

**FTMS USER - CODE OF CONDUCT**

The Foreign Travel Management System (FTMS) is **Department of Energy (DOE) Official Use Only (OUO)** and contains information that may be exempt from public release under the Freedom of Information Act (FOIA) (5 U.S.C. 552). FTMS may also contain information protected under the Privacy Act (5 U.S.C. 552a). Prior to public release of any information, approval must be obtained from: (1) a manager having cognizance over a program identified in the report; (2) each individual identified on the report for his/her personal information; and (3) a FOIA officer/legal authority.

**FTMS Rules of Behavior:** Users of FTMS are held accountable for their actions and the following rules of behavior apply to all users of the FTMS.

- FTMS Users must be a US Citizen and access by foreign nationals is prohibited.
- Do not disclose your password to other individuals.
- Comply with Password Requirements.
- Do not use FTMS for storing/saving any classified or other sensitive (project/program) information.
- Report any misuse or security related problems to your Senior OPOC.
- Consult with your local computer security manager for site restrictions.
- Notify your Senior OPOC when FTMS access is no longer needed.
- ALL FTMS users are subject to FTMS cyber security audits.

<b>Password Requirements</b>
<p>The following password requirements apply when accessing the FTMS.</p> <ul style="list-style-type: none"> <li>▪ Must be at least eight characters long.</li> <li>▪ Must contain at least one upper-case letter.</li> <li>▪ Must contain at least one lower-case letter.</li> <li>▪ Must contain at least one numeric digit.</li> <li>▪ Must contain at least one special character (i.e., !, @, #) within the first seven positions.</li> <li>▪ The password must begin and end with a non-numeric character.</li> <li>▪ The password cannot contain the username.</li> <li>▪ The password cannot contain blanks.</li> <li>▪ E.g., passwords complying with this guidance: AS#\$34ty, iN!30%Ak, and ok2!t8#E</li> </ul>

FTMS Security Awareness: **FTMS information, as an aggregated source of DOE travel practices and history, is OUO** and requires computer security mechanisms sufficient to protect **OUO** information.

Printed Reports: Printed reports may contain Privacy Act Information (Title 10 CFR, part 1008) and will require additional protection pursuant to the requirements of that act:

- An appropriate security authority must formally review any printed FTMS report prior to release from your immediate control.
- Access to FTMS reports are based on, and limited to, an official need-to-know.
- Paper reports no longer needed should be destroyed in accordance with local site OUO destruction procedures, or as classified waste.
- Access to FTMS reports should be limited, controlled, and/or stored in a locked desk/cabinet/safe drawer or other area not directly visible.

