State of Arkansas
Office of the State Executive Chief Information Officer
124 West Capitol Avenue Suite 990 Little Rock, AR 72201
Phone 501-682-4300 Fax 501-682-2040
http://www.cio.arkansas.gov/techarch

Agency #200-00

Best Practices – Non-Governmental Technical Equipment

Title: Non-Governmental Technical Equipment
Use for Official Business

Document Number: BP-00-001

Effective Date: 1/1/2007

Published by: Office of Information Technology

1.0 Purpose

1.1 This best practice document has been created to provide guidance on the use of non-governmental technology equipment (e.g., computers, handhelds, data storage devices and cell phones) for official business. At the direction and approval of a state agency, non-governmental equipment may be used to facilitate official state business.

2.0 Scope

2.1 These best practices address data security, network security, wireless security, email, instant messaging, software licensing, and equipment maintenance as they relate to non-state owned technology equipment.

2.2 State agencies, boards and commissions may limit or prohibit the use of non-governmental technology equipment for official business.

2.3 Individuals serving an official capacity in state government should recognize that most laws, policies and standards related to information technology regulate the data used for state business regardless of the ownership of the equipment on which that data resides. State-owned data maintained on non-governmentally owned equipment is subject to all applicable laws, rules and regulations of the State of Arkansas.

3.0 Background

3.1 State government serves the citizens of Arkansas through the efforts of thousands of employees and numerous volunteers located across the state. Increasingly, state government is called upon to deliver more and better services to a growing population that continues to expect ever increasing improvements in service delivery. Much of this productivity increase has come about through the use of modern information technology such as computers, facsimile machines, and the Internet.

3.2 State employees should be provided with a professional supportive work environment. They should be provided the tools needed to effectively carry out their assigned responsibilities.

3.3 Instances may arise in which there are insufficient state-owned technical resources to accomplish a task or instances in which results may be enhanced by utilizing outside resources. Additionally, state agencies may rely on non-state equipment for catastrophic disaster response, continuity of operations or telecommuting.

3.4 References:

- SS-70-001 Data and System Security Classification
- SS-70-002 Password Management
- SS-70-004 Virus Scanning for State of Arkansas Network
- PS-20 Software Licensing Policy
- PS-60 State Network Requirements
- BP-70-010 Wireless Security
- BP-70-020 Instant Messaging Security
- Internet Appropriate Use Guidelines
- Physical Security Guidelines Brochure

4.0 Best Practice Recommendations

4.1 Background

4.1.1 It is highly recommended that an agency require written approval for state employees to use personal, rented or loaned equipment when the agency does not own or have the necessary equipment available for the employee's use.

4.1.2 Members of governing boards and commissions may be supplied state-owned technical equipment if that equipment is deemed necessary for the performance of their duties and is available. If the necessary equipment is not available, board and commission members may use their own equipment for those duties, at no expense to the state, except as identified in this document or agency-specific legislation.

4.1.3 Management should review their Internet use policies, compensatory time policies, and other contracts to assure that existing documents are not in conflict with these guidelines.

4.2 Data Security

4.2.1 Personal information maintained on non-governmentally owned equipment is private and not subject to the Freedom of Information Act. Employees and members of governing boards and commissions should endeavor to keep their personal information segregated from state-related business.

4.2.2 State government has full ownership rights to all data related to state government business regardless of the hardware platform on which that data is maintained. State data kept on personally owned, rented or loaned equipment is subject to the Freedom of Information Act. Information which is subject to FOIA must be maintained in a format or medium which is readily accessible to the public.

4.2.3 Non-governmental equipment that will be exposed to state data or state data networks must comply with state standards regarding anti-virus and spyware protection software. That software may be provided by the owner of the equipment or by state government (SS-70-004).

4.2.4 Passwords protection must comply with State standards (SS-70-002).

4.2.5 Data maintained on non-governmental equipment must comply with all state security standards. Data or systems classified as Security Level C or D (SS-70-001) must adhere to the following standards*:*

4.2.5.1 Qualifying data should remain on non-governmentally owned equipment for as short a time as possible. When the need for the data no longer exists and is no longer needed to comply with Records Retention requirements of Section 4.9 below, the data should be thoroughly erased with a product that meets Department of Defense disk sanitation standards.

4.2.6 Appropriate physical security and access control measures should be in place to prevent the accidental or intentional destruction, modification or exposure of state data to unauthorized access. (Physical Security Guidelines Brochure).

4.3 Network Security

4.3.1 Internet appropriate use and security guidelines of the governing agency remain in effect when connected to a state network or exposing data to unauthorized access (SS-70-004).

4.3.2 Connecting a non-governmentally owned computer to a State network makes that computer subject to all requirements applicable to that network (SS-70-004, PS-60).

4.4 Wireless Security

4.4.1 Individuals using non-governmental computers should adhere to the Best Practices for Wireless Security document (BP-70-010).

4.5 Email

4.5.1 Email received and retained on a non-governmentally owned computer remains subject to the provisions of the Freedom of Information Act (FOIA). Personal email is exempt but email related to government business is not.

4.5.2 It is highly recommended that board and commission members and employees maintain a state government provided email address for state business. Agencies may purchase email accounts through the Arkansas Department of Information Systems for this purpose. Individuals using other email accounts must ensure that adequate security safeguards are maintained.

4.6 Instant Messaging

4.6.1 Public instant messaging programs can expose computers and other communication devices to unauthorized intrusion and loss of data. The Best Practices Statement on Instant Messaging Security applies to all equipment attached to all state networks (BP-70-020).

4.7 Software Licensing

4.7.1 Software licenses may be purchased for use on a non-governmentally owned computer when that practice is part of the agency's draft policy on software licensing (PS-20).

4.7.2 Software licenses purchased by the state remain the property of the state and must be removed from a non-governmentally owned computer when the owner's relationship with that agency is terminated.

4.8 Equipment Maintenance

4.8.1 At the discretion of the director of the state agency, state funds may be used for equipment maintenance during an individual's tenure of state service.

4.9 Records Retention

4.9.1 Email and other electronic records of state business are subject to the provisions of *Act 918 of 2005* and other legislative and/or management requirements specific to the agency, board or commission.

5.0 Procedures

Agencies and institutions of higher education should classify, develop and disseminate policy defining acceptable use of non-governmental technical equipment with regards to state-owned data.

6.0 Revision History

Date	Description of Change
01/02/2007	Original best practices statement published.

7.0 Inquiries

Direct inquiries about this best practice recommendation to:

Office of Information Technology
Enterprise Architecture
124 West Capitol Avenue Suite 990, Little Rock, Arkansas 72201
Phone: 501-682-4300
FAX: 501-682-2040
Email: SharedArchitecture@arkansas.gov

OIT policies, standards and best practices can be found on the Internet at:
http://www.cio.arkansas.gov/techarch