POLICY FOR TREATMENT OF SOCIAL SECURITY NUMBERS (SSNs)

Department of Finance and Administration (DFA) V2 04/17/2004

I. INTRODUCTION

The Department of Finance and Administration (DFA) is cognizant of the fact that it is necessary to record, store, process and transmit personal information in the form of social security numbers (SSNs) in order to conduct and maintain many of the business processes carried out by agencies of the State through the systems applications maintained by various offices of DFA. DFA takes its responsibilities with respect to the use of SSNs seriously and seeks to provide functional and secure systems for the appropriate handling of this information through the use of administrative, technical, personnel, and physical safeguards.

II. PURPOSE

In response to public concern and in an effort to comply with Section 25-1-111, Mississippi Code of 1972, Annotated, as amended, DFA has established the following policies regarding treatment of SSNs by users of any DFA maintained systems applications.

III. POLICIES

1. Access

   Access to SSN information by any individual shall be provided only in compliance with existing DFA security policies for the various systems applications. Individuals should be granted access to SSN data only if there is a demonstrated and legitimate need to know based upon normal job duties and falling within the purpose and scope for which the data was collected. Agencies authorizing such access to their employees or contractors accept the inherent responsibility for any breaches of confidentiality carried out by these individuals.

2. Collection of Information

   SSN information will be entered into DFA applications only by authorized individuals at the agency level or by authorized DFA staff as requested by agencies in accordance with DFA policies. Changes to SSN information that cannot be completed at the authorized agency level shall be accomplished by authorized DFA staff upon receipt of appropriate documentation from the agency and should be treated with the same level of confidentiality as the original information it replaces.

3. Disclosure of SSN Information

   SSN information should not be disclosed to persons or entities not meeting the criteria as stated above, or unless permitted by applicable law. More specifically, SSN information is exempt from inclusion as public record information and is never to be provided in response to such requests.

4. Disposal of SSN Information

   Destruction of SSN information that is no longer needed or required by law should be handled in an approved manner. Hard copies of reports, "screen prints", or other forms of documents containing SSN data should be shredded. Destruction of computer disk, media, and other data storage systems should be completed using accepted methods that will not enable inappropriate recovery of data.

5. Inadvertent Disclosure

   The display screens for all PCs, workstations, and terminals used to view or process sensitive data should be positioned such that unauthorized people cannot view them. Hardcopies of documents containing SSN information (such as printed reports, "screen prints", etc.) should be promptly picked up from printers and kept in secure areas until destroyed.

6. Testing and Training

   The same levels of security and control of SSNs should be utilized for testing and training purposes as is exercised in Production systems applications.

7. Expectation of Compliance

   Individuals and entities are expected to comply with laws and policies pertaining to the collection and use of SSNs and are expected to take the steps necessary to protect this information.