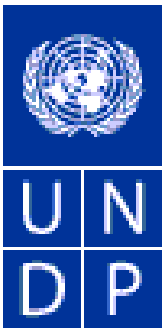

INFORMATION SYSTEMS SECURITY STANDARDS

Acquisition, Development, and Maintenance Requirements

BoM Office of Information Systems and Technology - United Nations Development Programme

304 E. 45th Street, New York, NY 10017 - oist.security@undp.org

DOCUMENT CONTROL

Document Name	**Information Systems Security Standards**
Language(s)	English
Responsible Unit	BoM - BoM/OIST
Creator (individual)	Paul Raines, Chief Information Security Officer (CISO)
Subject (taxonomy)	…/Prescriptive Content/Information Technology Management/ Requirements for Acquisition, Development, and Maintenance of Information Systems – Information Systems Security Standards
Effective Date	July 2010
Mandatory Review	12 months
Expiry Date	
Audience	All individuals accessing the UNDP Intranet
Applicability	All UNDP staff members at Headquarters, in Country Offices and at other offices worldwide and by all UNDP Associates using ICT resources owned or operated by UNDP
Replaces	NA
Is part of	NA
Related documents	Information Security Policy; Disaster Recovery Standards for UNDP Offices; Country Office & Regional ICT Security Standards; ICT Security and Awareness Standards; System Logon Banner Standards; ICT Security Best Practices Guide; IDM User Guide; UNDP Technical Secretariat Information Security Policy
UN Record Ref.	TBD

Date	Author	Version	Change Reference
13 Nov 2009	Paul Raines	1.0	Initial version
30 Nov 2009	Paul Raines	1.1	BoM/OIST Management; BoM units; MPN review; ICT Managers, LSO and OAI

TABLE OF CONTENTS

Compliance with ICT Policies and Guidelines

- Policies, Standards, Work Instructions, Checklists - Compliance is mandatory.
- Guidelines, Best Practices, White Papers - Compliance is not mandatory. Any deviation from guidelines, best practices, and white papers usually implies potential risks for which users are required to take mitigating measures.

Policies – Formal, brief, and high-level statements that embrace UNDP's ICT goals, objectives, and acceptable procedures. Compliance is mandatory and failure to comply may result in administrative action. Waivers to the policy must be requested in writing to and approved by the Chief Information Security Officer (CISO).

Standards – Written to directly support a policy and provides more detailed guidance in specific areas (e.g. security requirements for system acquisition and development). Compliance is mandatory and failure to comply may result in administrative action. Waivers to standards must be requested in writing to and approved by the Chief Information Security Officer (CISO).

Work Instructions and Checklists – Written to provide detailed instructions on the execution of a specific security task (e.g. checklist for generating a digital certificate for encryption and digital signing). Compliance is mandatory and failure to comply may result in disciplinary action. Waivers to standards must be requested in writing to and approved by the Chief Information Security Officer (CISO).

Guidelines and Best Practices – Provide a framework within which to implement procedures. Guidelines, guides, procedures, and best practices are not mandatory, but are rather recommendations. Any deviation from guidelines or best practices usually implies potential risks for which users are required to take mitigating measures.

White Papers – Authoritative reports or briefs that often address issues and how to solve them. White papers are used to educate readers and help people make decisions. White papers carry no compliance component, but are rather informative bulletins or reports.

1.0 INTRODUCTION

1.1 Security is an integral part of information systems. Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design, development, acquisition and implementation of the information system supporting the business process can be crucial for security. These standards have been developed toward that purpose.

2.0 SCOPE

2.1 These standards apply to all usage by persons involved in the acquisition, development and maintenance of UNDP's IT environment and are applicable to all UNDP networks and systems including any UNDP applications/systems developed for the Internet. All authorized UNDP users are bound by the provisions and intent of these standards and the UNDP Information Security Policy it supports.

2.2 These standards will cover how information security is ensured during the acquisition, development and maintenance of information systems at UNDP. It covers the following:

- Security requirements analysis and specification
- Correct processing in applications
- Cryptographic or secure communication controls
- Security in development and support processes
- Technical vulnerability management
- Data availability in new applications

3.0 REFERENCES

3.1 The following documents and authorities are referenced in these standards:

- Information Security Policy
- Standard on ICT Resources Use
- Change Control and Release Management Standards

4.0 DEFINITIONS

4.1 The following terms are used throughout these standards:

- IT environment - The computing and data processing systems that include, but are not limited to the local area networks, wide area networks, workstations, laptops, fixed or removable storage media, messaging systems (e.g. electronic mail and bulletin board), Internet access, voice mail, facsimile, telephone access, SMS, and related technologies.
- Program source code - Program source code is code written by programmers, which is compiled and linked to create executables.

- Interpretive software - Software programs which must be run with an interpreter, commonly called a runtime module.

5.0 RESPONSIBILITIES

5.1 The Chief Information Security Officer (CISO) shall be responsible for the periodic review and updating of this document. He shall be considered the "owner" of these standards. Staff members tasked with responsibilities in information systems acquisition, development and maintenance is responsible for following the requirements of these standards and the Information Security Policy. Toward that end, a checklist has been developed at the end of these standards that can assist in ensuring compliance with information security requirements.

6.0 APPROVALS OF NEW ICT PROJECTS, SYSTEMS, AND APPLICATIONS

6.1 New enterprise or corporate ICT projects, systems and applications must be coordinated with the UNDP Chief Technology Officer (CTO) and Director of IT (Office of Information Systems and Technology- OIST) and approval given through the UNDP ICT Board.

6.2 No new enterprise or corporate ICT projects, systems or applications shall proceed without first having been coordinated with the UNDP Chief Technology Officer (CTO) and arrangements made for its support, security and integration within the existing UNDP ICT environment.

6.3 Since UNDP ICT projects, systems, or applications can be invoked locally, local Country Offices should apply the rigorous principles of these security standards in all local Country Office settings.

7.0 SECURITY REQUIREMENTS - ANALYSIS AND SPECIFICATION

7.1 All security requirements shall be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall functional requirements for an information system. At a minimum the following documentation that must be developed at this point are:

- User functional requirements including security requirements
- Design specifications of system or application
- User Acceptance Test Requirements (including security requirements)

7.2 After the application has been developed but prior to its being placed into production, at a minimum the following documentation must be developed:

- User guides
- System administrator guides to include installation instructions, backup mechanisms, monitoring capabilities and a troubleshooting guide
- Documented test results for unit, system, integration, and user testing. The test results shall verify that user and security requirements have been met prior to being placed into production.

Note: Under incremental development approach it may not be possible to fully specify all of the user requirements at the outset. Thus, the functional requirements document may change as the project matures and depending on the feedback from business users.

7.3 Statements of functional requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls needed to ensure the confidentiality, integrity and data availability for the information system. These specifications should consider the automated controls to be incorporated in the information system, and the need for supporting procedural controls. Similar considerations should be applied when evaluating software packages, developed or purchased, for applications.

7.4 All new information processing systems shall be required to be approved by a minimum of the Change Control Board or other ICT governance body and the sponsoring unit prior to being taken into production or operations. Contracts with suppliers shall address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, then the risk introduced and associated controls required to address the risk should be reconsidered prior to purchasing the product. Where additional functionality is supplied which causes a security risk, this shall be disabled or the proposed control structure should be reviewed to determine if advantage can be taken of the enhanced functionality available.

8.0 CORRECT PROCESSING IN APPLICATIONS

8.1 Appropriate and adequate input validation controls shall be designed and incorporated into any operational or production application. Controls should be applied to the input of transactions, standing data and parameter tables. Specific areas to check can include, but are not limited to:

- Dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors:
  - Out-of-range values
  - Invalid characters in data fields
  - Missing or incomplete data
  - Exceeding upper and lower data volume limits
  - Unauthorized or inconsistent control data
  - Known scripting or injection-based attacks
- Periodic review of the content of key fields or data files to confirm their validity and integrity
- Procedures for testing the plausibility of the input data
- Defining the responsibilities of all personnel involved in the data input process

8.2 Validation checks should be incorporated into production applications to detect any corruption of information through processing errors or deliberate acts. Data that has been correctly entered can be corrupted by hardware error, processing errors, or through deliberate acts. Validation checks required will depend on the nature of the application and the business impact of a corruption of data. Specific areas to check can include, but are not limited to:

- The use of add, modify, and delete functions to implement changes to data
- The procedures to prevent programs running in the wrong order or running after failure of prior processing
- The use of appropriate programs to recover from failures to ensure the correct processing of data
- Protection against attacks using buffer overruns/overflows

Examples of controls that can be included in an application include:

- Session or batch controls, to reconcile data file balances after transaction updates
- Balancing controls, to check opening balances against previous closing balances, namely:
  - run-to-run controls
  - file update totals
  - program-to-program controls
- Validation of system-generated input data
- Checks on the integrity, authenticity or any other security feature of data or software downloaded, or uploaded, between central and remote computers
- Hash totals of records and files
- Checks to ensure that application programs are run at the correct time
- Checks to ensure that programs are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved
- Creating a log of the activities involved in the processing
- Recovery and roll-back controls which ensure data accuracy, completeness and integrity
- Audit trails

8.4 Requirements for authenticity and message integrity in applications shall be identified during the requirements phase of a project, and appropriate controls identified and implemented.

8.5 Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Output validation may include:

- Plausibility checks to test whether the output data is reasonable
- Reconciliation control counts to ensure processing of all data
- Providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information
- Procedures for responding to output validation tests
- Defining the responsibilities of all personnel involved in the data output process
- Creating a log of activities in the data output validation process

9.0 CRYPTOGRAPHIC OR SECURE COMMUNICATION CONTROLS

9.1 Any use of encryption shall be based on a risk assessment. The required level of protection should be identified taking into account the type, strength, and quality of the encryption algorithm used. Encryption should be considered for protection of sensitive information transported by mobile or removable media devices or across communication lines which include both physical and wireless networks.

All information exchanged between trusted/trusting applications on operational or production systems shall be encrypted to enforce trust levels and message integrity between systems. Where encryption cannot be used for message exchanges between trusted/trusting systems, this must be explicitly authorized by OIST. Use of specific

encryption algorithms and associated key lengths is subject to approval by OIST. Before using encryption, there should be a well-defined approach including the following:

- Methods to protect the cryptographic keys and the recovery of information in the case of lost or compromised cryptographic keys
- Roles and responsibilities for implementing encryption, key management, and key generation.

9.2 When implementing encryption, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information.

9.3 All cryptographic keys should be protected against modification, loss, unauthorized disclosure and destruction. Appropriate procedures for key generation, assignment, distribution, re-use and recovery shall be established for each operational or production system using encryption. Procedures for responding to key loss or compromise shall be established.

10.0 SECURITY OF DEVELOPMENT, TEST AND SUPPORT PROCESSES

10.1 Access to system files and program source code will be controlled and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in development and test environments.

10.2 Only approved software may be installed on operational or production systems, and software may only be installed by authorized staff in the execution of their officially approved duties.

10.3 Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Physical or logical access should only be given to suppliers for support purposes when necessary, and with appropriate management approval. The supplier's activities should be monitored with sufficient controls in place.

10.4 Specific sets of test data should be created to provide the basis for the conduct of tests to meet the acceptance criteria of any program to develop, procure or, upgrade any operational or production system. Such test data should be representative of operational data, but shall not be actual operational/production data. The use of operational databases containing personal information or any other sensitive information shall not be used for testing purposes unless explicitly authorized by the CISO and the data owner. In any such case, the following apply:

- The same levels of protection which apply to operational application systems shall also apply to test application systems
- There should be a separate authorization each time operational information is copied to a test application system
- Operational information should be erased from a test application system, in a manner consistent with that used on operational application systems, immediately after the need for testing is complete
- The copying and use of operational information should be logged to provide a trail of accountability

10.5 Program source code shall be adequately protected against unauthorized access or change. Access to development systems and their program source code and associated items will be strictly controlled, in order to

prevent the introduction of unauthorized functionality and to avoid unintentional changes. All changes to source code shall be coordinated via approved change control procedures. Version control shall be implemented and enforced.

10.6 Project and support environments should be strictly controlled. Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

10.7 Formal change control procedures shall be documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and major changes to existing systems shall follow a formal process of documentation, specification, testing, and quality control and managed implementation.

10.8 The change control process shall include a risk assessment, analysis of the impacts of changes and specification of security controls needed. This process shall also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

10.9 If required, adequate and appropriate regression and performance testing shall be conducted as part of the change management procedures using appropriate test data sets and test facilities.

10.10 Outsourced software development should be supervised and monitored by the ICT unit (e.g. HQ OIST or ICT staff in a country office). Where software development is outsourced, the following points should be considered:

- Licensing arrangements, code ownership, and intellectual property rights
- Certification of the quality and accuracy of the work carried out
- Escrow arrangements in the event of failure of the third party
- Rights of access for audit of the quality and accuracy of work done
- Contractual requirements for quality and security functionality of code
- Testing before installation to detect malicious and Trojan code
- Subcontracting restrictions

11.0 CONTROL OF TECHNICAL VULNERABILITIES

11.1 Appropriate timely action shall be taken in response to the identification of potential vulnerabilities in operational systems. The organization should define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required. Once a potential technical vulnerability has been identified, the organization should identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems and/or applying other controls. Depending on how urgently a technical vulnerability needs to be addressed, the action taken shall be carried out according to the controls related to change management or by following information security incident response procedures.

11.2 If a patch is available, the risks associated with installing the patch shall be assessed (the risks posed by the vulnerability shall be compared with the risk of installing the patch). Patches shall be tested and evaluated before

they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered such as:

- Turning off services or capabilities related to the vulnerability
- Adapting or adding access control
- Increased monitoring to detect or prevent actual attacks
- Raising awareness of the vulnerability
- An audit log shall be kept for all procedures undertaken
- The technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency
- Systems at high risk should be addressed first

12.0 DATA AVAILABILITY IN NEW APPLICATIONS AND SYSTEMS

12.1 Before new systems are deployed in an operational environment, the unit's business continuity plan shall be updated as necessary with the information on the new system.

13.0 GUIDELINES AND FURTHER INFORMATION

13.1 Work instructions or guidelines on the implementation of these standards may be developed to address internal requirements. Such working instructions and guidelines shall be read in conjunction with these standards. If there is a discrepancy between any provision of the standard and any such guideline, the provisions of the standard shall take precedence.

14.0 APPENDIX 1 - CHECKLIST FOR COMPLYING WITH SECURITY REQUIREMENTS

The following checklist is a recapitulation of the security requirements contained in these standards. It is recommended that the checklist be completed prior to any system being brought into production status.

Checklist of Requirements for Standards on Acquisition, Development, and Maintenance

Consider the following aspects relating to the information system or application being acquired or developed. Tick one box for each aspect.

Standard on Acquisition, Development and Maintenance Requirement	YES	PARTIAL	N/A
1.Has the following documentation been developed: • Design specifications of system or application • User Acceptance Test Requirements (including security requirements) • User manuals • System administrator manuals to include installation instructions, backup mechanisms, monitoring capabilities and a troubleshooting guide • Test plans and results for unit, system, integration and user testing			
2. Has the system or application been approved by the UNDP ICT Board (or local ICT governance bodies) and coordinated within OIST and respective ICT unit for its support, security and integration with the existing ICT environment?			
3. Have the following data input controls been considered incorporated? • Out-of-range values • Invalid characters in data fields • Missing or incomplete characters • Exceeding upper and lower data volume limits • Unauthorized or inconsistent control data • Known scripting or injection-based attacks • Periodic review of content of key fields			

• Periodic inspection of hard copy input documents for unauthorized changes • Procedures for responding to validation errors • Plausibility checks for input data • Defined responsibilities for personnel involved in data input process			
4. Have the following data validation checks been incorporated to detect any corruption of information through processing errors or deliberate acts? • Use of add, modify and delete functions to implement changes to data • Procedures to prevent programs running in the wrong order or running after failure of prior processing • Use of appropriate programs to recover from failures to ensure the correct processing of data • Protection against attacks using buffer overruns/overflows			
5.Has the application implemented the following controls: • Session or batch controls • Balancing controls • Validation of input data • Checks on integrity, authenticity • Hash totals of records or files • Checks to ensure application runs at correct time • Checks to ensure program runs in the correct order and terminate in case of failure • Creating a log of activity processing • Recovery and roll-back controls			
6. Has data output from the application been validated? • Plausibility checks • Reconciliation controls counts • Providing sufficient information for a subsequent processing system to determine accuracy, precision, and classification • Procedures for responding to output validation			

tests • Defined responsibilities of all personnel involved in data output processing • Creating a log of activities in validation of output			
7. Is information being exchanged between trusted/trusting systems? Has this been authorized by OIST for HQ and by a local ICT governance body for local offices?			
8. If vendor-supplied software is being used, will it be maintained at a level supported by the vendor?			
9. Has test data been created for the acceptance test? If personal or sensitive data must be used for the test, have the following requirements been met? • Same levels of protection applied as operational data • Separate authorization each time operation information is copied to the test system • Operational information should be erased from a test application immediately after the need for testing is complete • The coping and use of operational information should be logged to provide an audit trail			
10. Have project and support environments been strictly controlled?			
11. Has adequate and appropriate regression testing been performed in a test environment?			
12. Has the system owner's business continuity plan been updated with the information on the new system?			

If you have ticked any of the boxes marked either PARTIAL or N/A, you should indicate the reasons and justification in the following boxes.

Requirement from above	Reasons and justification (with reference to supporting evidence)	Action to be taken

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

INDEX