AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE

To ensure that all changes to systems, applications, services, configurations, or code are managed in a structured, secure, and controlled manner to minimize risk to information security, system availability, integrity, and compliance.

SCOPE

This procedure applies to all changes within the organization's development, staging, and production environments, including but not limited to:

- Source code and infrastructure-as-code
- Application deployments
- Configuration changes

Note: Office network infrastructure is managed by the shared office provider and is out of scope.

REFERENCE

ISO/IEC 27001 Standard Annex A 8.32 Change management

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.

The responsible party that will be implementing the change shall carry out change management in line with this procedure.

PROCEDURE

A. Initiation, Review and Approval

- A change request (CR) must be submitted through the change tracking system (e.g., ticketing tool).
- It must include:
    - Description of the change
    - Reason/justification
    - Systems/services affected
    - Risk and impact assessment
    - Proposed implementation schedule
    - Rollback plan

- Changes must be reviewed and approved by the authorized approver for the change (e.g., System Owner, Top Management).
- The Approving Authority grants approval based on risk, impact, and readiness, or rejects/request modifications.

B. Development and Pre-Deployment Preparation

Assigned developers shall develop new code, configurations, or infrastructure updates as specified in the change request, make the required modifications in the development or staging environment, and document changes made for traceability.

Deployment shall be planned, usually aiming for low-impact or off-peak hours. Backups or snapshots of affected systems shall be taken to enable rollback if needed.

C. Testing and Deployment

The assigned tester or QA shall conduct thorough testing in non-production environments. The testing may include any of the following whichever is applicable:

- Functional testing
- Integration testing
- Security testing
- Performance and load testing
- User acceptance test (UAT), if applicable

Testing results must be documented and approved prior to production deployment. Once approved, the changes will be deployed according to the approved schedule, preferably during low-impact periods.

Only authorized personnel shall perform deployment. Automated deployment processes shall be followed when possible, ensuring logging and traceability.

D. Post-Deployment Verification and Monitoring

Development team shall verify that the deployed change is functioning correctly immediately after deployment. They shall perform initial functional checks and troubleshooting if issues arise, and continuously logs and system performance closely. If critical problems arise, the rollback plan will be executed to restore the previous stable state.

The assigned developer shall document the outcome of the change including any issues or lessons learned, and update the change management records accordingly.

E. Exceptions

Certain routine or low-risk changes may qualify for a waiver from the full change approval process. A waiver request must be submitted and documented, including justification and risk assessment. Waivers shall be reviewed and approved by the top management or designated authority prior to execution.

Emergency changes necessary to address critical issues (e.g., security vulnerabilities, system outages) may bypass the standard request, review and approval process to enable rapid response. Emergency changes must still be documented in the change tracking system with a description of the urgency and risk. Post-implementation review and approval shall occur within a defined timeframe (e.g., 24-48 hours) after deployment to validate the change and ensure compliance.

All exceptions shall be recorded in the change tracking system, including approver details, reason for exception, and any compensating controls implemented.