Ministry of Finance – Information Technology Division

Change Control Procedure

Date Create: February 2010

Version 0.1

Table of Content

1. Purpose

This procedure defines how change control is handled in all systems developed by and for the Ministry of Finance including but not limited to the strategic systems.

Change control (configuration management) is the method by which Ministry of Finance (MoF) maintains control of changes to its information assets.

Where network, system, application, or facility capabilities or processes dictate a divergence from these policies, the reasons for the exception shall be documented and maintained by the controlling entity in its Information Security Control Exceptions Book.

2. Scope

This procedure applies to the Ministry of Finance, including all its subsidiaries. This procedure applies to all MoF Information assets including software, hardware, documentation of all types (user manuals, requirement specifications, contractual agreement, etc).

3. Procedure

Modifications to, or additions or removals of, hardware (systems, networks, firewalls, etc), software (operating systems, application, programs, etc), documentation (user manual, requirement specifications, contractual agreements, etc), or other information assets in the MoF production environment, shall be made in compliance with MoF approved changed control processes.

3.1 Hardware and Software Controls

Due to the fact that unauthorised additions of hardware and software may inadvertently create vulnerabilities in the MoF information technology environment or render archived media unrecoverable, it is imperative that changes to the production environment follow the approved process.

3.1.1 Hardware Controls

The hardware used at MoF shall be properly accounted for using the following guidelines

- All information asset hardware shall be inventoried on an annual basis
- An MoF property sticker shall be applied to all hardware assets
- Microcomputer equipment (PCs, Servers, etc) shall not be moved or relocated without the prior approval of the involved department manager.
- Loss or theft of information assets shall be reported to site security and <???>

3.1.2 Software Controls

The software used by MoF information assets must be properly licensed according to the particular license agreements. Ministry of Finance shall comply with all legislation, laws and regulations concerning the licensing of the software used in MoF's business practices.

A database of license information shall be maintained

- All software licenses whether paper or electronic, shall be maintained
- Annual audits of software and software licenses shall be conducted
- Agreements for all computer programs licensed from third parties shall be periodically reviewed to ensure compliance
- Third party software shall be registered with the appropriate vendor.

Illegal copies of software shall be removed from MoF information assets or the proper licenses for the software will be obtained.

<License management software that is used to assist in detecting the addition of licensed software and assist in detecting new and/or modified application programs developed by end-users?????>

3.2 Documentation (including Contractual Agreements)

This section applies to documents that have been signed off and now require modification. This change is usually caused by change in the software or hardware areas where documentation associated with it needs update in accordance with the changes made to the hardware or software.

It is important that version control is used on the changed document and that reason for the change is indicated.

The pervious electronic versions should be archived for later referencing in the event that "back-outs" occur.

If it appears that the impact of the change on the system that will result in a change to the documents could be significant, a full review of all other related documentation should be done.

3.3 Changes to Information Assets

Maintaining integrity of information requires application of change control principles. Change management processes shall be followed when:

- Installing software and security patches
- Upgrading or downgrading software to another version
- Increasing existing hardware capabilities and capacities
- Replacing existing hardware

3.4 Change Review Committee

A review committee shall review and approve all changes to the information assets that affect or have the potential of affecting the security, manner, cost, production, profitability, or any other aspect of MoF's business.

The committee shall review:

- New applications – developed internally or by consultant, or purchased from third party
- Modifications to existing applications
- Operating systems – changes, extensions, modifications or replacements
- Hardware – servers, firewalls, routers, etc
- Documentation – user manuals, requirement specifications, contractual agreements

The review committee shall be appointed by the Information Technology Division, of the MoF and should include representatives of user groups that could be affected by the change to information assets.

3.5 Change Control Process

The change control process shall include:

- Proposed changes shall be presented to the review committee prior to the beginning of the development process
- Security issues shall be discussed before developing, including the following
  - General security risks
  - Service interruptions
  - Compliance with the MoF Security Policies and Procedures
- The committee will approve all development and testing plans
- Upon completion on development; development staff shall not be permitted to access production data and systems that are not necessary for their current development and testing work
- All changes should be tested. Testing shall include but is not limited to hands-on functional testing, penetration testing, and verification of the results.
- Whenever appropriate, users shall be included o the testing team
- Testing shall not be performed in a production environment. Whenever possible, separation of testing and production environments shall be achieved via physically separate information systems. If this is impossible logical separation (separate directories/libraries with strictly enforced access controls or firewalls) shall be employed.
- Data used for testing shall be sanitized such that protected health information is sufficiently de-identified (scrambled or mismatched) to ensure confidentiality
- Testing data shall be treated with the same handling procedures that applied when it was production data

- Testing data shall be reviewed and authorised for use by the information custodian(s)
- Validate data prior to performing queries or updates on databases or any data repository. Employ parity checks, check-sums, and error detection data validation techniques.
- The review committee shall evaluate the test results, review the proposed changes, review the revised production schedule, and ensure that the back-out process is complete and tested before implementing the proposed change
- The review committee shall approve all implementations prior to their deployments
- When applying patches or similar software changes to a number of systems (i.e. servers, workstations), it is recommended that these changes be applied progressively from the least to the most critical information asset. This should assist in identifying implementation problems not discovered during testing prior to applying these changes to the facility's most critical information assets.
- A post implementation review shall be conducted and the results presented to the review committee
- All pre and post implementation review results must be documented and stored in a secure location
- Forms should accompany the request for change (appendix 2) when a problem has been identified (appendix 1).
- Once the changes have been made and tests are satisfactory a release form (appendix 3) should be completed and filed.

3.6 Release of Software

Certain controls shall be implemented before moving software from development and testing to the production environment, including:

- Development staff shall not move any software into the production-processing environment
- Technical staff not associated with the testing process shall perform review and recompilation activities
- Automatic updating of software on information assets via "push" technology shall be prohibited unless the involved software has first been tested
- When vendor-testing processes are adequate, and when reliable vendor quality control measures exist, exceptions can be made.
- Adequate "back-out" procedures shall be developed and documented for all changes to production systems, applications or other information assets to allow the original configuration to be re-installed.
- Configuration information, applications and data back-ups of the target system shall be stored separately from the target system.

3.7 Movement of Hardware and Electronic media

Certain procedures shall be followed when moving hardware and electronic media including:

- A retrieval, exact copy of the information stored on the hardware and/or electronic media shall be created prior to the movement of the equipment.
- Records of movements of hardware and electronic media shall be maintained by the responsible department. These records shall include a description of the equipment, the MoF property sticker identification number, date and time of the movement, and person(s) responsible for the movement

3.8 Release of Documentation

Certain procedures shall be followed when a document is released after a change:

- A retrieval copy of the previous document version must be kept in archive
- The new version of the document should be store as a separate version in a library that holds all the documents
- The change to the document should be identified in the change history of the document
- The document should be double-checked and crossed-check that the change has been applied consistently and correctly to all relevant document
- Wording of a change control procedure for inclusion in a contractual agreement should be carefully checked. The approval of the legal service should be sought.

4.1 Appendix 1 – Problem Report Form

4.3 Appendix 3 – Release Form