U.S. DEPARTMENT OF LABOR

Office of Workers' Compensation Programs

ECOMP RULES OF BEHAVIOR

OFFICE OF WORKERS' COMPENSATION PROGRAMS (OWCP)

DIVISION OF FEDERAL EMPLOYEES COMPENSATION (DFEC)

VERSION 1.2

CONTROLLED UNCLASSIFIED INFORMATION

Introduction

What are Rules of Behavior (ROB)?

Rules of Behavior (ROB) are a set of regulations that define the responsibilities and expected behavior of all individuals who electronically file claims via the Employees' Compensation Operations and Management Portal (ECOMP). Every user must understand that taking personal responsibility for the security of their computer workstation and the data it contains is an essential part of their job.

ROB are based on principles, regulations, standards, and guidance initiated by Congress, Presidential Directives, the Office of Management and Budget, and the National Institute of Standards and Technology. These guidelines make all users responsible for information system security and hold them accountable for actions that threaten that security.

What is the purpose of ROB?

The intent of OWCP's Rules of Behavior is to summarize the Federal, DOL, and OWCP regulations and policies that determine how we must secure our information and information systems.

ROB are part of the OWCP information system security program. This program includes a broad set of policies and standards that ensure the information and information technology resources are always available, reliable, and secure.

Who is covered by these Rules?

The ROB contained in this document must be followed by all users who access ECOMP. Users will be held accountable for their actions and federal or contract employees who violate OWCP's ROB may face disciplinary action.

It is every user's responsibility to keep informed about all DOL and OWCP, policies, procedures, and guidance that pertain to information system security.

Regulations that govern the use of federal information security resources include:

- Federal Information Security Management Act of 2002. http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
- Office of Management and Budget (OMB) Circular A-130, Revised. http://www.whitehouse.gov/omb/circulars/a130/a130.html
- 5 C.F.R. PART 2635 - Standards of Ethical Conduct for Employees of the Executive Branch. http://www.usoge.gov/laws_regs/regulations/5cfr2635.aspx
- Privacy Act 1974 As Amended. http://www.archives.gov/about/laws/privacy-act-1974.html
- National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/

What are the penalties for non-compliance?

Users who do not comply with the ROB are subject to penalties that can be imposed under existing policy and regulations, including:

- official written reprimands
- suspension of system privileges
- temporary suspension from duty
- removal from current position
- termination of employment
- criminal prosecution

OWCP will enforce the use of penalties against any user who willfully violates any OWCP, Department, or Federal system security (and related) policy.

The “ECOMP User Rules of Behavior” are based on the following eight principles of behavior:

- Restricted Use
- Accountability
- Access
- Confidentiality
- Integrity
- Authentication and Identification
- Awareness
- Reporting

Restricted Use

Respect OWCP/DFEC's sole ownership of ECOMP and its assets, including but not limited to:

- electronic or printed data
- electronic or printed information
- intellectual properties
- technical design and implementation
- and hardware and software technologies

Use information and data belong to ECOMP for ECOMP related business only

Do not use ECOMP information for private gain

Avoid the appearance of using ECOMP information in a way that is counter to laws and ethical standards

Do not use ECOMP information in way that would adversely affect public confidence in the integrity of the users' agencies and OWCP/DFEC

Do not tolerate nor collaborate with anyone who uses ECOMP sensitive information for other than official purposes

Accountability

Adhere to standards of conduct prescribed by OWCP, DOL, and Federal regulations

Behave in an ethical, informed, and trustworthy manner

Acknowledge actions and accept responsibility for correcting errors and rectifying problems

Log out of the ECOMP web site when finished using the system or leaving their computers

Avoid or use caution when accessing ECOMP from public computers or on a public or unprotected network

Keep computers updated with the latest security updates for operating system and antivirus software

Access

The following users are granted access to ECOMP via individually assigned user accounts:

- Super Agency Maintenance User (Super AMU)
- Agency Maintenance User (AMU)
- Agency Reviewer (AR)
- Agency Representative (ARi)
- Occupational Safety and Health Administration (OSHA) Record Keeper (ORK)
- Claimants

The following users are granted access to ECOMP on a one-time use basis and are not required to have a user account:

- Supervisors who have received a request to review a form
- Individuals who have sufficient information and authority to view the status of a form or document submission

Do not use granted access rights to exploit system controls or access data for any reason other than in the performance of official duties

Access and use only information for which users have official authorization

Remove associated accounts as soon as a Super AMU, AMU, AR, ARi or ORK is no longer eligible to have access to ECOMP

Grant access to ECOMP based on the user's duties

Follow "least privilege" and "need-to-know" practices when granting a user access

Confidentiality

Encrypt ECOMP data with the latest approved encryption technology when storing or transmitting data

Limit the use of portable storage media, devices

Protect confidential and/or sensitive information from disclosure

Limit sharing of ECOMP information only with users who have the need to know, in regard to ECOMP related business

Understand users' responsibilities under the Privacy Act <hyperlink to Privacy Act> to protect information that is transmitted through and resides in the ECOMP system from improper disclosure

Prevent unauthorized people from viewing the information whether on the network drive, computer screen or on paper

- Store data on approved network drives / folders, according to users' agency policies and federal regulations
- Ensure that the data stored on the network drives / folders are not accessible by unauthorized users
- Ensure that the computer monitor is not directly facing a public access area that could allow an unauthorized person to see the contents displayed on the monitor
- Protect physical copies from getting lost
- Do not leave printouts unattended
- Ensure that faxes are sent to the correct fax numbers and the recipients are aware of the incoming faxes

Integrity

Obtain training before using ECOMP to learn how to correctly enter and change data

Ensure that the information which users manage, and for which they have responsibility, is accurate and up-to-date

Prevent unauthorized changes, destruction, or tampering with information

Do not manipulate information inappropriately

Use protective measures to ensure against accidental loss of information integrity

Create only authorized records

Password and User ID

Safeguard passwords from access by other individuals

Change passwords every 60 to 90 days as directed by system warnings

Create complex passwords as directed by system on-line help pages

Do not share passwords or account information

Use only the user accounts to which users have been assigned to access the system

Protect accounts by memorizing passwords and never write them on paper or store them in an electronic file or a password vault

Change passwords immediately should users suspect that someone else knows their passwords

Awareness

Complete annual Information System Security Awareness training

Read security information available to ECOMP users through user manuals, electronic mail, log in messages, and other sources

Follow all procedures and comply with all written policies related to ECOMP security

Maintain up-to-date essential knowledge of computer security

Reporting

Report computer security and personally identifiable information (PII)-related incidents, or any incidents of suspected fraud, or misuse of ECOMP to the appropriate authorities and ECOMP Representatives immediately

Report security vulnerabilities due to software, or system glitches and exploitations of such vulnerabilities to appropriate authorities and ECOMP Representatives immediately

Report manual or automated data collection from ECOMP for non-ECOMP related business to the appropriate authorities and ECOMP Representative immediately, including but not limited to:

- data mining
- digital imaging
- duplication of electronic or physical files or records
- manually recording data on paper or computing devices