State of Arkansas

DRAFT Standard Statement – Remote Access

Title: Remote Access

Document Number: SS-70-009

Effective Date: x/x/2010

Published by: Department of Information Systems

1.0 Purpose

There are many instances when authorized individuals require remote access to sensitive state information technology resources. Examples of remote access include, but are not limited to, employees checking email while traveling, inspectors submitting reports from the field, and contractors accessing machines to troubleshoot problems. In many cases, these individuals are using personally-owned computing devices to gain access to state resources which could introduce these resources to cyber infection. Access to the state network and the state's sensitive information technology resources should be regulated to ensure effective protection measures are in place to minimize the risk of compromise.

2.0 Scope

This standard statement applies to all state agencies, boards and commissions and administrative portions of institutions of higher education.

3.0 Background

Arkansas Code Ann. Section 25-4-105(13) and (15)(Supp. 2007) gives the Department of Information Systems the authority to define standards, policies and specifications for state agencies and ensuring agencies' compliance with those policies, procedures and standards. In addition, the department develops information technology security policy for state agencies.

The State Security Working Group, made up of representatives of state agencies and higher education, wrote the Remote Access Standard.

4.0 References

4.1 Arkansas Code Ann. Section 25-4-105(13) and (15) (Supp. 2007) authorized the Department of Information Systems to develop statewide information technology security policies

5.0 Standard

5.1 Remote access of non-publicly available state information technology resources by state employees or authorized entities shall comply with the following requirements. Organizations have the right to establish more stringent patching standards.

5.1.1 Spyware Scanning Standard (SS-70-005)

5.1.2 Virus Scanning Standard (SS-70-004)

5.1.3 Client operating system and Internet browser security patches must be applied within 30 days of release by the vendor.

5.1.4 The client operating system and Internet browser versions must be currently supported by the manufacturer.

5.1.5 Each remote access client system shall be protected by a standalone or integrated desktop firewall configured to disallow unauthorized traffic.

5.2 Agency email accessed from outside the agency shall utilize technologies that encrypt the communications from the client to the email server.

5.3 Remote access of Level B (Sensitive), Level C (Very Sensitive) and Level D (Extremely Sensitive) data, classified by the Data and System Security Classification Standard (SS-70-001), housed by covered entities, must comply with the Encryption Standard (SS-70-006).

5.4 Any Level C or D data transferred to the client system must be encrypted on that system in compliance with Encryption Standard (SS-70-006) or securely destroyed at the end of the remote access session.

5.5 Split tunnel VPNs, unencrypted VPNs and https servers shall be configured to disallow general file access to Level B, Level C and Level D data.

5.6 Applications allowing controlled access to specific records containing Level B, Level C and Level D data may utilize encrypted split tunneling technologies and/or the https protocol.

5.7 All methods of encryption utilized during remote access must comply with the Encryption Standard (SS-70-006).

6.0 Procedures

The State Cyber Security Office reserves the right to audit for compliance with this standard. Furthermore, the State Cyber Security Office has the right to grant an exception or exclusion to any part of this standard.

7.0 Revision History

Date	Description of Change
x/x/2010	Original Standard Statement Published

8.0 Definitions

8.1 Controlled access:

Device or application that restricts access based on user rights or other form of authentication

8.2 Remote Access

Remote access is the ability to get access to a computer or a network from outside the organization through the use of an electronic device.

8.3 Secure Virtual Private Network (VPN)

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses. Secure VPNs do not allow split tunneling.

8.4 Split Tunneling

The process of allowing a remote VPN user access a public network, most commonly the Internet, at the same time that the user is allowed to access resources on the VPN. This method of network access enables the user to access remote devices, such as a networked printer, at the same time as accessing the public network. An advantage of using split tunneling is that it alleviates bottlenecks and conserves bandwidth as Internet traffic does not have to pass through the VPN server. A disadvantage of this method is that it essentially renders the VPN vulnerable to attack as it is accessible through the public, non-secure network.

9.0 Related Resources

9.1 Data and System Security Classification Standard (SS-70-001): http://www.dis.arkansas.gov/poli_stan_bestpract/standards.htm

9.2 Encryption Standard (SS-70-006): http://www.dis.arkansas.gov/poli_stan_bestpract/standards.htm

9.3 Spyware Scanning Standard (SS-70-005) http://www.dis.arkansas.gov/poli_stan_bestpract/standards.htm

9.4 Virus Scanning Standard (SS-70-004) http://www.dis.arkansas.gov/poli_stan_bestpract/standards.htm

9.5 COBIT standards: www.isaca.org/cobit.htm

9.6 Physical and Logical Security Standard (SS-70-008): http://www.dis.arkansas.gov/poli_stan_bestpract/standards.htm

9.7 NIST Publication 800-46 Revision 1, Guide to Enterprise Telework and Remote Access Security: http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf