to all information systems and resources that house Wyoming Department of Health (WDH) data. In terms of personnel, it applies to all WDH workforce.

Definitions:
Malicious software means software, for example, a virus, designed to damage or disrupt a system.

Virus means a self-replicating program that runs and spreads by modifying other programs or files.

Policy:

1. **Protection against unauthorized access**
   WDH shall assure that information systems and resources that create, receive, maintain, or transmit protected health information (PHI) on behalf of WDH are secure from unauthorized access. Information systems and resources include, but are not limited to:
   a. Workstations.
   b. Servers.
   c. Mainframes.
   d. Firewalls.
   e. Laptops.
   f. Other portable devices.

2. **Prevention**
   a. WDH workforce shall be trained regarding the vulnerability of information systems and resources to viruses and/or other malicious code, and their responsibility to report known or suspected infections.
   b. WDH workforce shall be informed of the procedures for detecting viruses and limiting the spread of infection.
   c. All software and data imported onto electronic computing devices shall be scanned prior to opening.
   d. Software configurations shall be scanned on a regular basis to reduce the likelihood of malicious software or virus introduction to the network.
   e. WDH shall utilize prevention techniques such as segmenting the network with firewalls to block unauthorized traffic and protect vulnerable systems.
   f. Anti-virus software shall be installed at the network perimeters and other locations as necessary.
3. **Detection**
   a. WDH shall ensure real time anti-virus software is utilized to scan all incoming and outgoing e-mail messages, attachments, and files for viruses and other malicious software.
   b. WDH shall ensure virus scanning results are logged, automatically collected, and audited.
4. **Removal**
   a. Any electronic computing device suspected of infection with an irremovable virus shall immediately be isolated and disconnected from the network.
   b. Appropriate measures shall be taken to remove the virus. If removal is unsuccessful, all software on the device, including boot records, shall be deleted, and software from uninfected sources shall be re-installed.
5. **Reporting**
   a. WDH workforce shall immediately report abnormal functioning or known or suspected viruses to both the WDH Compliance Office or designee and Wyoming Department of Enterprise Technology Services (ETS) in accordance with WDH Policy AS-009 and S-006a; Report and Response to Security Incidents, and by utilizing WDH Form SF-006; Incident Contact List.
   b. WDH Forms SF-004; WDH Computer Security Incident Reporting Form, and SF-003; Incident Communication Log, shall be utilized to document mitigation efforts.

Contacts:
De Anna Greene, CIPP/US, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer, (307) 777-8664
Tate Nuckols, JD, WDH Security Officer, (307) 777-2438

Forms:
SF-003; Incident Communication Log
SF-004; WDH Computer Security Incident Reporting Form
SF-006; Incident Contact List

Policies:
AS-009 and S-006a; Report and Response to Security Incidents

References:
45 CFR § 164.304
45 CFR § 164.308(a)(5)
NIST SP-800-61

Training: