INTERNATIONAL CIVIL AVIATION ORGANIZATION
ASIA AND PACIFIC OFFICE

ASIA/PAC
AERONAUTICAL TELECOMMUNICATION NETWORK
SYSTEM SECURITY POLICY

Second Edition - September 2008

ASIA/PAC AERONAUTICAL TELECOMMUNICATIONS NETWORK SYSTEM SECURITY POLICY

1. Purpose: This document prescribes the system security policy and associated requirements applicable to the Aeronautical Telecommunications Network (ATN). It applies to ATN implementations and defines the rules governing the protection of ATN data, services and resources associated with ATN applications and processes from both unintentional defects and deliberate attack. The design, implementation and operation of the ATN must support the complete and consistent enforcement of this system security policy.

2. Applicability: For the purpose of this policy, the ATN encompasses hardware, software, procedures, standards, facilities, and personnel. System security services provided in support of the ATN protect all data transmitted, stored, or processed by the system, for various levels of sensitivity.

3. Authority: This document is published in accordance with the authority of the International Civil Aviation Organization (ICAO).

4. Implementation and Enforcement: This system security policy defines a minimum set of rules to be enforced for the protection of data, services, and resources under ATN cognizance. Regional and local authorities may apply more stringent rules or constraints, while not degrading the ATN system security posture and maintaining consistency with the minimum essential required system security rules identified in this ATN System security Policy.

5. System security Requirements: System security requirements apply to the protection of the physical information technology, the communications equipment, and the data and information systems. Protection also applies to the facilities, environment, hardware, software, and people associated with the ATN. The fundamental ATN system security requirements are:

(1) Protect all ATN data directly associated with ATN applications and processes including ATN messages and stored information from unauthorized disclosure, modification, or deletion;

(2) Protect ATN services and resources from unauthorized use and denial of service.

6. System Security Services: Safe and secure operation of the ATN depends upon the accurate and consistent enforcement of six high level services: confidentiality, data integrity, authenticity, availability, accountability, and interoperability.

(1) Confidentiality: Ensures data is not disclosed to unauthorized entities. For the ATN, confidentiality, when appropriate, extends to data associated with ATN support applications and processes including system management and security applications;

(2) Data Integrity: Ensures data has not been altered or destroyed in an unauthorized manner;

(3) Authenticity: Ensures that the source of data or the identity of an entity is as claimed;

(4) Availability: Ensures resources, services, and data are accessible and usable on demand or in a timely, reliable manner by an authorized entity;

(5) Accountability: Enables activities to be traced to users and processes that may then be

held responsible for those actions.

7. System Security Policy Statements: The ATN system security policy is intended to result in management, operational, and technical controls implemented on a regional or local level to provide system security services meeting the fundamental system security requirements. Accordingly, the following functional policy statements are identified in terms of the defined services:

Functional Policy Statements:

a) Confidentiality:

(a) ATN data shall be protected from unauthorized disclosure during processing, transmission, and storage commensurate with the designated sensitivity of the data.

b) Data Integrity:

(a) ATN data shall be protected from unauthorized or undetected modification during transmission, storage, and processing.

c) Authenticity:

(a) ATN users and processes shall be uniquely identified.

(b) ATN users and processes shall be authenticated before being granted access to ATN data, services, and resources.

(c) ATN data, services, and resources shall be protected from unauthorized use or tampering.

(d) ATN users and processes shall have access only to those ATN data, services, and resources for which they have authorization.

d) Availability:

(a) ATN data, services, and resources shall be available for use by authorized users and processes.

e) Accountability:

(a) An audit trail of use of ATN data, services, and resources by ATN users and processes shall be maintained.

8. Verification and Authorization: The process used by an independent agent to confirm or establish that the management, operational, and technical controls effectively meet the system security requirements is termed *verification*. Verification includes establishing that the system security functional policy is adequately provided. The *authorization* by responsible entities to place a system into operation is based on the verified effectiveness of management, operational, and technical controls.

(1) Verification:

(a) ATN systems shall be verified to have system security commensurate with the risk and magnitude of harm resulting from unauthorized disclosure, modification, or deletion of ATN data, or unauthorized use and denial of service of ATN services and resources.

(2) Authorization:

(a) ATN systems shall be formally approved for operation by the cognizant Designated Approving Authority (DAA).

(b) Significant changes to ATN systems shall require another formal approval (or re-authorization).

– – – – – – – – – – – – – – –