



ECO RULES OF BEHAVIOR

EL-CID Online

January 7, 2022

Version 2.1

Version History

Date	Version	Document Status	Author/Editor
March 30, 2020	1.0	Review for A&A 2020	Robert Hite
October 20, 2021	2.0	Updated for EL-CID Online	GDIT
January 7, 2022	2.1	Updated for EL-CID Online	GDIT

1.0 Objective

The Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources requires that “Rules of Behavior” be established for each general support information technology (IT) system and major application processing government information. At the National Telecommunication and Information Administration (NTIA), these Rules of Behavior establish the principles for the use of National Telecommunications and Information Administration (NTIA) and Department of Commerce (DOC) information technology (IT) resources. The purpose of these rules is to increase individual awareness and responsibility and to ensure that all users utilize IT resources in an efficient, ethical, and lawful manner.

The Rules of Behavior are standards set to hold users accountable for security-relevant actions. They should be disseminated through the organization’s training and awareness program. All users are required to sign and date that they have read and understand the Rules Of Behavior for EL-CID Online ("ECO Rules of Behavior").

2.0 Responsibilities

1. The user has to sign the System Authorization Access Request (SAAR) form to get an account and right to access the EL-CID Online internal system.
2. The user ID and password are only to be used by the individual who is assigned, and should not divulge to any unauthorized user. Any group ID or group password is prohibited. The EL-CID Online users will manage the password in accordance with the DOC Policy on Password Management and the password management policy contained within NTIA’s IT Security Policy.
3. When the user uses the National Telecommunication and Information Administration resources, the user consents for monitoring and security testing to ensure proper security and appropriate usage.
4. The EL-CID Online user is responsible to report any suspect incidents (viruses, unauthorized access, theft, inappropriate use, etc.) to NTIA staff.
5. Tampering with another user’s account, files, data or processes without the other user’s express permission, use of the system resources for personal purposes, or unauthorized activities is strictly prohibited and will result in termination of access privileges.
6. EL-CID Online users are responsible for protecting and maintaining, to the best of their ability, any information used or stored in their accounts. They should not attempt to access any data or programs contained on systems for which they are not authorized or do not have explicit consent of the data/program owner.
7. When a user no longer requires access to NTIA resources, they should notify their immediate supervisor, and make no further attempt to access these resources.
8. Failure to adhere to these rules or subvert these rules may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

3.0 Policies and Procedures

I understand that I must read and acknowledge the ECO Rules of Behavior to receive access to the NTIA EL-CID Online internal system. I agree to comply with all DOC and NTIA IT policies and procedures to include the following:

1. I understand that I am given access only to those EL-CID Online information to which I require access in the performance of my official duties.
2. I will access the content of EL-CID Online and upload to or modify content of the EL-CID Online (including metadata) in accordance with only those roles and privileges for which I am authorized.
3. I will only use my authorized user identity (ID) and will not divulge my user ID. I will protect passwords, and PINs, from disclosure. I will not share passwords or PINs. I will not record user IDs, passwords, or PINs on paper or in electronic form on unencrypted workstations, laptop computers, or portable electronic devices.
4. I consent to monitoring and security testing to ensure proper security procedures and appropriate usage are being observed for NTIA IT resources. I understand that I have no expectation of privacy while accessing the EL-CID Online or other DOC and NTIA IT resources.
5. I am responsible for protecting and maintaining, to the best of my ability, any information used or stored in my accounts. I will safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or use.
6. I understand that I may not work on or store NTIA data categorized as Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), or Business Identifiable Information (BII) on non-US Government equipment. BII is defined, per Freedom of Information Act 5 U.S.C.552(b)(4), as “trade secrets and commercial or financial information obtained from a person (that is) privileged or confidential.”
7. I will properly handle and protect the information on this system.
8. I will be proactive in the management of federal electronic records.
9. I will cooperate with designated personnel during investigations of incidents, compliance reviews, audits, and surveys regarding the DOC and NTIA IT systems security posture.
10. I will log off or lock my workstation or laptop whenever I step away from my work area. I will log off from the system when I leave for the day.
11. I will scan all information, programs, and other files for viruses prior to uploading onto any DOC or NTIA IT resource.
12. I will not upload any documents containing sensitive PII or Classified information to the EL-CID Online unclassified system.
13. I shall complete the annual security & privacy awareness training provided by my agency within the designated timeframes.
14. When I no longer require access to EL-CID Online, I will inform my Agency’s IRAC Representative or NTIA Supervisor and make no further attempt to access these resources.
15. I will report immediately to the NTIA Help Desk, at ntiahelpdesk@ntia.doc.gov or (202) 482-4631, all EL-CID Online related security incidents to include the loss, theft, or compromise of the EL-CID Online system.

3.0 Acknowledgement

Unauthorized use of the EL-CID Online accounts and its resources to which I am granted access is a violation of Section 799, Title 18, and U.S. Code: constitutes theft; and is punishable by law. I have read and understand these rules.

Name

Signature

Date

I authorize the above-signed individual to have an account on EL-CID Online.

System Owner Name

System Owner Signature

Date