Office of Legacy Management

Computer Security Rules of Behavior

1. Introduction

The following rules of behavior are to be followed by all users of the Office of Legacy Management (LM) network. The rules clearly delineate responsibilities of and expectations for all individuals with access to the LM network. Noncompliance of these rules will be enforced through sanctions commensurate with the level of infraction. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

2. Responsibilities

The Information Systems Security Site Manager (ISSSM) is responsible for ensuring an adequate level of protection is afforded to the LM network through an appropriate mix of technical, administrative, and managerial controls. The ISSSM develops policies and procedures, ensures the development and presentation of user and contractor awareness sessions, and inspects and spot checks to determine that an adequate level of compliance with security requirements exists. The ISSSM is responsible for periodically conducting vulnerability analyses to help determine if security controls are adequate. Special attention will be given to those new and developing technologies, systems, and applications that can open or have opened vulnerabilities in the security posture of the LM network.

3. Other Policies and Procedures

The rules are not to be used in place of existing policy; rather they are intended to enhance and further define the specific rules each user must follow while accessing the LM network. The rules are consistent with the policy and procedures described in *U.S. Department of Energy, Office of Legacy Management, Grand Junction Location Unclassified Computer Security Program.*

4. LM Network Rules

4.1 **Authorized Use.** LM network users are authorized by the activity/functional manager. Users are authorized to perform only those functions that are consistent with their job duties.

4.2 **Individual Accountability.** Access to the LM network is controlled through unique passwords. Users must use only the ID and password assigned to them.

Computer Security Rules of Behavior (continued)

4.3 **User passwords.** Passwords will conform to the general LM network password requirements, including the use of a strong password, which is a password made up of letters, numerals, and symbols, and protection from disclosure of that password.

4.4 **Unattended computers.** When connected to the LM network, unattended computers will have a password-protected screensaver activated.

4.5 **Connection from off-site locations.** Access to the LM network is permitted from off-site locations, provided the access method is approved by LM and includes authentication and encryption mechanisms adequate to protect the LM network and data.

4.6 **Protection of software copyright licenses.** LM network users must comply with copyright licenses and not install software on any computer system other than the system for which it is issued, not duplicate software, and not resell software. Failure to comply with copyright laws is a criminal offense. Failure to adhere to company policies and procedures may result in disciplinary action, up to and including termination of employment, and any unauthorized use of computing resources is subject to criminal and civil penalties.

4.7 **Unofficial use of government equipment.** Users should be aware that personal use of information resources is not authorized.

4.8 **Application and data awareness.** It is the user’s responsibility to know what applications are processed on the assigned hardware. The user must know where the data is stored, and must protect the data and software commensurately with its value to the business. It is the user’s responsibility to comply with all policies and procedures to safeguard the data from unauthorized access or disclosure.

I, the user, understand that the computer hardware, software, and Internet access used in relation to this form is government property and may only be used to conduct government business. In using these computing resources, I understand that I have no expectation of privacy (implied or otherwise) and the use of government computer resources is subject to monitoring and review. I acknowledge receipt of these rules, understand my responsibilities, and will comply with the rules of behavior for the LM network.

Signature of User

Date