



JOUF UNIVERSITY

INFORMATION TECHNOLOGY DEPARTMENT

IT Change Management Policy

COPYRIGHT NOTICE
Copyright© 2020 by ITD-JU

ALL RIGHTS RESERVED

The information contained herein is proprietary and confidential information for the use of IT Department of Jouf University, personnel only. No part of these materials should be reproduced, published in any form by any means, electronic or mechanical including photocopy or any information storage or retrieval system nor should the materials be disclosed to third parties unless previously authorized in writing by IT Department of Jouf University. Product names mentioned herein are for identification purposes only and may be Trademarks and/or Registered Trademarks of their respective companies. This document is proprietary and confidential for Integrated Telecom Company.

Document Control

Document Number
JUIT-POL-02

Review History Sheet

Process Owner	Author	Next review date

Version Control Sheet

Version	Date	Author	Revision Notes
1.0			

Quality Management

This document shall be reviewed on an annual basis or more frequently if required. The Head of IT Department shall approve any changes or amendments to this document and revisions to this document shall specify the previous versions of the plan.

Distribution List

All IT Personnel

Table of contents

Contents

Section A – Overview	5
1. Purpose.....	5
2. Scope	5
3. Responsibility	5
4. Distribution	5
5. Review and Update	5
6. Effective Date	6
Section B – Mandate	6
7. Change Request.....	6
8. Change Review and Management.....	6
Section C – Policy Governance	7
9. Procedures for Amendment	7

Section A – Overview

1. Purpose

The purpose of this policy is to institute a robust IT Change Management Process that governs the changes proposed in JUIT environment and to ensure that all changes are made in a thoughtful way that minimize negative impact to systems and services. The policy aims to establish standard procedures for managing change requests in an agile and efficient manner in an effort to drastically minimize the risk and impact a change can have on business operations.

2. Scope

- 2.1. The scope of Change Management covers the life cycle of strategic, tactical, and operational changes to JUIT environment.
- 2.2. The contents of the policy are applicable to all of the JU's personnel. Any exceptions to these are strictly discouraged and shall require prior approval by the Top Management.
- 2.3. The policy should be read in conjunction with the IT Procedures, for further guidance on how to execute the policy.

3. Responsibility

- 3.1. The Head of the IT is the custodian of this policy and he/she is responsible for implementation of this policy.

4 Distribution

- 4.1 This Policy shall be made available to the employees in a non-editable version on JU's intranet. All employees who are involved in the IT Service Management activities shall have a thorough understanding of this Policy. JOUF UNIVERSITY and Departments within JOUF UNIVERSITY will, where deemed necessary, implement more detailed procedures which are designed to support the fund's on-going compliance with among other things, this policy.

5 Review and Update

- 5.1 This policy shall be reviewed on an annual basis, or more frequently if required, by the Head of IT.
- 5.2 Any changes to the policy, however, shall be approved by the Top Management, based on a recommendation from the Director IT Services.
- 5.3 Any amendments and revisions to the policy shall specify the superseded versions of the policy, which shall be retained for future reference.

6 Effective Date

6.1 The policy is effective from the date it is approved by the Top Management.

Section B – Mandate

7 Change Request

7.1 The IT Department shall develop a pre-approved list of simple, routine and minor changes that involve little to no risk. The list shall be approved by the Head of IT and the Head of IT Security. These changes shall be designated standard changes for the purposes of tracking and approval.

7.2 The IT Department shall only proceed with changes that are compliant with the [Minimum Security Requirements] provided by the IT Security Department.

7.3 The IT Department shall follow the relevant procedures for change management.

7.4 Where a change is required to restore normal functionality, the Head of IT shall be authorized to designate a change as an "emergency" change. For an emergency change, the IT Department shall allocate resources and begin work before obtaining the necessary approvals.

8 Change Review and Management

8.1 Major technology and system changes shall go through a Change Advisory Board (CAB).

8.2 The IT Department shall segregate the development, testing and production environments to reduce the risks of unauthorized access or errors in the production systems.

8.3 The test system environment shall emulate the production environment as closely as possible, but shall not include confidential data.

8.4 The IT Department shall restrict access of the Development Team to the Development and Testing environments only, in addition the developer who shall program or develop the change shall not promote changes/ programs in and out of production, or perform monitoring controls related to program development and changes.

8.5 User acceptance testing shall be performed for all changes by requesting business user. In addition, considering the nature of change, the Change Manager shall decide if any other type of testing (such as technical, integration) is required or not.

8.6 The IT Department shall prepare periodic change management status reports as a part of the Performance Management process.

- 8.7 Information Security Department shall review all changes prior to implementation in production, so that the change is in compliance with the Information Security Policy and that the change does not introduce any security vulnerabilities to the JU's information systems environment.
- 8.8 Rollback plans shall be established prior to implementing any change by the respective IT implementation team.
- 8.9 Upon successful implementation of the change in production environment, the change shall also be implemented in the Disaster Recovery environment by the respective IT implementation team, if applicable.
- 8.10 Processes for the transfer of software from development to production environment shall be defined and documented by IT Department.

Section C – Policy Governance

9. Procedures for Amendment

- 9.1. Any changes to this policy may be requested to and/or initiated by the Head of IT under the following circumstances:
- a) Changes in applicable statutes;
 - b) Any operational requirement as approved by the Top Management; or
 - c) Any other situation where the revised policy will bring about economies of scale and improved efficiency.
- 9.2. The proposed amendment shall be prepared in draft form and shall be forwarded to the Head of IT with justification for the amendment.
- 9.3. The Head of IT shall review and forward the same to the Director IT Services.
- 9.4. The Director IT Services shall review and recommend the same to the Top Management for its approval and upon getting approval from Top Management, the amendments shall be incorporated in this policy.
- 9.5. At the beginning of the policy, an Amendment History Sheet will be kept to record the changes in the Policy, along with a Version Approval Sheet which will be kept to record the approval of new versions of the policy from time to time.