5003.0.0 DHS REMOTE ACCESS POLICY

5003.0.1 This policy defines procedures for persons employing a remote connection to access the Department of Human Services (DHS) Information Systems. It applies to all DHS Information Systems users in all DHS divisions and to all non-DHS organizations to whom DHS offers remote access.

5003.0.2 DHS Users and non-DHS Users, as defined below, may use various forms of remote connection technologies to gain access to DHS Information Systems. Access requires the user to present authenticated credentials when prompted.

5003.0.3 See DHS Policy 5001, Information Systems Security Access, for related security requirements and definitions of security terminology.

5003.1.0 Definitions

5003.1.1 Access: Upon the presentation of authenticated credentials, permission to use DHS information systems.

5003.1.2 Credentials: A combination of a user's User Name (or similar user identifier), and Password. Users present credentials, when prompted, to access DHS Information Systems.

5003.1.3 DHS Information Systems: DHS Network services (Network access, Email, 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 for which the privacy is required to be safeguarded.

5003.1.4 DHS User: A person, DHS employee, who has been granted access to any DHS information system and is accountable for the security of such access.

5003.1.5 Non-DHS User: A person, not a DHS employee, who has been granted access to any DHS information system and is accountable for the security of such access.

5003.1.6 Remote Connection: Includes a variety of technologies that enable a user to connect to the DHS Network from devices not directly linked to DHS's Network. For DHS purposes, Virtual Private Network (VPN) technology is preferred where deployed. Methods typically in use include Terminal Server (TS), Remote Desktop Connection (RDC), and Remote Access Server (RAS). Typical hosting services enabling these methods include Internet Service Providers (ISP), connection through an organization's own internet hosting service, or dial-in through a telephone line (RAS).

5003.1.7 Security Gateway Administrator: Persons performing this role serve as the common point of entry for all user access requests. Primary functions include initial evaluation of received access requests, validation of identity, and re-directing of requests for additional processing.

5003.1.8 Virtual Private Network (VPN): A VPN is a secure, private network that uses a public network (usually the Internet) to connect hosts (such as DHS's network) with remote users.

5003.2.0 Request for Access

5003.2.1 Requests for Remote Access must be submitted by the division's Authorized DHS Approving Manager (ADAM) to the Security Gateway Administrator, using DHS Form 359 (DHS Systems Access Request, available on DHS Gold). See DHS Policy 5001, Information Systems Security Access, for the ADAM's System Security Certification requirements.

5003.2.2 ADAMs certify by signature on DHS Form 359, the following:

A. That such access requests are made on behalf of persons who are DHS employees in good standing, or if a non-DHS user, have been verified to be a member of an organization with whom a formal agreement is in place to permit access to DHS systems and to safeguard protected information.

B. That users have provided accurate identifying information and that the user has a legitimate and official purpose for the requested level of access.

C. That the users have been apprised of DHS policies pertaining to the appropriate use of state equipment and systems services, pertaining to the safeguarding of private information, and have received HIPAA privacy training as required by DHS policy or contracts.

D. That they agree to notify the DHS Systems Security Gateway of material changes in users' employment status as relates to any DHS network services or systems applications for which users have been granted access.

5003.3.0 Management of Authorizations

5003.3.1 The Network Administrator is responsible for maintaining a list of users granted remote access privileges and for submitting a monthly report of such users to the DHS IT Security Officer.

5003.3.2 The DHS Chief Information Officer reserves the right to approve requests for remote access to DHS Information Systems, and reserves the right to terminate access at any time.

5003.4.0 Responsibilities of Remote Access Users

5003.4.1 This policy applies to persons employing a remote connection (see Remote Connection definition above) to access DHS Information Systems. It applies to all DHS Information Systems users in all DHS divisions and to all non-DHS organizations to whom DHS offers remote access. Also included are persons who remotely access a DHS Email

account, who remotely connect to a DHS application or network service, or who remotely connect to a computer device at their work site. This policy applies without regard to: the remote connection method employed (see Remote Connection definition above); who pays for the method of connection; where the remote site is located; what type of remote computer device is used.

5003.4.2 Requests for Remote Access must be submitted, using Form DHS-359 (DHS Systems Access Request) through the user's DHS Approving Manager (ADAM). Form DHS-359 requires the user's signature to a Security Agreement and Confidentiality Statement.

5003.4.3 It is the responsibility of the user to comply with DHS Policy 5001, Information Systems Security Access, and the terms of the signed Security Agreement and Confidentiality Statement.

5003.4.4 It is the responsibility of remote access users to ensure that connection to DHS Information Systems is not used by unauthorized persons who may have access to their devices. Users must be made aware that remote access connects from their remote site (e.g., Home, facility, travel locations, etc.) to the DHS Network, so that their device becomes an extension of the network and can provide a path to expose DHS's most sensitive information. The user must take every reasonable measure to protect DHS Information Systems from intrusion and exposure.

5003.5.0 Disciplinary Action for Violation of Policy

Supervisors should refer to DHS Policy 1084, Employee Discipline, to determine the appropriate disciplinary action for violations of this policy.

5003.6.0 Originating Section/Department Contact

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