

Introduction

Controls are needed for Remedy to ensure all users are accountable for their own actions and to protect mission-related data and equipment from malicious and accidental loss or damage. The following rules have been developed to govern the behavior of all Remedy users to ensure they know and accept their responsibilities with respect to Remedy security. Individuals must agree to conform to these rules. Consequences for violating Remedy Rules of Behavior vary according to the seriousness of the violation.

Minor infractions of the rules will result in management notification. More serious or continued infractions will result in the loss of system privileges. Major infractions that violate United States law, Department of Defense directives or regulations, will be referred to the office of the Inspector General for investigation and disciplinary action, which may include dismissal and/or criminal prosecution.

Remedy Rules of Behavior are listed in Table 1-1 below.

APPLICABLE TO	AREA	RULES
All Users	General Security	Users must ensure that the network resources and automated information systems (AISs) which they have been entrusted with are used properly, taking care that the laws and regulations governing the use of such resources are followed and that the value of all information assets are preserved.
		Each user is responsible for any and all activity performed under their assigned user ID.
		Users must be knowledgeable of Remedy security features and policies and seek additional information if it is not adequately provided during system training.
		Users are given access to this system based on a need to perform specific work. Users shall work within the confines of the access allowed and shall not attempt to access systems or applications to which access has not been authorized.
		Users must not circumvent any Remedy security control mechanism.
		Users must not read, alter, insert, copy, or delete any Remedy data except in accordance with their assigned job responsibilities. Ability to access data does not equate to authority. In particular, users must not browse or search Remedy data except in the performance of their authorized duties. It is a violation of federal law to access US Government data in excess of one's authorization (18 USC 1030).
		Users must not reveal information produced by Remedy except as required by their government job function and within established procedures.
		Users must notify supervisors when a particular access or authority is no longer required to perform their approved duties.
		If required, users must provide assistance with security audits and reviews.
		Users must report any known security breaches to their security officer, the Remedy Help Desk and/or other Remedy management immediately after discovery of the occurrence.
		Users shall protect sensitive information from disclosure to unauthorized individuals or groups. Classified information is not authorized for this system.
		Users must report any attempts of bribery or extortion or any instances thereof to their management immediately.
Users must ensure that anyone seen using a Remedy workstation in the area is authorized to do so.		

Remedy System Rules of Behavior

APPLICABLE TO	AREA	RULES
		Before accessing sensitive or Privacy Act information via Remedy, users must ensure that no unauthorized individuals can view their screen contents.
		Users must not leave an active workstation unattended. Active workstations may be locked (by using the authorized mechanisms) while unattended.
		Users must follow proper Remedy logon and logoff procedures.
	Passwords	Users must protect user IDs and passwords from improper disclosure. Passwords provide Remedy access and are specifically assigned for accountability purposes. Users are responsible for any access made under their logon ID.
		Do not reveal passwords under any circumstances. If password disclosure occurs, immediately select a new one and report the disclosure to the ISSO.
		Do not share passwords with anyone else or use another person's password.
		Do not write passwords down.
		Change passwords at least every 90 days.
		Change passwords immediately if others know them.
		Choose "hard-to-guess" passwords by mixing upper and lower case letters, and at least one special and one numeric character.
		Do not use, in forward or backward sequence, whole or partial words, acronyms, or repetitive or commonly sequenced strings of three or more characters. Do not use strings of three or more characters from the previous five passwords, or a password based on intentional substitution of a part of any previous password.
	Media	Ensure that paper copies of sensitive and private information are properly secured when not in use, and destroyed when no longer needed.
		Use proper procedures to dispose of media that is no longer needed.
		Shred sensitive documents or place them in special collection bins where authorized personnel will collect them and ensure their proper destruction. Shred reports down the page instead of across.
		Ensure that floppy disks (and other storage media) are wiped before they are removed from a protected environment or reused for other purposes.
Do not remove Remedy data from the workspace without written authority from Remedy management.		
System Administrators, Network Administrators, Application Developers, Troubleshooters, and Remedy Support Personnel	Misc. Admin Security	Support personnel will not read or alter any data except as required to complete the support duties assigned to them.
		Except for Network and System Administrators, and Remedy Help Desk staff, support personnel will not define new users to Remedy or alter user access privileges except on an emergency basis. After emergency procedures, control of user access will be returned to normal user administration as soon as possible.
		Support personnel will inform Remedy management of any special procedures or conditions, which may temporarily or permanently alter Remedy's security features.
		Support personnel will inform Remedy management of any maintenance performed on any Remedy system security mechanism.
		Support personnel will inform Remedy management of any diagnostic test result which indicates that a system security mechanism is not functioning properly.
		Support personnel will not change any information in any audit log under any circumstances.
		Support personnel will inform Remedy management in advance (except for emergencies) of any support procedure that involves disabling any audit log.
		Support personnel will ensure that any copies of sensitive information is properly secured and properly disposed of when no longer needed.
		Configuration Managers
Configuration managers will not introduce any unapproved components into Remedy.		

Non-Compliance

Any violation of the rules of behavior shall be considered a security incident. If the incident is deemed willful, it will be escalated to a security violation. Depending on the number of security violations and the specific information involved, disciplinary action for the violation may consist of a letter or warning/caution, or revocation of access to the Remedy System. The individual may also be subject to criminal prosecution.

Acknowledgement

By logging into and accessing the Remedy System, users acknowledge that you understand and will comply with these rules of behavior when using the Remedy System. Non-compliance or behavior inconsistent with these rules can result in immediate suspension from the Remedy System or disciplinary action, which may lead to a formal criminal investigation, as appropriate.