1.   Purpose

The purpose of this Guideline is to define and provide guidance on
the requirements for managing and documenting changes which take place during
the development, implementation or operation of a computerised system,
including its supporting operating environment.

2.   Scope and Applicability

The change control principles in this Guideline support the delivery and ongoing
support of well-defined systems to meet user requirements. They are essential
when supporting validated processes and maintaining regulatory
compliance.

This Guideline applies to information/business systems, process control systems
and laboratory instrumentation/systems. It applies to the following as applicable
to the specified system throughout its life cycle:

- Application Software
- Operating System Software
- Embedded Software
- Computer Hardware (including microprocessors, PLCs etc)
- Networks
- System and Configuration Data
- System Documentation

This Guideline does not apply to routine changes to data, methods, reports or
facilities that, in principle, are subject to predicate rules (e.g. Good Laboratory
Practice, Good Manufacturing Practice and Good Clinical Practice).

3.   Definitions

3.1   Computerised System

A group of hardware components assembled to perform in conjunction with a set
of software programs which, collectively, are designed to perform a specific
function or group of functions in a defined environment (and including peripheral
devices, personnel and documentation, e.g. manuals, SOPs).

3.2   Change Control

The process of maintaining control of the status of computerised systems by the
establishment of local procedures requiring the evaluation, documentation,
approval and controlled implementation of all changes by qualified
representatives of appropriate disciplines.

3.3   Predicate Rule

The governing national and international regulations and guidance covering Good
Laboratory Practice, Good Manufacturing Practice and Good Clinical Practice.

- Ensure proper communication and consultation regarding the change particularly where a system crosses organizational or functional boundaries

4.3　Central Super User

- Coordinate/implement/manage routine activities so that the change controls are properly applied.

4.4　Project Manager

- Ensures that relevant procedures are followed and that suitable change control procedures are in place before any development or enhancement is made during new system developments or amendments to existing systems.
- Act, with appropriate business support, on behalf of the system owner until formal handover.

4.5　Infrastructure/ Service Manager

- Ensures that due consideration is given to the potential impact of infrastructure changes on supported applications in consultation with the system owner or project manager as appropriate.
- Ensures that formal change control procedures are established and followed for the installation, maintenance and operation of computer hardware and networks, infrastructure software and system and configuration data.

4.6　System Developer

- Uses the formal change control procedure as appropriate to the stage and type of the system development or change
- Evaluates the requested change and providing resource estimates
- Uses appropriate documented development methodologies, including version control and revision comments as applicable
- Implements the requested change when authorised to do so.

4.7　Quality Management

4.7.1　*GxP QA*

- Review and approve, if appropriate, for compliance with GxP.

4.7.2　*IS QM*

- Review and approve for adherence to the IS quality management system.
- Contribute to the development of the validation/qualification approaches for the change.

- Any new support requirements

5.8 Change Completion and Approval

When all elements of a change have been implemented, documentation revised and appropriate testing carried out the system owner or delegate, together with QA as appropriate, should review and approve the formal change request, which should then be archived and the change history updated to include this change.

5.9 Exceptions

5.9.1 Like-for-like (i.e. functionally identical) replacements

It is not always easy to assess whether a situation is truly like-for-like and consideration should always be given to the potential impact of any subtle change. Where there is no discernible change then replacement can be by normal maintenance procedures. Like-for-like replacement should still be recorded in the system history.

5.9.2 Emergency changes

It is recognised that certain changes need to be implemented as quickly as possible. These situations will commonly arise when a user or system owner reports a fault in a critical area of use or operation and its resolution is essential to completion of a time-dependent task. What constitutes an emergency change should be clearly defined.

Even in an emergency, testing of critical elements of the change should be carried out before implementation to avoid unforeseen serious repercussions. Any necessary interim procedures should be considered and specified. **The change must be subsequently reviewed, tested, documented and approved according to the appropriate procedure and in a timely manner.**