Integrated Automated Travel System (IATS)
Security Policy Statement

The DFAS-IN Travel Systems and Procedures Office does not have the authority nor the resources to ensure adequate security at every Integrated Automated Travel System (IATS) deployed location, therefore, each site is responsible for addressing their own unique security issues as they relate to use of the IATS software.

Travel office managers are charged with the responsibility of ensuring that internal controls are in place to prevent erroneous or fraudulent travel payments. Managers and System Administrators are required to assist the Information System Security Officer (ISSO) with enforcing security for the system support environment.

Each Terminal Area Security Officer (TASO) shall be responsible for ensuring established security procedures are followed for the assigned work area. Procedures should be in place to inform users of how to report security violations to their TASO.

Each operational IATS user is responsible for providing a minimal level of security for IATS Automated Information System (AIS) resources.

Each user shall protect information and AIS resources against occurrences of sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse or release to unauthorized persons. The System Administrator should provide user documentation and training that identifies procedures for protection against these occurrences.