Change Management and Control Policy

For NimonikApp and Nimonik Audit for iOS and Android

Last Update: February 2021

Owner: ISMS IT Lead

Contents

1 Introduction

1.1.1.1 Operational change management brings discipline and quality control to IS. Attention to governance and formal policies and procedures will ensure its success. Adopting formalised governance and policies for operational change management delivers a more disciplined and efficient infrastructure. This formalisation requires communication; the documentation of important process workflows and personnel roles; and the alignment of automation tools, where appropriate. Where change management is nonexistent, it is incumbent on IS's senior management to provide the leadership and vision to jump-start the process. By defining processes and policies, IS organisations can demonstrate increased agility in responding predictably and reliably to new business demands.

1.1.1.2 Nimonik (hereafter called 'the company') management has recognised the importance of change management and control and the associated risks with ineffective change management and control and have therefore formulated this Change Management and Control Policy in order to address the opportunities and associated risks.

2 Scope

2.1.1.1 This policy applies to all changes to customer facing commercial products and currently includes:

2.1.1.1.1 NimonikApp.com

2.1.1.1.2 NimonikApp.com.cn

2.1.1.1.3 Customer specific instances of these products

2.1.1.1.4 Nimonik Audit for iOS (in Apple Store)

2.1.1.1.5 Nimonik Audit for Android (in Google Play Store)

3 Purpose

3.1.1.1 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:

- Interruption to services to customers
- Change of functionality that alters customer use of the products
- Information being corrupted and/or destroyed;
- Computer performance being disrupted and/or degraded;
- Productivity losses being incurred; and
- Exposure to reputational risk.

4 References and definitions

4.1 Normative references

4.1.1.1 The following documents contain provisions that, through reference in the text, constitute requirements of this policy. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this policy are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

- Nimonik Information Security Policy (overall)
- Information Security - Systems Development and Maintenance
- Information Security - Business Continuity Management
- Information Security - Physical Asset Classification and Control Policy

4.2 Definitions and abbreviations

4.2.1 Audit trail

4.2.1.1 A record or series of records which allows the processing carried out by a computer system to be accurately identified, as well as verifying the authenticity of such amendments.

4.2.2 Information resources

4.2.2.1 All data, information as well as the hardware, software, personnel and processes involved with the storage, processing and output of such information. This includes data networks, servers, PC's, storage media, supporting equipment, fall-back equipment and back-up media that are used in the creation, maintenance and changes to the products outlined in the Scope.

4.2.3 Abbreviations

- **PC:** Personal Computer
- **BCP:** Business Continuity Plan
- **SLA:** Service Level Agreement

5 Policy

5.1 Preamble

5.1.1.1 Changes to information resources shall be managed and executed according to a formal change control process where deemed ISMS In-scope. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

5.1.1.2 In order to fulfil this policy, the following statements shall be adhered to:

5.1.2 Operational Procedures

5.1.2.1 A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.

5.1.2.2 At a minimum the change control process should include the following phases:

- Logged Change Requests;
- Identification, prioritisation and initiation of change;
- Proper authorisation of change;
- Requirements analysis;
- Inter-dependency and compliance analysis;
- Impact Assessment;
- Change approach;
- Change testing;
- User acceptance testing and approval;
- Implementation and release planning;
- Documentation;
- Change monitoring;
- Defined responsibilities and authorities of all users and IT personnel;
- Emergency change classification parameters.

5.1.3 Documented Change

5.1.3.1 All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented.

5.1.3.2 No single person except the CIO should be able to effect changes to production information systems without the approval of other authorised personnel.

5.1.4 Risk Management

5.1.4.1 A risk assessment shall be performed for all changes and dependant on the outcome, an impact assessment should be performed.

5.1.4.2 The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

5.1.5 Change Classification

5.1.5.1 All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.

5.1.5.2 Nimonik releases an annual product development plan, that can be requested by any customer at any time.

5.1.5.3 Changes to Nimonik customer facing products are categorized as follows:

Level	Description	Examples	Customer Notification
1	Very substantial changes that will change the core functionality of the platform.	Removal of Incidents module with no replacement	Minimum 6 months
2	Significant changes to the products that will alter documented workflows, how-to guides, and support manuals. These changes will substantially change the way users interact with the software.	Removal of Scheduler module and replacement with Internal Documents	Minimum 2 month
3	Small changes to functionality that will affect the workflow and the way the platforms are to be used	Deployment of Internal Actions, Change of terminology on certain buttons	Minimum 2 Weeks
4	Bug fixes, security patches, upgrades to underlying software, and minor improvements to the web portal	Upgrade to MySQL, Change of drop down to multi-select, Addition of new options on a report, etc.	None - Change. Release notes on Nimonik.com

5.1.6 Testing

5.1.6.1 Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

5.1.6.2 Changes are then published to the Staging environments. Upon receipt of a notification that a change is upcoming on the Nimonik platform, customers can request to test a level 1 or 2 Change and validate it is acceptable.

5.1.7 Changes affecting SLA's

5.1.7.1 The impact of change on existing SLA's shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

5.1.8 Version control

5.1.8.1 Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.

5.1.9 Approval

5.1.9.1 All changes shall be approved by Nimonik Product Management prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.

5.1.10 Communicating changes

5.1.10.1 All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change. See section 5.1.3 Change Classification

5.1.11 Implementation

5.1.11.1 Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Level 1 changes will be classified according to effort required to develop and implement said changes.

5.1.12 Fall back

5.1.12.1 Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

5.1.13 Documentation

5.1.13.1 Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.

5.1.13.2 Information resources documentation is used for reference purposes in various scenarios i.e. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer and/or development house being unavailable. It is therefore imperative that information resources documentation is complete, accurate and kept up to date with the latest changes. Policies and procedures, affected by software changes, shall be updated on completion of each change.

5.1.14 Business Continuity Plans (BCP)

5.1.14.1 Business continuity plans shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness, accuracy and availability of BCP documentation. BCP documentation is the road map used to minimise disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of disasters.

5.1.15 Emergency Changes

5.1.15.1 Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.

5.1.16 Change Monitoring

5.1.16.1 All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

6 Roles and Responsibilities

ROLE	FUNCTIONAL RESPONSIBILITIES
See ISMS Roles and Responsibilities	● As defined

7 Compliance

7.1.1.1 Any person, subject to this policy, who fails to comply with the provisions as set out above or any amendment thereto, shall be subjected to appropriate disciplinary action

8 IT Governance Value statement

8.1.1.1 Changes that materially affect the financial process may be evaluated.

9 Policy Access Considerations

9.1.1.1 Access to this policy shall be granted to:

- All ISMS affected IT personnel
- Interested stakeholders such as customers and partners