



Version	Date	Author	Description of Change
1.0	6-04-13	M. Klosterman	Original

USGS EROS ADMINISTRATIVE PROCEDURE

COORDINATION:

[Redacted signature area]

EROS Director Deputy Director Administrative Officer

SUBJECT / TITLE: Elevated Privilege (PR) Account Access

DATE: June 4th, 2013

VOL / INDEX #: EROS-IS-01

PREPARED BY:

Copies will be provided to:

[Redacted name]

Preparer Date Supervisor Date

OTHER COORDINATION: GS-N-EDC Federal Employees
CORs distribute to contracts.

STATUS: Permanent
 Temporary

EXPIRATION DATE: June 4th, 2014

PROCEDURE / MEMO: Original
 Supersedes

ATTACHMENT TO: N/A

PURPOSE: To provide guidance for elevated privilege account access
to EROS Production / Business Systems.

UTILIZATION: Daily, Weekly, Monthly, Other

TEXT: Procedure follows on next page.

1.0 References and Authorities.

FISMA

<https://collaboration.usgs.gov/wg/erosdc/infosec/Reference/Legislato/FISMA-FederalInformationSecurityManagementAct>

FIPS

<https://collaboration.usgs.gov/wg/erosdc/infosec/Reference/NIST/PubsFIPS.pdf>

NIST

<https://collaboration.usgs.gov/wg/erosdc/infosec/Reference/NIST/SP.800-53r4.pdf>
https://collaboration.usgs.gov/wg/erosdc/infosec/Reference/NIST/nistir_7298r2_pre-publication.pdf

DOI

DOI Security Control Standards

[https://portal.doi.net/CIO/ITPMgmt/Documents/IT_Standards/IT_Security/DOI_Security_Control_Standards_\(based_on_NIST_SP_800-53_Revision_3\)](https://portal.doi.net/CIO/ITPMgmt/Documents/IT_Standards/IT_Security/DOI_Security_Control_Standards_(based_on_NIST_SP_800-53_Revision_3))

DOI Rules of Behavior

http://internal.usgs.gov/gio/security/doi_it_rules_of_behavior.pdf

USGS

Separation of Credentials

http://internal.usgs.gov/gio/security/rierson_separation_of_credentials_memo_2006_03_07.html
http://internal.usgs.gov/gio/security/standard_usgs_separation_of_credentials.doc

EROS

USGS/EROS Rules of Behavior

https://edchome.cr.usgs.gov/ecms/upload/spetersw/files/Shared/User%20Forms/USGS_and_EROS_IT_RULES_OF_BEHAVIOR-2011.doc

2.0 Purpose.

The purpose of this procedure is to provide guidance for elevated privilege account access to a USGS EROS production system. It applies to all users with elevated privileges beyond standard user access on computing devices connected to USGS EROS Center information systems.

The Federal Information Security Management Act (FISMA) requires federal agencies to implement information systems security controls in accordance with National Institute of Standards and Technology (NIST) and the Federal Information Processing Standard (FIPS). This procedure addresses control requirements to formally address privileged account management.

3.0 Definitions.

Configuration Control – Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation.

Elevated Privilege (PR) Account – An information system account with approved authorizations of a privileged user. Other names for elevated privilege accounts include, but are not limited to: privileged account; administrator; root; super user; etc.

EROS Information Security Manager (EISM) – EROS Centerwide Information Security Manager.

EROS PR Account Rules of Behavior – Rules of behavior specific to elevated privilege account access. See Appendix A of this procedure.

Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
[Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.]

Line of Business – The following Office of Management and Budget (OMB)-defined process areas common to virtually all federal agencies: Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure.

Privileged User – A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Production/Business Systems – Information systems supporting a line of business.

Sensitive Information (SI) – Information that requires protection due to the risk and magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, loss, corruption, or destruction of the information. Sensitive information includes, but is not limited to: proprietary data, records about individuals requiring protection under the Privacy Act, data such as payroll, financial, or management information, or data that is critical to the mission of the USGS. Passwords, pass phrases, personal identification numbers, and social security numbers (whole or partial) are among items that are considered sensitive information. Sensitive information includes personally identifiable information (PII).

System Owner – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system..

User – Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

4.0 Requirements and Responsibilities.

Elevated privilege accounts are restricted to users that require elevated privileges as a requirement of their IT responsibilities. Recognized roles include, but are not limited to:

- System Administrators
- Network Administrators
- Desktop Support Staff
- Server Application Administrators
- Data Base Administrators
- Web Administrators

All elevated privilege accounts will be set to expire after one year. Recertification/renewal will be required annually, and the elevated privilege account holder is responsible for ensuring they have recertified prior to the expiration date or their account may become disabled.

Unused elevated privilege account passwords will expire after 30 days. Expired elevated privilege accounts will be deleted or disabled and the user will need to re-apply for the account.

Elevated privilege account holders are required to sign the Elevated Privilege Account Rules of Behavior and successfully complete annual Role Based Security Training.

Elevated privilege account holders are responsible for any systems changes or software they install.

Elevated privilege account passwords shall not be written or stored electronically using unapproved methods. Approved methods of storing passwords include EROS/FIPS approved methods, and a paper copy stored under lock and key.

By granting approval for an elevated privilege account, the system owner accepts the risk(s) associated with elevated privilege accounts to their systems.

For all elevated privilege accounts, the principle of "least privilege" is required. Elevated privilege accounts shall only be used to the extent and period of time necessary to complete required job functions.

The EROS Director has directed the EROS Information Security Manager to report on projects and user compliance with privileged access policy.

5.0 Violations.

Any employee or contractor, who is requested to undertake an activity which he or she believes is in violation of this procedure, must provide a written or verbal complaint to his or her manager, any other manager, or their Human Resources Department, as soon as possible.

6.0 Appendices.

Appendix A. EROS Elevated Privilege Account Rules of Behavior.

Appendix A. EROS Elevated Privilege Account Rules of Behavior.

EROS Elevated Privilege Account Rules of Behavior

1. Elevated privilege account passwords shall be unique, different passwords for their privileged and non-privileged accounts, and shall be changed every 60 days.
2. Elevated privilege account holders:
 - a. may only use their elevated privilege accounts to perform administrator functions.
 - b. may not use their elevated privilege accounts for web browsing; unauthorized viewing, modification, copying, or destruction of system or user data.
 - c. are required to complete role based training specific to elevated privilege accounts.
 - d. are required to submit a plan for the maintenance and patching of hardware and software not installed by the EROS Centerwide IT Team.
 - e. are prohibited from installing unauthorized software as defined in the DOI Security Control Standards.
 - f. have a responsibility to protect the confidentiality of any information they encounter while performing their duties.
 - g. are responsible for complying with all applicable copyright laws in addition to the regulations, policies, and procedures listed in the 1.0 Reference section of the EROS-IS-01 Elevated Privilege (PR) Account Access Procedure.
 - h. acknowledge obtaining an elevated privileged account places them in a position of considerable trust. Elevated privilege account holders must not breach that trust by misusing privileges or failing to maintain a high professional standard.
 - i. must follow applicable configuration control processes when making changes to the system.
 - j. acknowledge that failure to comply with the policy may result in immediate removal of the elevated privilege account and disciplinary action.
 - k. will abide by the conditions outlined in this agreement in addition to other rules of behavior they have signed.

- l. agree to recertify the need for the privileged account on an annual basis.
 - m. acknowledge additional monitoring of elevated privilege accounts may occur.
 - n. agree to use unique complex passwords of at least 12 characters for the elevated privilege accounts.
 - o. agree not to change applicable system settings defined by DOI/USGS/EROS Security Technical Implementation Guide(s) (STIG) without written authorization.
 - p. agree to notify the EROS Information System Manager and change the password immediately if the elevated privilege account password is inadvertently disclosed.
 - q. agree to minimize the use of the elevated privileged account by:
 - i. not reading or sending email, web browsing, or performing internet downloads with the elevated privileged (PR) account.
 - ii. agree to utilize single-use elevated privilege account commands such as "run as" or "su" when possible.
3. I understand that:
- a. elevated access on the computer systems in my area of responsibility is a privilege.
 - b. I am responsible and accountable for all actions performed through my elevated privilege account.
 - c. intentional abuse of USGS data processing resources, actions resulting in disclosure of sensitive information, or failure to follow security procedures may result in disciplinary action and the immediate loss of special access privileges on USGS / EROS systems.