CHANGE MANAGEMENT POLICY

Quality Department

1 Policy Statement

The Change Management Policy shall help to communicate the Management's intent that changes to Information and Communication Technology (ICT) supported business processes will be managed and implemented in a way that shall minimize risk and impact to ***Safe and Secure trading Est***. and its operations. All changes to IT systems shall be required to follow an established Change Management Process. This requires that changes to IT systems be subject to a formal change management process that ensures or provides for a managed and orderly method by which such changes are requested, approved, communicated prior to implementation (if possible), and logged and tested.

2 Definition

Change Management: 'Any change which may affect financial reporting, operations or compliance. This includes the Control Environment (i.e. all systems business processes including IT which may impact the above). The key activities required are;
• Monitoring,
• Informing and communicating,
• Control activities (reviews and reports).
• Risk Assessments
• Control environment (i.e. passwords, user access).

3 Purpose

The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:
i. Information being corrupted and/or destroyed.
ii. Computer performance being disrupted and/or degraded.
iii. Productivity losses being incurred.
iv. Exposure to reputation risk.

4 Scope

4.1 Employees

This policy applies to all parties operating within the organization's network environment or utilizing Information Resources. No employee is exempted from this policy.

4.2 IT Assets

This policy covers the data networks, local servers, and personal computers (stand-alone or network-enabled), located at offices and depots, where these systems are under the jurisdiction and/or ownership of the organization, and any personal

computers, laptops, mobile devices, and servers authorized to access the organization's data networks.

4.3 Documentation

The Policy documentation shall consist of Change Management Policy and related procedures and guidelines.

4.4 Document Control

The Change Management Policy document and all other referenced documents shall be controlled. Version control shall be used to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purposes.

4.5 Records

Records being generated as part of the Change Management Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

4.6 Distribution and Maintenance

The Change Management Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

5 Privacy

The Change Management Policy document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

6 Responsibility

The CISO / designated personnel is responsible for the proper implementation of the Policy. The Department Manager ensures that changes follow the Change Management Process. The Director of Central Services reviews the Change Management Schedule monthly to ensure all changes follow the Change Management Process. The Management Executive Committee reviews the Change Management Schedule quarterly to ensure changes follow the Change Management Process.

7 Policy

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed

are reviewed, authorized, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored. In order to fulfill this policy, the following statements shall be adhered to:

1. A current baseline configuration of the information system and its components shall be developed, documented and maintained.
2. A current inventory of the components of the information system along with the owner shall be developed, documented and maintained.
3. The baseline configuration of the information system shall be updated as an integral part of the information system component installation.
4. Changes to the information system shall be authorized, documented and controlled by the use of formal change control procedure.
5. Changes in the configuration of the information system shall be monitored through configuration verification and audit processes.
6. The information system shall be configured to provide only essential capabilities and shall prohibit and /or restrict the use of specific functions, ports, protocols, and/or services. A list of prohibited and/or restricted functions, port, protocols etc. shall be defined and listed.
7. The inventory of the information system components shall be updated as an integral part of the component installation.
8. Automatic mechanism/tools shall be employed to maintain an up-to-date, complete, reliable, accurate and readily available configuration of the information system.
9. Automatic mechanism/tools shall be employed to initiate changes/change request, to notify the appropriate approval authority and to record the approval and implementation details.
10. The information system shall be reviewed at a defined frequency to identify and eliminate unnecessary functions, ports, protocols, and/or services.

8. Change Procedure:

For compliance purposes all communications need to be in writing, i.e. by email, meetings need to have minutes taken, etc. This documentation will be retained by the Change Management Controller and filed with the Change Documentation relating to the change. For this reason, verbal requests and authorization are not acceptable.

8.1 Risk

If not properly controlled changes could be made which negatively impact the business and prevent people from fulfilling their roles. Changes could be made by individuals who are not fully aware of the impact on other areas of the business. If change is not controlled the Business could be exposed to fraudulent activities.

8.2 Roles

It is the Change Management Controllers' role to facilitate communications between the Department Manager requesting the change and any other affected Department Managers, these will be referred to as the Stakeholders. The Change Management Controller will coordinate all of the documentation, acquisition of requirements, formulations of plans, and scheduling of projects and tasks. It is the role of the

requesting Department Manager and other Stakeholders to review, comment on and authorize documents relating to the change, instruct staff, and participate in meetings to ensure that the change goes as smoothly as possible and that compliance is retained.

8.3 Submit the Change Request Form

- Complete a Change Request Form. This form and information about how to complete it can be found IT Manager.
- Enter as much detail as possible in the Request Details section. If this change will affect other departments please enter the names of the Department Managers in the Other Departments Affected section.
- Once the form has been completed use the office or branch scanner to scan the authorized form and email it to the IT Help desk. They will log the form and pass it to the Change Management Controller so that the change can be scheduled.

8.4 Review the Specification

The Change Request Form will be reviewed by the Change Management Controller who will gather additional information, add Department Managers deemed to be affected, and arrange meetings. Then the Change Management Controller creates a Specification detailing exactly what is being changed, which is sent to all Stakeholders. The Specification should incorporate all the requirements.
• The Change Stakeholders carefully review the Specification to ensure that all the requirements and their particular interests are covered.
• The Change Stakeholders will need to approve the specification by email.

Note regarding the Change Rating:
The Change Management Controller will discuss what the appropriate Change Rating should be with all the Stakeholders. In essence, the Change Rating indicates the level of compliance required by the change and the priority that the change is being given.

8.5. The Risk Assessment

The Change Management Controller will conduct a risk assessment based on the agreed specification. They will check all the systems and processes affected by the proposed change and list any risk areas. The Risk Assessment is used to create a change Recommendation to ensure that any risk to the business has been identified and mitigated. The Recommendation will include items such as specific training and testing requirements. A copy of the Risk Assessment, including the recommendation, will be sent to the Stakeholders.

- Check the Risk Assessment and Recommendation carefully to make sure that nothing has been missed.
- Notify the Change Management Controller, by email, of any missing risks or if there are problems with the Recommendation.
- Authorize the Risk Assessment and Recommendation by email.

8.6 The Implementation Plan

The Implementation Plan details all the stages that are required in order to successfully manage the change and includes a Test Plan and Roll Back Strategy. In more complicated changes this may also include a project schedule and timeline.

- Review the Implementation Plan.
- Make the Change Management Controller aware of any amendments or changes.
- Make note of the timeline and any training or testing and how this will affect department staff.
- Make note of any dependent tasks (i.e. if one department is unable to make a change until another has completed theirs).
- Authorize the Implementation plan by email.

8.7 Pre-Change

Once the Implementation Plan has been approved it is vital that the staff in each department are made aware of what needs to happen, when and by whom. The Department Manager:

- Notifies affected Staff of the change and assigns actions and makes them aware of the Roll Back Strategy.
- Ensures that Staff who have been allocated Test Actions have copies of the Test Plan and are aware that all test documentation is to be retained.
- Leases with other Stakeholders and the Change Management Controller to ensure that all aspects of the change are progressing as planned.

8.8 . Change

To minimize unnecessary disruption ensure that the plan is followed as closely as possible and any issues are highlighted to the Change Management Controller as soon as possible. The Change Management Controller will coordinate communications between all the Stakeholders. Ensure all staff follows the Implementation Plan.

8.9 Post Implementation Review:

Once a change has been implemented it is important that the situation is reviewed to identify any problems that could be prevented in the future or improvements that could be made. The Stakeholders will carry out a Post Implementation Review one month after the change has been promoted to Live (unless problems or issues present themselves more immediately). Two months after the change has been implemented the Stakeholders will conduct a further review. The Management Executive Committee will review Change Documentation and follow up material quarterly. The minutes and action points of these reviews are held on file with the Change Documentation. The Internal and External Auditors will examine the Change Management Documentation on a half-yearly and End Year basis and their comments and recommendations will be acted upon.