 <p style="text-align: center;">Heritage Provider Network & Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No. 14-014	Effective Date: 04/20/2005	Page - 1 -
	Authored by: David Pfafman	Date: 04/14/2005	Revised by: Scott Bae
	Approved by: Scott Bae	Date: 02/02/2015	Date: 02/02/2015
Title of Policy: Intrusion Detection			


POLICY:

It is the policy of Heritage Provider Network and its Affiliated Groups (HPN) to provide information for management and workforce members regarding the detection of intruders onto the computers and computer systems and networks, and the mechanisms that determine when to activate planned responses to an intrusion incident.

DEFINITIONS:

1. Information Resources (IR) - Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
2. Security Incident Information - Operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.
3. Information Attack - An attempt to bypass the physical or information security measures and controls. The attack may alter, release, deny or destroy data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.
4. Information Operations Actions - Taken to affect adversary information and information systems while defending one's own information and information systems.
5. Security Officer (SO) - Responsible for administering information regarding security policies.

DEFINITIONS (continued):


 <p>Heritage Provider Network & Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No. 14-014	Effective Date: 04/20/2005	Page - 2 -
	Authored by: David Pfafman	Date: 04/14/2005	Revised by: Scott Bae
	Approved by: Scott Bae	Date: 02/02/2015	Date: 02/02/2015
Title of Policy: Intrusion Detection			

6. Host - A computer system that provides computer service for a number of users.
7. Server - A computer program that provides services to other computer programs in the same or another computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.
8. Firewall - An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

PROCEDURE:

1. Operating system, user accounting, and application software audit logging processes must be enabled on all computers, networks, hosts and server systems.
2. Alarm and alert functions of all firewalls and other network perimeter access control systems must be enabled.
3. Audit logging of all firewalls and other network perimeter access control systems must be enabled.
4. Audit logs from the perimeter access control systems must be monitored/reviewed on a regular and routine basis by the system administrator or Information Security Officer.
5. System integrity checks of all firewalls and other network perimeter access control systems must be performed on a regular and routine basis. At a minimum, it is performed on a monthly basis.
6. Audit logs for computers, servers and hosts must be reviewed on regular routine basis. These are reviewed as needed as well as at a minimum on a monthly basis.
7. It is standard group policy for Heritage domain access to lock accounts after three consecutive unsuccessful attempts. Intrusion tools will be checked on a regular and routine basis. The intrusion tools consist of monitoring log-in attempts and reporting lockouts and discrepancies to the Security Officer. This is performed on a monthly basis.
8. All trouble reports should be reviewed for symptoms that might indicate intrusive activity.
9. All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported to the Security Officer and to the Compliance Committee.

DEFINITIONS (continued):

 <p>Heritage Provider Network & Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No. 14-014	Effective Date: 04/20/2005	Page - 3 -
	Authored by: David Pfafman	Date: 04/14/2005	Revised by: Scott Bae
	Approved by: Scott Bae	Date: 02/02/2015	Date: 02/02/2015
Title of Policy: Intrusion Detection			

10. Users shall be trained to report any anomalies in system performance and signs of wrongdoing to the Security Officer.

Enforcement

1. Heritage Provider Network's Security Officer, office manager and supervisors are responsible for enforcing this policy. Employees and workforce members who violate this policy will be subject to disciplinary action, up to and including termination or dismissal.