Ministry of Finance – Information Technology Division

Standards and Guidelines for Strategic Systems

Version 0.1

Table of Content

1. STRATEGIC SYSTEM PLATFORMS

1.1 Definition of Strategic Systems

A strategic system is one that meets several of the following criteria:

1.1.1 Supports and shapes the corporate strategy of an organization, often leading to innovation in the way the organization conducts its business

1.1.2 An information system established with the goal of creating competitive advantage and improving the competitive position of an organization.

1.1.3 Information systems that are developed in response to corporate business initiative.

Examples of such systems within the Ministry of Finance, among others, are:

- IFMS (Integrated Financial Management System)
- Asycuda (Customs System)
- IRD System

1.2 Management of Strategic Systems

The following guidelines apply to strategic systems:

1.2.1 Strategic platforms (Technical) will be managed and operated by the ITD (Information Technology Division) and consultants as determined by the ITD.

1.2.2 Strategic applications will be managed by the designated custodian of the application

1.3 Physical Security

The following standards must be met:

1.3.1 Premises must be physically strong and free from unacceptable risk, from flooding, vibration, dust, etc.

1.3.2 Air temperature and humidity must be controlled to be within acceptable limits.

1.3.3 Platforms must be electrically powered via UPS to provide the following

1.3.3.1 Minimum of 30 minutes' operation in the event of a power failure

1.3.3.2 Adequate protection from surges and sags

1.3.3.3 Trigger an orderly system shutdown when deemed necessary

1.3.3.4 Seamless change over to auxiliary service

1.4 Physical Access

1.4.1 The premises will be staffed and controlled by designated ITD staff and consultants as determined by ITD.

1.4.2 External doors will remain locked, preferably with electronic locks

1.4.3 There will be a security screen on all external windows

1.4.4 Access must be permitted by the Deputy Director of ITD

1.5 User Access

1.5.1 New User

New *user ID's* will be handled as follows

1.5.2 Written application must be submitted on an official form
1.5.3 The application form must be signed by head of Department/Directoriate/Division
1.5.4 The application must have clear indication of requirement, including the details of the applicant
1.5.5 The application form will be kept indefinitely by ITD
1.5.6 If the system supports a password aging facility, then it must be set to force password change on the first login.
1.5.7 The access level will be no higher than required as approved by the owner.
1.5.8 Access to the system is based on an individual basis (unless otherwise indicated); therefore the password will remain the sole possession of the owner and should not be shared (unless authorised by head of Department/Directoriate/Division)

1.5.2 Terminating User

The userids of persons leaving the Ministry of Finance (or the government) or of those no longer requiring access will be disabled. All files will be referred to the system owner for disposal

1.6 Fire Detection and Control

1.6.1 There will be smoke and thermal detectors on the premises
1.6.2 Underfloor areas will have smoke and water detectors
1.6.3 The detectors should be checked on a regular basis [Press the test button on your detector and check that the device beeps or rings loudly. Never use open flame devices to test an alarm. Repeated use of smoke to activate detectors can cause them to fail when a real fire occurs]
1.6.4 Keep extinguishers in a visible place and full at all times
1.6.5 Fire drill schedules and an escape plan must be drawn up and implement.

1.6.6 *Guidelines (tips & warnings) on Fire detector*

1.6.6.1 If your detector runs on batteries, change them when you change your detector
1.6.6.2 If your smoke detector starts chirping or beeping off and on, it's time to change the batteries.
1.6.6.3 If a smoke detector goes off, you literally have seconds to respond. There is absolutely no time to gather possessions your best response is to leave the premises, gather at your prearranged meeting place, whilst waiting for help
1.6.6.4 Avoid getting any paint or dust on your smoke detector.
1.6.6.5 Make sure the smoke detector you choose has been tested by an independent

1.7 Information Integrity

Integrity, in terms of data and network security, is the assurance that information can only be accessed or modified by those authorized to do so.

1.7.1 Guidelines in ensuring integrity

1.7.1.1 Maintain current authorization levels for all users
1.7.1.2 Document system administration procedures, parameters and maintenance activities
1.7.1.3 Control the physical environment of the networked terminals and server
1.7.1.4 Restrict access to data and maintain a rigorous authentication practice
1.7.1.5 Ensure that servers are only accessible to network administrators
1.7.1.6 Keep transmission media (cables and connectors) covered and protected from possible tapping
1.7.1.7 Protect hardware and storage media from power surges, electrostatic discharges and magnetism
1.7.1.8 Have an updated disaster recovery plan for occurrences such as power outages, server failure, virus attacks, etc

1.8 Password Aging

If the system provides for the facility, automatic password aging must be enforced. The life of a password should be no more than one (1) month.

1.9 Disaster Recovery Plan

There should be a Disaster Recovery Plan for every Strategic system

1.10 Documentation

All documentation for the various Strategic systems must be kept at the ITD; below is a list of the documents, though not limited to such:

1.10.1 Technical and User Documentation with version control
1.10.2 SLAs (Service Level Agreements)
1.10.3 Project Plans
1.10.4 User requirements, Feasibility Studies, Business Case, Test documents, etc with version control
1.10.5 DRP (Disaster Recovery Plan)

2. Change Control

2.1 Definition

Change Control covers the control of all aspects of the strategic systems including the operating systems, its associated packages (DBMS, etc) and utilities, third party and Ministry of Finance developed applications, together with any command procedures and documentation to support and run them

2.2 General Obligations

When changes are required to any system software, associated packages and utilities, applications software, command procedures, or documentation, it is essential that the changes are:

2.2.1 Clearly documented including reasons for such change
2.2.2 Appropriately authorised and approved
2.2.3 Made in consultation with the Ministry of Finance Internal Audit Division, where appropriate
2.2.4 Thoroughly tested and sufficiently documented
2.2.5 Implemented at the appropriate time

Any change must only be transferred to the production environment when approved by the appropriate system custodian(s).

A set of Change Control Procedures should be in place to guide and manage the change process of applications and systems.

2.3 Change Control Responsibilities

The responsibility for change implementation, after thorough testing in the test environment and moving such to the production environment after appropriate authorisation and approval, will be given to specific staff members.

All elements of the system will be subject to Change Control Procedures.

2.4 Change Control Environment

Three separate environments should be maintained for every strategic system, where possible:

2.4.1 Development
2.4.2 Testing
2.4.3 Production

Migration between the environments should only be undertaken after obtaining the appropriate sign-offs as specified in the Change Control Procedure

Changes to existing system or the development of new systems should be done in the ***development environment*** by authorised personnel or consultants. Applications should be specified, designed and coded according to the Ministry of Finance systems development methodology.

Upon satisfaction and approval from the appropriate individuals the system can be moved to the ***test environment.*** There the system will undergo acceptance testing by an appropriate group and this shall be done according to a pre-agreed test procedure. No changes to the system will be done in this environment.

Following the successful completion of testing and approval by the appropriate system's custodian(s), the software will be transferred to the ***production environment*** for implementation under the control of ITD Operations staff. A contingency plan should be prepared, where appropriate, in the event that restoration to the previous version is required.

2.5 Documentation

The following documents are required to affect change to the strategic systems

2.5.1 Change Control Procedures

Procedures that reflect how the change will be affected; this must be documented and kept by the ITD.

2.5.2 Change Request (Service Request) Form

No software change is to undertaken without an appropriately authorized service request. The service request is also the principal documentation to be completed for the change management process

2.5.3 Technical, Operations and End User Documentation

Appropriate documentation in respect of the change must be completed in sufficient detail and accepted before the change is implemented in the production environment.

3. Communications

Network access can be categorised in the following major areas:

1. Ministry of Finance (Fiscus building) Local Area Network
2. Windhoek Interoffice Network
3. Regional Offices
4. Internet (Wide Area Network)

Responsibility and control of these networks, apart from the internet, is that of staff of the Information Technology Division of the Ministry of Finance in conjunction with the Office of the Prime Minister.

3.1 Physical Security

The following standards of physical security should be met:

3.1.1 Premises housing the network control equipment must be physically strong and free from unacceptable risk from flooding, vibration, dust, fire, etc

3.1.2 External building ducts must be properly secured

3.1.3 Internal building distribution of cables within ceiling, wall or floor cavities must be placed in protective conduits.

3.1.4 Network electronics must be powered via Un-interruptible Power Supplies (UPS) to provide the following:

3.1.4.1 Minimum of 30 minutes' operation in the event of a power blackout

3.1.4.2 Adequate protection from surges and sags.

3.2 Physical Access

3.2.1 Access to areas housing network electronics will be controlled by designated ITD staff (no unauthorized entrance)

3.2.2 Doors to areas housing network electronics will be locked with a unique key, the distribution of which will be determined by ITD staff

3.3 Data Integrity

3.3.1 Maintain current authorization levels for all users

3.3.2 Documenting system administration procedures

3.3.3 Parameters, and maintenance activities,

3.3.4 Creating disaster recovery plans for occurrences such as power outages, server failure, and virus attacks.

3.3.5 Implement eavesdrop protection, if necessary, at the network hardware level

3.3.6 Implement intrusion protection to prevent unauthorised access