Catholic Diocese of Columbus
Change Management and Control Policy

Catholic Diocese of Columbus
Office of Information Technology
Steven Nasdeo, Director

Contents

1 Introduction 4
2 Scope 4
3 Purpose 4
4 References and definitions 5
4.1 Normative references 5
4.2 Definitions and abbreviations 5
4.2.1 Audit trail 5
4.2.2 Information resources 5
4.2.3 Abbreviations 5
5 Policy 6
5.1 Preamble 6
5.1.2 Operational Procedures 6
5.1.3 Documented Change 6
5.1.4 Risk Management 7
5.1.5 Change Classification 7
5.1.6 Testing 7
5.1.7 Changes affecting SLA‘s 7
5.1.8 Version control 7
5.1.9 Approval 7
5.1.10 Communicating changes 7
5.1.11 Implementation 8
5.1.12 Fall back 8
5.1.13 Documentation 8
5.1.14 Business Continuity Plans (BCP) 8
5.1.15 Emergency Changes 8
5.1.16 Change Monitoring 8
6 Roles and Responsibilities 9
7 Compliance 11
8 IT Governance Value statement 11
9 Policy Access Considerations 11

1 Introduction

Operational change management brings discipline and quality control to Information Technology. Attention to governance and formal policies and procedures will ensure its success. Adopting formalized 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 IT's management to provide the leadership and vision to jump-start the process. By defining processes and policies, IT organizations can demonstrate increased agility in responding predictably and reliably to new business demands.

1.1.1.1 Office of Information Technology (hereafter called 'the IT Department') 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 to address the opportunities and associated risks.

2 Scope

2.1.1.1 This policy applies to all parties operating within the Catholic Diocese of Columbus' network environment or utilizing Information Resources. It covers the data networks, LAN servers and personal computers (stand-alone or network-enabled), located at diocesan offices, where these systems are under the jurisdiction and/or ownership of the diocese, and any personal computers, laptops, mobile device and or servers authorised to access diocesan data networks. No employee is exempt from this policy.

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:

- Information being corrupted and/or destroyed
- Computer performance being disrupted and/or degraded
- Productivity losses being incurred
- 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.

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

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, printer, photo copiers, fax machines, supporting equipment, fall-back equipment and back-up media.

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. 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.

1. In order to fulfil this policy, the following statements shall be adhered to:
2. All changes must follow these procedures
3. All non-emergency changes will have prior approval before going into production
4. All emergency changes will have the change request form submitted after the change is completed and the environment is back online

5.1.2 Operational Procedures

5.1.2.1 The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical diocesan 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, prioritization and initiation of change;
- Proper authorization 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, in the Application Change Request system, accessed on the Diocesan Intranet SharePoint Home page. The approval of all change requests and the results thereof shall be documented.

5.1.3.2 A documented audit trail, maintained within SharePoint, containing relevant information shall always be maintained. This should include change request documentation, change authorization and the outcome of the change. No single person 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.

5.1.6 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 minimize 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.

5.1.7 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 diocesan retention and storage management policies.

5.1.9 Approval

5.1.9.1 All changes shall be approved 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.

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. Major 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 diocesan 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, authorization, 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
Members of the IT Steering Committee (ITSC)	• Members of the ITSC shall ensure that the necessary information security controls are implemented and complied with as per this policy. • Members of the ITSC will have final approval for all change requests.
Director, Office of Information Technology	• Establish and revise the information security strategy, policy and standards for change management and control with input from interest groups and subsidiaries; • Facilitate and co-ordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards; • Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products; • Co-ordinate the overall communication and awareness strategy for change management; • Acts as the management champion for change management and control; • Provide technical input to the service requirements and co-ordinate affected changes to SLA's where applicable. • Establish and co-ordinate appropriate interest group forums to represent, feedback, implement and monitor change management and control initiatives; and • Co-ordinate the implementation of new or additional security controls for change management. • Implement, maintain and update the change management and control strategy, baselines, standards, policies and procedures with input from all stakeholders; • Approve and authorize change management and control measures on behalf of the Catholic Diocese of Columbus; • Ensure that all application owners are aware of the applicable policies, standards, procedures and guidelines for change management and control; • Ensure that policy, standards and procedural changes are communicated to applicable owners and management forums; • Appoint the necessary representation to the interest groups and other forums created by each company for Information Security Management relating to change management and control;

	• Establish and revise the information security strategy, policy and standards for change management and control
	• Facilitate and co-ordinate the necessary change management and control initiatives within each company; • Report and evaluate changes to change management and control policies and standards; • Co-ordinate the overall communication and awareness strategy for change management and control; • Co-ordinate the implementation of new or additional security controls for change management and control • Review the effectiveness of change management and control strategy and implement remedial controls where deficits are identified; • Provide regular updates on change management and control initiatives and the suitable application; • Evaluate and recommend changes to change management/ version control solutions; and • Co-ordinate awareness strategies and rollouts to effectively communicate change management and control mitigation solutions in each company. • Establish and implement the necessary standards and procedures that conform to the Information Security policy; • Responsible for approving, authorizing, monitoring and enforcing change management initiatives and related security controls within all Catholic Diocese of Columbus departments and agencies. • Ensure that all solution owners are aware of policies, standards, procedures and guidelines for change management and control. • Ensure the compliance of this policy and report deviations to the Information Manager.
IT Staff	• Shall comply with all change management and control statements of this policy.
Solution Owners	• Shall comply with all information security policies, standards and procedures for change management and control; and • Report all deviations.

Table 1 Roles and Responsibilities

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 or legal action in accordance with the Office of Human Resources policy in effect for Information Technology. Diocesan Information Security policies, standards, procedures and guidelines shall comply with legal, regulatory and statutory requirements.

8 IT Governance Value statement

8.1.1.1 Changes that materially affect the financial process must be evaluated and reported quarterly. Financial system upgrades or replacements will require new certification. The implication is that Sarbanes-Oxley compliance is reliant on the changes you make to the operational systems and procedures.

9 Policy Access Considerations

9.1.1.1 Access to this policy shall be granted to:

- All IT personnel
- Members of the ITSC
- All Directors and Associate Directors