Executive Office for Immigration Review

INFORMATION TECHNOLOGY SYSTEMS SECURITY
RULES OF BEHAVIOR for DHS employees who access the CASE Application

TO: All *Department of Homeland Security (DHS)* employees that have been granted access to the Executive Office for Immigration Review (EOIR) CASE application.

1. PURPOSE. This memorandum describes the requirements for establishing and abiding by rules of behavior for DHS employees who has been granted access to *the* CASE application.
2. SCOPE. This order applies to all system owners, managers and employees within the *DHS who* have been granted access *to EOIR* CASE application.

3. REFERENCES.

a. OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources.

b. OMB Circular A-123, Management Accountability and Control.

c. NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems.

d. DOJ Order 0904, DOJ Order 0904, Cybersecurity, issued September 15, 2016.

4. BACKGROUND. OMB Circular A-130 requires agencies to establish rules of behavior for all systems as part of the security plan for that system. The rules of behavior delineate responsibilities and expected behavior for all individuals with access to the system, set appropriate limits on interconnections with other systems, define service provisions and restoration priorities, and define the consequences of behavior not consistent with the rules. All individuals must be trained on these rules prior to being granted access to the system. The rules of behavior should be acknowledged in a signed "Customer Agreement".

5. IMPLEMENTATION.

a. The approved rules of behavior for DHS employees and customer agreement shall be published as a policy or procedures. EOIR=s Office of Information Technology (OIT), Systems Security & Integrity Staff *is responsible for* securing the CASE application and the EOIR OIT ServiceDesk shall provide a copy of the rules of behavior to each DHS employee prior to receiving their username and password for the system.

b. All *DHS* employees that have been authorized access to EOIR=s CASE application must sign the Arules of behavior@ prior to being granted access to CASE and then annually thereafter.

c. A certification statement should be signed by the user stating that they have read and fully understand the rules of behavior. A copy of this signed statement will be provided to the user. The original will be kept on file at the *Executive Office for Immigration Review* headquarters located at 5109 Leesburg Pike, Suite 900, Falls Church, VA 22041.

6. QUESTIONS. Direct questions to the OIT, Systems Security & Integrity Staff *via the OIT Service Desk at* 703- 305-7347.

Executive Office for Immigration Review

INFORMATION TECHNOLOGY SYSTEMS SECURITY PRINCIPLES and
Rules of Behavior for DHS employees who access the CASE application

VIOLATION OF THESE RULES MAY
RESULT IN DISCIPLINARY ACTION

GENERAL PRINCIPLES

The following rules of behavior apply to all Department *of Homeland (DHS)* employees who access the Executive Office for Immigration Review (EOIR) CASE application. Because written guidance cannot cover every contingency, personnel are asked to go beyond the stated rules, using their best judgment and highest ethical standards to guide their actions. Personnel must understand that these rules are based on Federal laws, regulations, and DOJ Orders. As such, there are consequences for non- compliance with the rules of behavior. Depending on the severity of the violation, at the discretion of management and through due process of the law or in accordance with employee conduct policy, consequences can include: suspension of access privileges, reprimand, suspension, demotion, removal, and criminal and civil penalties.

1. ACCOUNTABILITY: DHS employees must be accountable for their actions and responsibilities related to information resources entrusted to them.

2. CONFIDENTIALITY: DHS employees must protect sensitive and personal identifiable information from disclosure to unauthorized individuals or groups.

3. PASSWORDS AND USER IDS: DHS employees must protect information security through effective use of user IDs and passwords which must not be shared. Each system user will be assigned a unique personal identifier and password that shall be used to establish all personal accounts and access privileges for the individual. Passwords must be at least 12 characters long, it must have at least 1 numeric character, 1 uppercase character, 1 lowercase character and 1 special character. (Example: $ThemonthofJunehas30days). Passwords expire every 60 days.

4. REPORTING: DHS employees must report security violations and vulnerabilities regarding the CASE application to the EOIR OIT Service Desk at 703-305-7347.

5. USERS OF PERSONAL INFORMATION: DHS employees must acquire and use personal information only in ways that respect an individual's privacy. This includes properly destroying personal information contained in hardcopy or softcopy, ensuring that personal information is accurate, timely and complete, and relevant for the purpose which it is collected, provided, and used.

Executive Office for Immigration Review
INFORMATION TECHNOLOGY SYSTEMS SECURITY
RULES OF BEHAVIOR for DHS employees who access the CASE Application

The following rules are based upon, used in conjunction with, and are in addition to the general rules of behavior for DHS employees who access the CASE application.

1. OFFICIAL BUSINESS

   a. Do not steal information from the CASE application.
   b. Do not use the CASE application for non-work purposes.
   c. Do not access the CASE application unless necessary to perform an official duty.

2. ACCESS

   a. Only DHS employees whose managers or supervisors have certified that the users have completed the computer security and awareness training will be granted authorization to access the CASE application.
   b. Read, understand, and acknowledge the DOJ standard network security warning banner prior to logging onto the network.
   c. Only use data for which you have been granted authorization.
   d. Do not retrieve information from the CASE application for someone who does not have authority to access the information, provide only the information to people who have access authority and who need the information for official government business.
   e. Abide by procedures governing the channels for requesting/disseminating information.
   f. Remember your password, the system will disable user accounts after more than 3 consecutive invalid attempts are made to supply a password, and will require the reinstatement of a disabled user account by an administrator. Please contact the EOIR OIT Service Desk at 703-305-7347 to have your account unlocked.
   g. Do not attempt to gain access to information to which you do not have authority, your user account will be audited.
   h. Safeguard your computer from unauthorized access.
   I. Log all data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased 90 days or its use is still required.

3. INTEGRITY

a. Discontinue use of any workstation or networked system or software that shows indications of being infected with a virus.
b. Protect against viruses and similar malicious programs: use only authorized software; do not use shareware, public domain software, or similar programs unless they are authorized.
c. Never enter unauthorized, inaccurate, or false information.
d. Do not manipulate information inappropriately.
e. Create only authorized records or files.
f. Execute virus protection on your workstation according to procedures defined by your organization. Scan all files and disks for viruses before use, especially if they are received from external sources.

4. AVAILABILITY

a. Plan for contingencies such as disaster recovery, loss of information, and disclosure of information by preparing alternate work strategies and recovery mechanisms.
b. Be familiar with the part you play in local contingency plans.

5. Application

a. Notify the EOIR OIT Service Desk at 703-305-7347 if you are experiencing problems with the CASE application.
b. Safeguard against loss of data, unauthorized use, and misappropriation of the CASE application.
c. Only use the CASE application for which you have been granted authorization.

6. REPORTING

a. Report all computer security violations, viruses, incidents, and vulnerabilities regarding the CASE application to the EOIR OIT Service Desk at 703-305-7347.

7. MANAGERS

a. Notify the EOIR OIT Service Desk at 703-305-7347 whenever an employee terminates or changes status by submitting a Request for Action form.

c. Counsel terminating employees on non-disclosure of confidentially-sensitive information.

d. Terminate access to information and computer systems immediately in the event of an unfriendly separation.

f. Ensure employees get adequate and appropriate training to conduct their job functions.

g. Ensure that all employees take annual computer security awareness training.

U.S. Department of Justice

Executive Office for Immigration Review

Rules of Behavior for DHS employees who access the CASE Application

CUSTOMER AGREEMENT

CERTIFICATION

I_____certify that I have read, understand, and shall comply with the *Rules of Behavior* for the CASE application. I understand that the rules of behavior delineate responsibilities and expected behavior for all individuals with access to the system, set appropriate limits on interconnections with other systems, define service provisions, restoration priorities, and define the consequences of behavior not consistent with the rules. I further understand that I must receive training on these rules prior to being granted access to CASE. I acknowledged the rules of behavior by signing this Customer Agreement.

_____ _____

Signature Date

_____

Organization