CHANGE MANAGEMENT INFORMATION TECHNOLOGY POLICY

Policy Code: TM5
Version: 2
Approved by: The Board
Approval Date: 11/04/2024
Decision No.: B.01.2024.04

The Da Vinci Institute for Technology Management (Pty) Ltd
Registered with the Department of Education as a private higher education institution
under the Higher Education Act, 1997. Registration Certificate No. 2004/HE07/003

Table of Contents

1. INTRODUCTION

Information Technology (IT) 'change management' refers to a formal process for making changes to information technology services. The purpose of change management is to implement proposed changes across the institution and ensure that all changes are made in a considerate manner that minimise negative impact to services and customers.

Adopting formalised governance and policies for operational change management contributes to a more disciplined and efficient infrastructure. The goal of the change management process is to ensure that any changes to existing, or introduction of new software or hardware within the Da Vinci Institute's information technology production environment is done in an orderly and controlled manner. Ensuring effective change management within the IT production environment is extremely important in ensuring the efficient delivery of IT services while reducing the risk of service interruption.

DEFINITIONS

Term	**Definition**
Emergency	A serious, unexpected, and often dangerous situation requiring immediate action
Hardware	Is the physical parts or components of a computer, such as monitor, keyboard, computer data storage, graphic card, sound card, motherboard, etc., all of which are tangible objects
Maintenance window	Is the defined period of time when maintenance such as patching software or upgrading hardware components can be performed
Patching	A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually called bugfixes or bug fixes, and improving the usability or performance of programs
Software	Is a set of instructions and associated documentation that tells a computer what to do or how to perform a task or it can mean all the software on a computer, including the applications and the operating system

2. LEGISLATIVE CONTEXT

The Change Management Information Technology Policy is benchmarked against, and should be read in the context of the relevant legislation underpinning the principles against which institutional policies, processes and standard operational procedures are developed, implemented and maintained. This includes:

i. Electronic Communications and Transactions Act No. 25 of 2002.

Da Vinci policies:

ii. Electronic Information and Communication Systems
iii. Finance
iv. Firewall
v. Incident and Service Management
vi. Information Security
vii. Language
viii. Privacy and Confidentiality
ix. Records and Administration Management
x. Reputational Risk
xi. Wireless Communications.

3. SCOPE

Da Vinci's Change Management Information Technology Policy applies to all IT changes including any alteration to any software system or application, hardware or network infrastructure that in any way may impact on operations at Da Vinci at any of its premises, or any remote location directly connected to the Da Vinci network.

4. PURPOSE

The purpose of the Change Management Information Technology Policy is to provide a sound understanding of Da Vinci's change management process for all information technology-related changes. 'Changes' in IT refer to any alteration to any software system or application, hardware or network infrastructure that in any way may impact on operations at Da Vinci.

5. CHANGE MANAGEMENT CONTROL PROCESS

The purpose of the change management control process is to communicate the process and the appropriate controls to manage and mitigate the risk and potential negative impact any change may have on the systems, hardware and networks of Da Vinci.

5.1 Change initiation

Change initiation is the first step towards implementing a change. It is the acknowledgment from the parties concerned that they are ready and prepared to implement the change. For software changes the necessary configuration or development has already been completed and tested. For hardware and network infrastructure changes it may not be practical to test, but an effort should be made to test changes as far as possible.

6. Communication

An important aspect of change management is the necessary communication before, during and after the change. All affected parties and stakeholders must be made aware of the intent to make changes in the live environment and their consent is required to do so.

Communication is not an official approval, but a check to ensure the users and other parties affected by the change are comfortable with the changes before official approval from the IT Steering Committee is obtained.

6.1. Planning the Change

Once the users and other stakeholders have given their approval for the change, formal application to approve the change will be initiated. The first step is to plan the details of the change.

6.2. Change details to be considered

The following details must be considered when planning IT system changes:

6.2.1 The persons responsible for the change.
6.2.2 The effect the change will have on the business.

6.2.3 When the change will have the least chance of interfering with business operations.
6.2.4 The appropriate support staff that should be available.
6.2.5 If the change could be made within the standard maintenance window.
6.2.6 If enough time is available to review and test the proposed change.
6.2.7 What the risks are associated with the change.
6.2.8 What the risks are should the change not be implemented.
6.2.9 How the changes will be made.
6.2.10 If the change will result in any additional security issues or increase the risk to the system.
6.2.11 Back-out procedures in case the change was not implemented successfully.
6.2.12 Any additional training and documentation that will be necessary for both support staff and end-users.

6.3. Logging the Change

Once all the change details have been planned, the IT Committee will record the proposed changes according to all the appropriate fields and workflow ability to facilitate approval by an authorised person.

6.4. Change Control Committee review

6.4.1 The IT Steering Committee is responsible for the change control review of any change requests, and determines whether or not the proposed changes should be implemented.

6.4.2 The committee consists of the Information Technology Manager, the Operations Manager and the Chief Executive Officer. Other participants to the committee include any person who has applied for a change to be approved. The committee meets once a month on an agreed date and time.

6.4.3 The committee may determine that certain changes to the proposed plan for implementing the proposed change must be made in order for the plan to be acceptable. The committee will assess the impact of the change and consider the risk of implementing the change, and the risk of not undertaking the change.

6.4.4 The agenda resulting from the committee meeting consists of all the change requests that have been logged. All the changes must be reviewed for approval, and a decision must be made whether to approve, delay or decline the request.

6.4.5 All decisions and actions must be logged on the Da Vinci Change control system.

6.5. Executing the change

6.5.1 The relevant support staff should be available and prepared to assist in the change process.

6.5.2 If system availability will be affected while the change is being made, the affected individuals must be notified of what to expect, and when to expect it. The affected parties should be informed whom to contact should they experience any difficulty as a result of the change.

6.5.3 Support staff must verify that the change was implemented successfully and that the system is stable. If the change wasn't implemented successfully, it needs to be determined what can be done to rectify the problem, or initiate the back-out plan.

6.5.4 Support staff must provide documentation and instructions to users that will be affected by the change.

6.5.5 Support staff must record the change that was implemented in the Change Log Register.

6.6. Monitoring the change

Support staff has to monitor and ensure that there are no bugs or undesired consequences from the change, and that system stability is maintained.

6.7 MAINTENANCE WINDOW

The maintenance window is the defined period of time when maintenance such as software patching or upgrading hardware components can be performed. Clearly defining a regular maintenance window is key as it provides a time when users

should expect service disruptions. This will usually be a timeslot where there is minimal impact on users and operations.

6 CRITICAL OR EMERGENCY CHANGES (FAST-TRACKING THE PROCESS)

7.1 In some cases events are critical in that they must be rushed into production; as much consideration as possible must be given to the possible consequences of attempting the change.

7.2 Approval must still be obtained from the relevant business unit or department for these critical changes.

8. REVIEW OF POLICY

Regular review and amendments of this policy will be done in line with the approved institutional policies. This will take place in consultation with the relevant quality assurance structures at departmental and institutional level, under the auspices of the official custodians of this policy, namely the Executive: Operations.

9. REVISION HISTORY

Version No.	Amendment Details	Approval date	Approving Committee	Chairperson Signature
Version 1 (V1)	Various	01/04/2019	EXCO	
Version 2 (V2)	Amendments as per review tracking document: Amendment review	11/04/2024	The Board	