

5007.0.0 SECURITY INCIDENT REPORTING AND RESPONSE POLICY

5007.1.0 Purpose

To establish a reporting requirement for security incidents affecting the confidentiality, integrity, or availability of DHS information and a DHS Computer Incident Response Team (CIRT) made up of managers, workforce members and other authorized information users.

5007.2.0 Applicability

5007.2.1 These rules apply to all DHS employees, volunteers, contractors, temporary workers, those employed by others to perform DHS work, and others authorized to access DHS information, networks, or systems.

5007.2.2 All individuals granted access to DHS information or systems are covered by this policy and shall comply with this and associated policies, standards, guidelines and procedures. These individuals include all employees, volunteers, contractors, sub-contracts temporary workers, those employed by others to perform DHS work, and others authorized to access DHS information and network systems.

5007.3.0 Definitions

5007.3.1 Authentication: The automated comparison of presented user credentials with credentials on record for access to DHS Information Systems.

5007.3.2 Availability: The assurance that a resource is available for access by authorized users whenever needed.

5007.3.3 Confidentiality: A requirement that applies to data that must be held in confidence and describes that status or degree of protection that must be provided for such data about individuals as well as organizations.

5007.3.4 DHS Information Systems: DHS Network services (Network, access, E-mail, Internet, etc.), DHS applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the DHS devices for which it was intended. Also includes any computer file, on any device in use by DHS or its agents that is shared across the DHS network or requires DHS support or that contains DHS-related information, the privacy of which must be safeguarded.

5007.3.5 DHS Security and Privacy Officers: DHS Security and Privacy Officers consist of the DHS IT Security Officer, DHS HIPAA Security Officer, and DHS Privacy Officer who have responsibility for the safeguarding of data and sensitive information for DHS.

5007.3.6 Integrity: Verification that an unauthorized modification (including changes, insertions, deletions and duplications) has not occurred either maliciously or accidentally.

5007.3.7 Person: For the purposes of this policy, a person is defined as a uniquely identifiable and distinguishable human being, whose identity has been validated and whose association with DHS has been certified by the division requesting access credentials. A person may or may not be a DHS employee.

5007.3.8 Security Incident: The suspected or actual attempted or successful unauthorized acquisition, access, use, disclosure, modification, or destruction of DHS information or interference with a DHS Information System. Examples include:

- A. Copyright infringement (downloaded movies and music);
- B. Denial of service attacks or attempts;
- C. E-mail hoaxes;
- D. Failure to follow DHS security policies;
- E. Unauthorized access, acquisition, use or disclosure of Personally Identifiable Information (PII) or Protected Health Information (PHI) as those terms are defined under state and federal law;
- F. Misuse of a State personal computer or DHS Information System; including unauthorized use or disclosure of confidential or sensitive information, accessing the internet from a DHS computer without logging on to the DHS Network or a DHS approved network, installing or downloading software onto a DHS computer other than what is explicitly required in the conduct of DHS related business
- G. Password sharing;
- H. Phishing scams;
- I. Physical intrusion or attempted intrusions into DHS facilities containing Information Systems;
- J. Port or network scans or probes;
- K. Requirement for emergency deactivation of User's access to Information Systems due to perceived insider threat;
- L. Social engineering attempts;
- M. Behavior that might threaten the safety or security of DHS information or Information Systems;
- N. Suspected hacking attempts;
- O. Exploiting System vulnerabilities;

- P. Theft or attempted theft of computers, flash drives, mobile devices, BlackBerries®, or any Protected Health Information or personally identifiable information;
- Q. Unauthorized devices connected to DHS Information Systems or containing DHS information;
- R. Unauthorized software installed or located on a DHS Information System;
- S. Virus, worm, or “Trojan Horse” activity;
- T. Web site defacement.

5007.4.0 Failure to Comply

Failure to comply with this policy and associated policies, standards, guidelines, and procedures may result in disciplinary actions up to and including dismissal from state service for employees (DHS Policies 1084 and 1085) or volunteers or termination of contracts for contractors, partners, consultants, and other entities. Legal actions may also be taken for violations of applicable regulations and laws.

5007.5.0 Policy

- 5007.5.1 DHS managers, workforce members, and other authorized information users are required to report security incidents affecting the confidentiality, integrity, or availability of DHS information.
- 5007.5.2 DHS Reports shall be submitted as outlined in DHS Procedure 5007.A, Security Incident Reporting Procedure.
- 5007.5.3 The DHS IT Security Officer shall establish a DHS CIRT as set out in the CIRT procedures to provide quick, effective, and orderly response to security related incidents.
- 5007.5.4 The DHS CIRT shall maintain incident response handling procedures regarding notification, assessment, investigation, remediation, monitoring, and final reporting of incidents. (DHS Procedures 5007.B – 5007.F)
- 5007.5.5 The DHS CIRT shall maintain procedures to report criminally related security incidents to outside authorities in compliance with appropriate legal requirements and regulations.
- 5007.5.6 The DHS CIRT shall designate secondary members to serve in the event of manpower shortages.
- 5007.5.7 The IT Security Officer shall maintain contact information for all members of the CIRT, designated secondary members of the DHS CIRT, the DHS CIO, and appropriate points of contact at relevant law enforcement agencies.
- 5007.5.8 DHS shall provide appropriate means to allow immediate notification of the DHS CIRT as required by DHS procedures 5007.A and 5007.B.

- 5007.5.9 DHS Security and Privacy Officers shall document security incidents and maintain incident activity logs.
- 5007.5.10 DHS Security and Privacy Officers may facilitate security related process improvement activities to reduce the risk of repeated incidents.
- 5007.5.11 DHS Security and Privacy Officers shall inform DHS executive management of information security vulnerabilities and incidents that threaten the confidentiality, integrity or availability of DHS information, network or systems and provide strategies to mitigate the identified risks through the communication liaison of the CIRT.

5007.6.0 Related Polices and References:

DHS Security Incident Policy (DRAFT)
DHS Security Incident Reporting Form
DHS Policy 1084 Employee Discipline Policy
DHS Policy 1090 Incident Reporting Policy
DHS Policy 4001 Notice of Privacy Practices Policy
DHS Policy 4004 Mitigation of Violations of Privacy Rights
DHS Policy 4004 DHS Protected Health Information Complaint Procedure
Health Insurance Portability and Privacy Act of 1996
ISO 27002
Arkansas Personal Information Protection Act, Act 1526 of 2005 and amendments thereto codified at A.C.A. §4-110-101
Health Insurance Portability and Accountability Act
NIST Guide to Protecting the Confidentiality of Personally Identifiable Information

5007.7.0 Exceptions to Policy

Exceptions to this policy must be requested in writing to the DHS IT Security Officer. Exceptions are granted in writing on a per instance basis. Individual exceptions do not extend beyond the party to which they are issued.

5007.8.0 Originating Section/Department Contact:

Office of Systems and Technology
1st Floor Donaghey Plaza North
PO Box 1437, Slot N101
Little Rock, AR 72203-1437
Telephone: 682-0032