OPM COMPUTER USER RESPONSIBILITIES

As a user of OPM's computer systems, you are expected to understand and comply with the responsibilities outlined below. You will be held accountable for your actions when using these systems. If you violate OPM policy regarding these responsibilities, you may be subject to administrative action ranging from counseling to removal from the agency, as well as any criminal penalties or financial liability, depending on the severity of the misuse.

Privacy While Using Government Equipment – You do not have the right to privacy while using any Government equipment, including Internet or email services. Furthermore, your use of Government office equipment, for whatever purpose, is not secure, private, or anonymous. While using Government office equipment, your use may be monitored or recorded.

Protection of Software, Data, and Hardware – You are not allowed to introduce any unauthorized software and data (including software and data protected by copyright, trademark, privacy laws, other proprietary data, or material with other intellectual property rights beyond fair use), hardware, or telecommunication devices or modify any configurations. You are not allowed to interconnect to other computer systems or networks without the authorization of OPM's chief information manager. Access to the Internet via the OPM network is authorized. In addition, you will protect all sensitive information residing in OPM computer systems, preventing unauthorized access, use, modification, disclosure, or destruction of that information. This includes records about individuals requiring protection under the Privacy Act, sensitive financial information, and information that cannot be released under the Freedom of Information Act. Disclosure of sensitive information, trade secrets, and intellectual property to unauthorized individuals is also prohibited.

Service Restoration – The availability of the computer systems is a matter of importance to you. You are responsible for assisting in any way that you can for restoring service in the event that the computer systems become non-operational. Priority is given to restoring the general support systems and the applications supporting OPM's mission-essential functions as defined in the agency's Continuity of Operations Plan (COOP).

System Privileges – You are given access to the computer systems based on a need to perform specific work at OPM. You are expected to work within the confines of the access allowed and are not to attempt to access systems or applications for which access is not authorized.

Telecommuting – The OPM Human Resources Handbook, Chapter 368, Telecommuting, contains the policy and procedures for authorizing telecommuting. In general, immediate supervisors approve, on a case-by-case basis, employee requests to telecommute. Telecommuters who access OPM's general support systems must adhere to all IT security policy and procedures that would apply if the individual was accessing OPM's systems in the office. Dial-in access for telecommuters or other users whose job functions may require it is authorized by the chief, Network Management Group.

Use of Government Office Equipment – You will comply with the policies specified in the OPM Policy on Personal Use of Government Office Equipment.

Use of Passwords – You will create and use passwords as specified in the Information Security and Privacy Policy. You must keep your passwords confidential and not share them with anyone.

Individual applications may have more stringent password requirements than the general policy requirements.

NOTE: This document is extracted from and supports OPM's Information Security and Privacy Policy Volume 2 as approved in July 2009.