Aberrant Open-ISM™

CHANGE CONTROL POLICY

Property	Description
Document Version	1.0
Status	DRAFT
Last Update	2022-03-25
Document Owner	Risk Management
Next Scheduled Review	

Document Approvals		
Approver Name	**Title**	**Date**
???	???	???

Revision History			
Version	**Date**	**Description of Changes**	**Revised by**
1.0	2022-03-25	DRAFT	Aberrant

TABLE OF CONTENTS

1 OVERVIEW

Change Management is necessary to ensure that any modifications to the IT environment that affects information security is properly assessed, authorized and monitored. The Change Management policy provides guidance on how change will be conducted in the <<Company Name>> environment and defines the types of changes that are covered by this document. This policy is synonymous with secure configuration.

2 PURPOSE

The purpose of this policy is to communicate the intent that changes to the supported information technology and applications at <<Company Name>> will be managed and implemented in a procedure that minimizes risk and impact to the organization. Per this policy, a change is defined as anything that transforms, alters, or modifies the operating environment or standard operating procedures that have potential to affect the stability and reliability of <<Company Name>>'s supported information technology infrastructure, and disrupt day to day operations. A change, as defined by this policy, can be planned or unplanned.

3 SCOPE

This policy covers changes to <<Company Name>> supported systems, such as hardware, software, applications and the networking environment, of which any business line of <<Company Name>> relies upon to perform normal business activity. Changes may be required for many reasons, including:

- User requests
- Vendor recommended/required changes
- Changes in regulations
- Hardware and/or software upgrades
- Acquisition/implementation of new hardware or software
- Hardware or software failures
- Changes or modifications to the infrastructure
- Environmental changes (electrical, air conditioning, data center remodels, etc.)
- Unforeseen events
- Periodic maintenance

Changes not covered by this policy include:

- Changes to an employee's desktop/laptop.
- Allocation of IP addresses.
- Updates to an office phone, etc.
- Unlocking locked accounts.

- Password resets.
- Changes implemented via the Software Development Lifecycle (SDLC).

This Policy applies to personnel who install, operate, or maintain the aforementioned information technology upon which any unit of the business relies on in order to perform its normal activities. In addition, the policy applies to all employees, as they need to be informed and aware of the policy since they may have occasion to request a change, approve, test, and thus are thereby subject to following the prescribed process.

3.1 DISRUPTIVE CHANGES

Some requests may have a material impact on operations. As a result, it imperative for IT Operations Management to coordinate disruptive changes with impacted stakeholders. There are several types of changes described as follows:

- **Scheduled Change**: Changes are planned in advance with appropriate approvals, notification to stakeholders, change scripts and back-out planning in place ahead of time;
- **Emergency Change**: When an unplanned immediate response is needed to prevent widespread service disruption. Approval will be sought as soon as practical for any such change. Failure to plan ahead does not constitute an emergency change;
- **Unscheduled Change**: Failure to present notification to the formal process in advance of the change being made or following appropriate emergency change procedures. Unscheduled changes are not acceptable.

Changes will be implemented to minimize disruption to users. Notification will be provided to all internal and external stakeholders with enough information and in enough time for them to request changes to the implementation schedule or make alternate arrangements. Please review the Scheduled Maintenance section of the Information Security Policy for more information.

3.2 CHANGE CONTROL AND THE SDLC

SDLC changes deployed to production require a change control request prior to migration of the deployment into production—this ensures a smooth hand-off to operations and site-reliability engineering when code is deployed.
SDLC code deployments should always incorporate a rollback strategy in the event that a deployment goes badly. Deployments should conduct smoke testing to ensure a deployment is stable before finalizing the deployment.

4 DESIGN PRINCIPLES

4.1 SEGREGATION OF DUTIES

The ability to migrate changes into the production environment is restricted to authorized and appropriate users based on job description.

Temporary access to the production environment can be granted to users on a timebound basis. An example, developers are generally prevented from accessing production systems, however, periodically a production issues arise that are difficult or impossible to create in a lower non-production environment. In this case, temporary access to the production system may be granted to so that the developer can forensically troubleshoot the issue using production log data.

4.2 PRINCIPLE OF MINIMALISM

Requests should be approved based on a principle of minimalism. For example, software that isn't directly required by an employee to perform their job function should not be approved. Likewise, the least amount of privilege should be granted to employees regarding systems access or user roles.

4.3 TRANSPARENCY

Access to work items submitted to the change control process should be visible to the requestor, and to IT management.

4.4 WORKFLOW

The change control process should leverage Kanban with the following swim lanes:

- Awaiting Assignment
- In-Process
- Completed
- Awaiting Review
- Reviewed
- Closed

4.5 COMPLIANCE MEASUREMENT

Change control requests should meet a defined SLAs, SLOs, RPO, and RTOs. The security personnel will verify compliance to this policy.

5 POLICY COMPLIANCE

Any change that falls with the scope of the Change Control Policy must be entered in <<Name of Change Control System>>. <<Name of Change Control System>> is the system of record for change control at <<Company Name>>.

5.1 REQUEST TYPES

The following request types should be supported.

1. "Access Control" Changes: adding users or groups, removing users or groups, modifying permissions, service accounts.
2. "End User Devices": laptops, user operating systems, installed software, including portable and mobile, non-computing/IoT devices.
3. "Platform Infrastructure": containers, servers, server operating systems. installed software, certificates.
4. "Deployment": Deployment into production from the SDLC.
5. "Network Infrastructure": WAFs, DLPs, CASBs, CDN, DNS, Network Firewalls, Load Balancers, HSMs, Cloud Infrastructure, Web Access Points, etc.
6. "POC": test deployments of applications or systems prior to acquisition.

It should be noted that as the company "shifts left" the percentage of activities that fall with the scope of the SDLC will increase as change control diminishes.

5.2 THE CHANGE CONTROL PROCESS

5.2.1 CREATING A CHANGE CONTROL REQUEST

The change control request should include the following information:

- Type of request: ["Access Control", "End User Devices", "Platform Infrastructure", "Deployment", "Network Infrastructure", "POC"]
- Request Title
- A reason for the change.
- A detailed description of the requested change.
- The identity of the requestor.
- Documentation of impact so that the change can be validated as successful.
- User Acceptance Tests (UAT)—when applicable.

5.2.2 REVIEW OF CHANGE CONTROL REQUESTS

IT Management should review

IT Operations should review the request after it has been entered into the change control system. IT Operations personnel should verify the following information:

- Verification that the change control request is completed correctly.
- Verify the UAT.

5.2.3 CHANGE CONTROL REQUEST APPROVAL AND PRIORITIZATION

IT Management should:

- Approve or reject the request.
- Evaluated the request against priorities and approved.
- Identify requests that have the potential to impact normal operations.
- Assign the request to a resource.

5.2.4 CONTROL REQUEST IMPLEMENTATION

IT Operations should:

- Schedule the request.
- Functionality testing and verification of successful completion or a rollback of the procedure in the event of failure.
- Management of the request through the Kanban swim lanes.
- Ensuring notification to external or internal customers in the event of a disruptive change.

5.2.5 QUALITY CONTROL AND USER ACCEPTANCE

- Changes should be validated by Operations.
- The business-owner should sign-off that the ticket once it is completed.

5.3 EXCEPTIONS

Any exception to the policy must be approved by a owner of IT Operations.

5.4 NON-COMPLIANCE

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.5 RESPONSIBILITY AND AUTHORITY

All employees within the organization have a role and responsibility with regards to change management.

5.5.1 END USER MANAGEMENT / FUNCTIONAL USER

End users / functional users are responsible for:

- Submitting change requests with complete information.
- Participating in testing, pre-deployment testing, and post deployment testing, and
- Timely sign off for the change

5.5.2 IT OPERATIONS

The IT Operations is responsible for:

- Following the prescribed change management processes and procedures.
- Ensure requests are completed in a timely fashion and meet compliance requirements—e.g. SLOs.
- Implementing requests.

5.5.3 IT OPERATIONS MANAGEMENT

Is responsible for:

- Overseeing the change management policy and process.
- Reviewing changes and closing tickets to ensure that the work was completed correctly.
- Ensuring compliance with policies and procedures, e.g. management of privileged access rights, etc.
- Ensuring oversight of the process, such as prioritization of change control requests, and final approval of implementation of any change into production.
- Ensuring notification to external or internal customers in the event of a disruptive change.

6 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

7 DOCUMENT RACI

Responsible	Assigned to do the work	Security Program Manager
Accountable	Final decision, ultimately answerable	ISM Governance Committee
Consulted	Consulted BEFORE an action or decision is taken (proactive)	Executive Management
Informed	Informed AFTER a decision or action has been taken (reactive)	Named Participants in this document Other parties affected by the change

8 LICENSE INFORMATION

APPENDIX A: GLOSSARY OF TERMS

RPO: Recovery Point Objective.

RTO: Recovery Time Objective.

SLA: Service Level Agreement.

SLO: Service Level Objective.