

# Department of Finance and Administration

## Telephone and Information Technology Resources Policy and Procedures

March 2007

### I. Statement of Policy

The Department of Finance and Administration (DFA) makes extensive use of technological resources (**Resources**) in support of its day-to-day operations and in order to provide services to agencies throughout Mississippi government. This policy governs the use of all **Resources** in use by the Department. These **Resources**, whether leased or owned, include, but are not limited to the following: computers, computer-based communications networks, routers, firewalls, telephones, modems, cellular telephones, pagers, add-in modules, memory expansion boards, PCI cards, auxiliary hardware, facsimile transmission equipment, personal digital assistants (PDAs), printers, servers, e-mail, voice-mail, networks, custom developed and shrink-wrapped software, and applications, websites, files, whether electronic or paper or a combination, data of all forms including, but not limited to, digital recordings and photographs made to support business functions, and databases regardless of platform. This policy includes all **Resources** administered and hosted by DFA as well as the use of equipment, software, applications, and data controlled by other entities that have granted DFA users express approval to access these.

Under the federal statutes and the sections of the Mississippi code that regulate the use of these **Resources**, DFA is required to ensure that these **Resources** are used properly and for the purpose for which intended. The intent of this policy is to allow maximum freedom of use consistent with state and federal law, DFA policy, policies of the Department of Information Technology Services (ITS), and a productive working environment.

No employee of DFA may directly or indirectly use, or allow the use of the DFA's Resources for other than officially approved activity. Any restriction of use contained within this statement is intended to protect DFA's resources for DFA's intended use and for which funding is appropriated.

DFA contractors and contract workers are also required to adhere to this policy. A copy of this policy, where appropriate, will be included as a part of Requests for Proposals for services, Invitations to Bid for services, Request for Quotes for services, and any executed agreement for services involving the use of DFA's resources.

### II. Scope of Policy in General

A user is defined as any person employed by DFA, which includes full-time, part-time, temporary, contract employees, persons who are employed by contractors or subcontractors of DFA, and any other individuals who are authorized to use DFA's resources. These **Resources** are to be used for DFA business purposes only.

Individuals may use DFA's **Resources** only with the express authority of the Office of Information Technology (OIT), Mississippi Management and Reporting System (MMRS) or as authorized via an outside entity after approval for that access provided by the appropriate DFA Office Director, the Deputy Director, or the Executive Director.

DFA's **Resources** are not to be used for individual commercial purposes or financial gain, or for partisan political purposes. Activities having valid state citizenry benefit to DFA, but which are not specifically tied to routine work assignments, are generally allowed; however, they may be limited or banned at the discretion of OIT or MMRS, as appropriate, according to system load and system function.

Access to most Resources is through a specific user ID. The sharing of user ID's for **any reason is strictly prohibited**. Each user is responsible for all activity originating from his or her ID(s). All usage is to be for the benefit of state government and the citizens of the State of Mississippi.

Individuals found using DFA's **Resources** without express authorization are subject to disciplinary action and possibly criminal prosecution. Individuals found assisting others in gaining unauthorized access to DFA's **Resources** are subject to the suspension or revocation of all privileges, disciplinary action, and/or criminal prosecution.

Employees are hereby notified that DFA will enforce this policy through a variety of methods. Users should be aware that use of any of DFA's **Resources** are not to be considered private or confidential, and may be searched or monitored at any time to ensure compliance. All users are hereby notified that **Resource** security features allow messages and/or other usage to be monitored and archived regardless of passwords and message deletions. Access can be traced back to the individual.

The controlling office for this policy for all offices within DFA except for MMRS is OIT. The directors of OIT and MMRS will ensure that where rules must differ to ensure support of the applications within DFA's purview, that these policies and rules are consistent with the intention of the agency-wide policy statement.

Questions regarding this policy are to be directed to the Directors of OIT or MMRS, as appropriate, or to the Personnel Director. For any related issue not specifically addressed here, please ask your supervisor or the Personnel Director.

### III. Telephone and Telecommunication Procedures

- A. Generally, land-line telephones should be used for legitimate state business only; however, brief and occasional personal use is acceptable.
- B. Personal use of State-owned wireless communication devices, to include, but not be limited to, pagers, personal digitals assistants, and cell phones, is strictly prohibited.
- C. Long distance cellular calls that are not business related, long distance access codes, and state issued calling cards are never authorized for personal use.
- D. Personal use of phones and pagers must never directly or indirectly impede the conduct of state business.
- E. Access privileges may be revoked at any time and for any reason. Abuse of access privileges may result in appropriate disciplinary action.
- F. Employees need to be aware that cellular phone transmissions are not secure transmissions. Confidential information regarding official business should be made from a secure environment.
- G. Business facsimile/telefax transmissions shall include a confidentiality notice that shall limit delivery and distribution. A template for a fax cover sheet can be found at [www.dfa.state.ms.us](http://www.dfa.state.ms.us) under the DFA Forms link for General Policy.

### IV. Use and Management

- A. User Responsibilities
  - 1. No individual shall, without authorization, access, use, configure, reconfigure, destroy, alter, dismantle or disfigure DFA **Resources**.

2. If an individual encounters or observes vulnerability in **Resource** security or physical security, then that individual must report the vulnerability to OIT or MMRS, as appropriate. Individuals must refrain from exploiting any vulnerability in security.
  3. No individual shall use DFA **Resources** to gain illegal access or entry into other computers or networks. DFA users must follow any policies (which may be more restrictive than this policy) governing the use of any remote hosts accessed.
  4. **All users** are required to lock their PC when they step away from their workstation.
  5. **All users**, unless authorized to work remotely via a secure connection from home or another location outside of the office, are required to log-off the network and power down their PC when leaving the DFA facilities each day.
  6. Publishing or distributing in any manner information that enables or encourages unauthorized access to any **Resources** is specifically prohibited.
  7. Illegal, fraudulent or malicious activities are expressly prohibited, as are partisan political activities, religious lobbying or proselytizing, and political lobbying.
  8. Activities for the purpose of personal or commercial gain are expressly prohibited.
  9. Any use of DFA **Resources** that violate the privacy of any other individual is prohibited.
  10. The creation or transmission of defamatory material is expressly prohibited.
  11. Users must respect the finite capacity of systems.
  12. Printing or displaying materials (images, sound, messages) that are unsuitable for public display or that could create an atmosphere of discomfort or harassment for others are prohibited.
  13. Representing personal opinions as official DFA statements is strictly prohibited.
  14. **Resources** are not to be used in a wasteful or frivolous manner. Examples of misuse include, but are not limited to, tying up system or network resources, sending trivial or excessive messages, publishing personal web pages, downloading music, **“chat” and “instant messaging”**, printing excess copies of documents or files, running grossly inefficient programs, running unauthorized jobs against production database files, and Internet radio (audio) streaming. Internet video streaming is permitted only for participation in duly authorized web seminars.
  15. Individuals must not attempt to circumvent or subvert **Resource** security measures.
  16. No user is **ever** authorized to give out their password for access to DFA Resources.
  17. **All employees must protect their User IDs. Activity tied to your ID can and will be used against you if use is determined to be improper or unauthorized.**
- B. Hardware
1. All **Resources** are the property of the State of Mississippi and should not be used for purposes other than business.
  2. Except for appropriately issued **Resources** used in daily offsite work, no **Resources** should be removed from office premises without the permission of OIT or MMRS, as appropriate. In the event a **Resource** is to be off premises for some time, the employee responsible for the **Resource** must file a written hand receipt with the Director of OIT or MMRS, as appropriate.
- C. Software
1. Software shall not be installed on a **Resource** by anyone other than a duly authorized representative from OIT or MMRS, as appropriate. Software is also not to be downloaded from the Internet for installation without the express authorization of a duly authorized representative from OIT or MMRS, as appropriate. **You are expressly prohibited from downloading “BONZI”, “GATOR”, “WEBSHOTS”, or similar programs.** The agency’s network contains software that performs an inventory of each PC on a regular basis to ensure compliance with this rule.
  2. No software is to be installed locally (i.e., C: drive) without prior approval from OIT or MMRS, as appropriate.
  3. Use of inappropriate graphics in your wallpaper and/or screensaver can be considered harassment and is strictly prohibited.

4. Software owned or licensed by DFA may not be copied to alternate media, distributed by e-mail, transmitted electronically, or used in its original form on non DFA **Resources** unless performed by or with express written permission from OIT or MMRS, as appropriate.
5. Software copyrights are never to be violated.
6. Standard software is to be used for all internal functions. Approved non-standard software is only to be used to interface with customer or vendor organizations when they require the non-standard software and then only after written approval by OIT or MMRS, as appropriate.
7. Software licensed to DFA is to be used for its intended purpose according to the license agreement. Employees are responsible for using software in a manner consistent with the licensing agreements of the manufacturer. License agreements are maintained by OIT or MMRS, as appropriate.
- 8. Recreational game playing on DFA resources is expressly prohibited.**
9. DFA system and network administrators will take reasonable precautions to ensure that potentially offensive materials do not reside on local facilities; however, DFA cannot be held responsible for materials residing on remote sites.
10. Individuals who transfer offensive material to DFA **Resources** will be disciplined.

## V. Practices

- A. No materials are to be disseminated in any manner which are derogatory to any person or group, obscene, racist, sexist, harassing or offensive based on color, religion, creed, national origin, age or disability.
- B. System identification codes and passwords are for the use of the specifically assigned user and are to be protected from abuse and/or use by unauthorized individuals.
- C. All diskettes, e-mail attachments and executable e-mail messages are automatically scanned for viruses using the virus detection software installed on all computer workstations which have been configured by OIT or MMRS, as appropriate.
- D. Users are **never to disable virus protection software** unless expressly authorized by the director of OIT or MMRS, as appropriate.
- E. No configuration changes are to be made to **Resources** assigned to you without the express written permission of OIT or MMRS, as appropriate. If you have made any configuration changes to your workstation, even with the approval of OIT or MMRS, as appropriate, it is your responsibility to ensure virus protection prior to opening/executing diskettes, e-mail attachments or executable e-mail messages.
- F. Internet access and e-mail are for work-related use. Access and sites visited can and will be monitored at the specific individual level. All messages and files created are and will remain the property of the State and DFA. DFA reserves the right to retrieve and review any message or file composed, sent or retrieved. It should be noted that although a message or file is deleted or erased, it is still possible to recreate the message.
- G. Information contained on the agency network and workstations is strictly proprietary to the State of Mississippi and DFA. Copying or disseminating any of this information for any purpose other than State business is strictly prohibited. Access to this information must be considered confidential.
- H. You are expected to report violations of this policy, which you observe to your supervisor, or, in the event that the violation involves the supervisor, the Personnel Director. Likewise, if you are a witness to a violation you are required to cooperate in any investigation of the violation.
- I. Questions about the legal use/installation of resources should be directed to OIT Help Desk at 601-359-3695 or the MMRS Network Manager at 601-359-1302, as appropriate.

**VI. Consequences**

Statutes governing the use of these **Resources** include, but are not limited to, the Mississippi Computer Statutes (Sections 97-45-1 through 97-45-13 of the Mississippi Code of 1972 [1994]), Section 25-53-191 and the Federal Computer Fraud and Abuse Act of 1986. According to the U.S. Copyright Statutes, illegal reproduction of software can be subject to civil damages of \$50,000 or more, and criminal penalties including fines and imprisonment. Under the Mississippi Computer Crimes Law, the maximum fine is \$10,000 and the maximum imprisonment sentence is five years.

Any user who knowingly and willingly violates this policy is subject to discipline up to and including:

- ! Limiting or prohibiting public access to files or directories on WWW, gopher, or FTP servers;
- ! Suspension for varying amounts of time or the permanent revoking of **Resource** access privileges;
- ! Contract termination;
- ! Issuing a reprimand or administering other disciplinary action in accordance with the procedures documented in the *Mississippi State Employee Handbook*;
- ! Reporting of the violation to the appropriate disciplinary organizations for users not directly associated with DFA;
- ! Referral to the appropriate law enforcement agency in cases of violations of state or federal law.

DFA reserves the right to immediately restrict access privileges of individuals who have violated this policy until suitable, comprehensive disciplinary action is determined. Action may be taken immediately by DFA in any case of suspected violation of this policy. The affected user will be notified when such action is taken and may file any resulting grievance according to the grievance procedures outlined in the SPB Policies and Procedures Manual.

**VII. Revision**

This policy is subject to revision. When revised, users/employees will be expected to sign the updated version of the policy. A copy of the signed policy will be placed in each employee's personnel file or in the file of the contractor, temporary worker, or contract employee, as applicable.

**VIII. Acknowledgement**

Acknowledgment of this policy statement authorizes DFA to examine and monitor **Resources** assigned to DFA employees, if necessary. DFA reserves the right to stop any process, restrict any individual's use, inspect, copy, remove or otherwise alter any **Resources** that may undermine or adversely affect the overall performance or integrity of the computing facilities or is otherwise in violation of this policy.

**Acknowledgement of Receipt**

\_\_\_\_\_  
Employee's Name (Please Print)

\_\_\_\_\_  
Employee's Signature

\_\_\_\_\_  
Date

**Cc: Personnel File or Contract File**

Initials _____
Date _____