

## **Guiding Information Technology (IT) Security Commandments:**

**Purpose:** The purpose of this document is to identify best security practices that should be integrated into IT security environments. This applies to all state agencies that are responsible for implementing the security control of information systems, where Federal Tax Information (FTI) is stored, transmitted, or processed.

**Background:** The Tactical Advisory Group (TAG) Security Subgroup (SS) was established to develop security solutions for systemic security problems. As part of this process, the IRS identified many security issues related to the IRS' Computer Security Material Weakness and to data warehousing issues. The TAG SS discussed how to take identified weaknesses and ensure these were not carried into their own individual IT environments. The consensus was to take key security issues and change the wording to make these become best practices or "10 Commandments". This document is a result of that effort.

By implementing the "10 Commandments", this will not guarantee a passing and/or failing grade for upcoming Safeguard Reviews. By implementing these controls, an organization will be better postured in the entire area of IT security.

**Recommended Use:** To ensure state taxation agencies implement security controls effectively, the TAG SS recommends that this document, *Ten Security Commandments for Protecting Federal Taxpayer Information* be duplicated and provided to managers, developers, and any organization/staff responsible for providing IT and IT security controls to the organization. This document will serve as a reminder of the necessary security controls within an IT environment.

**Version #:** 1.0, dated September 1, 2006

**Questions:** Questions regarding this document may be addressed to [ellen.o.pieklo@irs.gov](mailto:ellen.o.pieklo@irs.gov). Any questions and/or feedback will then be forwarded to the TAG SS for archival purposes.

# **Information Technology (IT) Security: Ten Security Commandments For Protecting Federal Taxpayer Information**

1. Ensure the system is built using principles from the Federal Information Security Management Act (FISMA), National Institute of Standards & Technology (NIST), and Publication 1075.
2. Ensure development of security policies and procedures that sufficiently describe the security requirements and controls of the systems and processes.
3. Integrate access controls for access to data and applications to ensure access is controlled on a need to know basis and granted for authorized purposes, such as State Tax Administration. When strict access cannot be controlled, audit controls must be able to identify who accessed the information and for what purpose.
4. Define roles and responsibilities to ensure all personnel understand security-related responsibilities and that these personnel have separations of duties, as necessary.
5. Ensure disaster recovery procedures are in place to provide for the protection, backup, and recovery of IRS data
6. Provide security awareness training, including IT security awareness, at least annually. Ensure training is role specific.
7. Ensure auditing is built into the systems, applications, routers, and databases to ensure that transaction and security-related events are recorded and able to be investigated. Auditing should allow management to determine the Who, What, When, and Where of events. Auditing should include the review of access made by system administrators, database administrators, and others who have super-user capabilities.
8. Ensure that test environments are afforded the same security controls as production environments. All Federal Taxpayer Information must be protected.
9. Ensure that process authorizations are in place to allow a system to be validated for effective security controls, and authorized by management prior to being brought into production.
10. Develop and implement an effective Incident Response Program to allow for both automated and manual controls to handle security relevant incidents.