CONTENT:

This General Instruction (GI) outlines the IT Change Management necessary guidelines to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of IT resources. This GI includes:

1.0 PURPOSE

The purpose of this policy is to communicate IT Change Management's intent that any direct or indirect changes to IT production infrastructure be managed and implemented in a way that minimizes risk and impact to the company. For purposes of this policy, a change is defined as anything that transforms, alters, or modifies the operating environment or standard operating procedures that have the potential to affect the stability and reliability of IT production infrastructure and disrupt the business of the company. A change, as defined by this policy, can be planned or unplanned. All changes to IT production systems are required to follow the established IT Change Management Policies, Processes and Procedures. Changes to IT production infrastructure must 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, logged and tested.

2.0 SCOPE

This GI covers changes to IT production systems (hardware, software, applications, facilities and network environment) upon which any functional unit of the company relies on, in order to perform its normal business activities. Power sources supporting these systems are also included.

3.0 DEFINITIONS

** 3.1 Change Requester – The initiator of the Change Request. This could be the business proponent or the support staff analyst implementing the change.

** 3.2 Change Coordinator (CC) – The support staff analyst responsible for administering and supervising the implementation of the change request.

** 3.3 Task Implementer – The individual who is responsible for implementing the task assigned by the CC in the change request.

3.4 Technical Change Coordinator (TCC) – The Department's technical authority that reviews and approves change requests.

* 3.5 Change Manager (CM) – The highest authority that performs the final review of change requests in order to have them approved and scheduled.

* 3.6 Change – Any alteration to the state or configuration of any production software or hardware under IT management and support. This includes adding new functionality, modifying, repairing or removing functionality. It also includes IT environment scanning and any changes to the power systems feeding the IT infrastructure as well as facility changes.

3.7 Change Request (CR) – Used to document details and approvals of a request for a change, which is sent as an input by the Change Requestor to IT Change Management and all involved TCCs.

3.8 IT Change Management (ITCM) – The process of controlling modifications to hardware, software, applications, facilities and network environment, to ensure IT resources are protected against improper modification during and after system implementation.

* 3.9 Change Advisory Board (CAB) – Group of designated individuals that represent business entities who meet weekly to discuss and authorize CRs.

3.10 Scheduled Change (Planned) – Formal notification received, reviewed and approved through the review process in advance of the change being made.

3.11 Unscheduled Change (Planned/Unplanned) – Failure to present notification to the formal process in advance of the change being made.

* 3.12 Normal Change (Service Affecting) – Impacts service delivery such as all shared hardware, systems software, application software, or procedural changes which could impact the infrastructure, and possibly impacts production services.

* 3.13 No Impact Change (Non-Service Affecting) – This is a change that proves to be of no impact on the service delivery, such as weekly routine jobs and new installations.

3.14 Emergency Change (Unplanned) – A change that does not present notification to the formal process in advance of implementation. An emergency change is the result of a system failure, a potential system failure or the discovery of security vulnerability. Assessment and approval for such change will take place post implementation.

3.15 Project CRs – This type of CR is used to correlate changes (Service affecting and non-service affecting), such as a set of changes for a particular project. Project changes are not considered routine weekly/monthly work.

3.16 Post Implementation Review (PIR) – A standard method to follow-up with the change owner and/or customer on the results of a CR.

4.0 POLICIES

4.1 A CR can be for a global (companywide) or a specific location (e.g., area, city, building, etc.), and has to specify the system(s) (e.g., server, router, switch, etc.), applications (e.g., SAP, proxy, Remedy, etc.) and affected services.

** 4.2 Third-party vendors related activities must be covered under a CR, or otherwise through separate task(s) under the main CR.

* 4.3 A CR must have the implementation plan, backout plan, test plan, risk assessment and users' notification documents attached, and all required assessment fields filled, and at least one task created. This applies to all CRs Normal, No Impact or Emergency. The only exception is not being required to attach the users' notification for: 1) No Impact CRs, 2) Normal CRs occurring during predefined and approved block times.

* 4.4 Emergency, global, international, and users/assets affecting CRs must be nominated as IT morning report (ITMR) items and their relevant ITMR forms completed.

* 4.5 Any post approval modification to the CR should be coordinated through the CM.

** 4.6 The CM must be involved in any coordination with other entities after the change has been approved and scheduled.

4.7 A CR must be put on HOLD with an update in the comments log in case a TCC/CM requires more assessment.

4.8 CCs and/or task implementers must not start the implementation until the CR is approved and scheduled, with the exception of a CR that is classified as Emergency.

* 4.9 A Service Affecting (Normal) change must not be implemented during prime time or office hours, except with proper justification. Additionally, proponent concurrence (site Foreman/Superintendent) or a Department Head (Manager) approval is required.

* 4.10 Modifications to the CR must be documented in the work detail log.

4.11 A justification must be provided in the approval comment/work detail log activity when the CR is rejected or its approval process is cancelled.

4.12 Any non-Emergency CR reaching the CM after implementation will be rejected.

* 4.13 All change participants must close their assigned tasks and CRs within 24 hours after implementation, excluding weekends and holidays.

4.14 One representative from every TCC discipline must attend the weekly CAB meeting.

* 4.15 Any extension of a service affecting CR duration while under implementation must be justified and linked with an Emergency CR to cover the overrun to the original CR's schedule.

** 4.16 Any extension of a non-service affecting CR duration while under implementation is permitted with business justification up to the maximum allowed duration based on the non-service affecting guidelines.

** 4.17 Post-change reviews must be performed for Emergency and Unsuccessful changes, to ensure implementation activities are documented and reviewed.

* 4.18 The change requester and/or coordinator will be responsible for planning to replicate changes to applicable and corresponding disaster recovery (DR) systems.

** 4.19 Any change to a system/service which is identified to have a corresponding DR system, must include a documented plan to replicate this change to its relevant DR system. The main CR must either include a task in case an immediate replication to the DR system is required (e.g., Server OS patching), or include a CR# in case a deferred replication is required (e.g., DB upgrade). This change must also be approved by the IT Business Continuity Management Group.

** 4.20 The change implementer and/or coordinator will be responsible for the update of relevant documentation affected by the change (such as IT Service Catalog/CMDB, system documentation and inventory lists, operational procedures, configuration information, application documentation, help screens, and training.)

* 4.21 Standard Risk Assessment Rating Guidelines must be followed and performed for all types of CRs.

* 4.22 Each CR in the ITCM Documenting Tool must have accurate actual start and end date & time to reflect the time spent to resolve.

4.23 In compliance with the segregation of duties principle, the Change Requester and/or the CC must not approve their own CRs.

* 4.24 A CR must be in any approver's basket minimum of four business (4) hours for assessment and approval prior to its scheduled start date & time. Assessment and approval should not exceed eight (8) business hours for any approver. Should there is a need for additional time beyond the specified time, policy 4.7 must be exercised. This excludes emergency CRs.

5.0 VIOLATIONS

Violating this GI, or the promulgated policies, processes, and/or procedures may result in disciplinary actions that can be classified as follows:

5.1 Violation will be issued when:

* 5.1.1 An Emergency CR was initiated and implemented but didn't meet the Emergency CR guidelines.

* 5.1.2 Unauthorized work carried out without a CR or before the CM's approval.

* 5.1.3 Approved CR was implemented before or after the scheduled implementation date and time.

** 5.1.4 A SAP Transport is implemented resulting in service outage without a documented CR in the IT Change Management Documenting Tool.

* 5.2 Observation will be issued when a Non-Service Affecting Change turns into a Service Affecting Change, with the escalation below:

** 5.2.1 The observation will be sent to the Head of the involved Department.

** 5.2.2 The second observation onward by the same Department during a calendar year will automatically turn into a violation.

** 5.3 Warning will be issued when not complying with the GI or its associated ITCM Guide, Process & Procedure Manual, with the escalation below:

* 5.3.1 The warning will be sent to the employee copying his/her Unit Head (Supervisor).

** 5.3.2 The third warning onward by the same employee during a calendar year will automatically turn into an observation.

* 5.4 First three (3) Department violations within a calendar year:

For each committed violation, a violation report will be sent to the Head of the violating Department.

5.5 Four (4) or more Department violations within a calendar year:

5.5.1 For each committed violation, a violation report will be sent to the IT Admin Area Head copying the proponent's Department Head.

5.5.2 If the violating Department is non-IT, the report will be sent to the violating Department's Admin Area Head copying the IT Admin Area Head and the proponent's Department Head.

5.5.3 The annual violation counter for the Department will be reset to zero at the end of each calendar year.

** 5.5.4 Any post violation feedback should be communicated by the Department Head.

** 6.0 ROLES & RESPONSIBILITIES

6.1 The CC is responsible for identifying approximately the number of users impacted or by location.

6.2 The CC is responsible for required communication and announcements for Emergency CRs, where applicable.

6.3 The Information Protection Management Division (IPMD) is the owner and custodian of this GI.

6.4 The Services Management Division (SMD) is the owner and custodian of the IT Change Management Guide, Process & Procedure Manual.

**

7.0 REFERENCES

* For operational details, please refer to the IT Change Management Guide, Process & Procedure Manual by **clicking here**.

______________________ Date	Concur:	______________________ **IT Change Management Process Owner**
______________________ Date	Concur:	______________________ **Manager,** Communications Operations Department
______________________ Date	Concur:	______________________ **Manager,** Information Protection & Technology Planning Department
______________________ Date	Approve:	______________________ **Executive Director,** Information Technology