# Change Management Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of this policy is to define a consistent approach to manage changes to the IT environment at [Insert Company Name].

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

According to the ITIL Service Management framework: “change management is responsible for managing change processes involving:

* Hardware
* Communications equipment and software
* System software
* Live applications software
* All documentation and procedures associated with the running, support, and maintenance of live systems.”

This policy is consistent with ITIL and covers all changes to **existing** IT applications within the enterprise. Excluded from the scope of this policy are changes to applications that **are in the process of being implemented.** These changes are controlled by the change control process established for the particular project that is underway.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Responsibilities** | **Implementation Considerations** | **Contact Information** |
| Change initiator or requestor | Business or IT representative who initiates a request for change. This person is responsible for filling out the Request for Change (RFC) form, getting approval for the change, and submitting it according to the change management process. For more information, refer to the Info-Tech research note, [*Request for Change Form*](http://www.infotech.com/research/request-for-change-form)*.* |  | Can be anybody in the enterprise. |
| Change Manager (also called Change Management Specialist) | This person has overall management responsibility for the change management process in the IT department. For a detailed list of the skills and responsibilities of this role, refer to the Info-Tech job description, *Change Management Specialist.* | **Small and Mid-sized Enterprises (SMEs)** don’t need a full-time person dedicated to this role. They can assign this part-time function to an existing business systems analyst, to the help desk leader, or to another key support person in the team.  **Large companies** need a full-time person dedicated to this role. Given the size and volume of change requests in large enterprises, the change manager is usually supported by another role called the RFC coordinator. These coordinators are responsible for screening, filtering, and logging change requests for one application or a family of applications (e.g. one RFC coordinator for all financial systems). The RFC coordinator is a part-time role assigned to people who have expertise in the application and its processes. The best suited people for this role are in the business systems. | List here the name of the change manager and RFC Coordinators. |
| Role | Responsibilities | Implementation Considerations | Contact Information |
| Change Advisory Board (CAB) | The CAB is a cross-functional team responsible for assessing change requests in terms of business need, cost/benefit, viability, and potential impacts to existing systems or processes. The CAB decides whether to approve, defer, return, reject, or cancel changes and assigns a priority. Also, the CAB makes recommendations related to change implementation. | Typical people who are part of the CAB include:   * Change manager * One representative for each business department. This person must be able to represent his/her department and must be empowered to make decisions on behalf of his/her department. * IT Operations Manager * IT Infrastructure Manager * IT Applications/Development Manager * Contractor or third-party representatives if required | List here the CAB members. |
| Change Advisory Board/ Emergency Committee (CAB/EC) | This team (or individual) is a subset of the CAB that is responsible for dealing with emergency changes. The CAB/EC must be able to meet on a very short notice and authorize or reject changes with emergency priority. | The people must be able to meet at any time to make emergency decisions. Recommended members include:   * Change manager * One representative for each business department (only one will be consulted, depending on the scope of the change). * IT Operations manager | List here the respective CAB/EC members. |
| IT Operations Manager (also called IT Service Manager) | Approves or rejects the introduction of changes into the production environments. |  | List here the name of the IT Operations Manager. |
| IT Infrastructure Manager | The IT Infrastructure manager is usually a member of the CAB. They review RFCs and assess the potential impact that the request may have on existing infrastructure. The IT Infrastructure manager will make decisions and allocate resources from their team as required. |  | List here the name of the IT Infrastructure Manager. |
| Role | Responsibilities | Implementation Considerations | Contact Information |
| IT Applications/  Development Manager | The IT Applications/Development manager is usually a member of the CAB. They review RFCs and assess the potential impact that the request may have on existing applications. The IT Applications/Development manager will make decisions and allocate resources from their team as required. |  | List here the name of the IT Applications/ Development Manager. |

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

Each change request will follow these steps:

1. **Change request creation.** Therequestor fills out a [Request for Change Form](http://www.infotech.com/research/request-for-change-form) to document the change request and submits it to the change manager. The change manager supports the requestor during this step by resolving questions about how to use the RFC form.
2. **Change assessment.** The change manager receives the RFC and reviews it for completeness. If some important information is missing, the change manager returns the RFC to the requestor. Once the RFC is properly documented, the change manager performs an initial assessment of the RFC, and negotiates with the requestor an initial priority for the request. This initial priority can later be changed by the CAB. Possible priorities include:

|  |  |
| --- | --- |
| **Priority** | **Explanation** |
| Immediate | Requests that, if not addressed immediately, will create a large risk to the enterprise. Immediate action is required. The CAB/EC must be convened and resources may need to be allocated immediately if the request is authorized. |
| High | A request that is important for the enterprise and should be implemented soon, but not immediately. |
| Medium | A request that should be implemented to gain benefits, but is not time pressing. |
| Low | A request that is nice to have. |

As part of this step, the change manager also assesses the impact of the RFC and categorizes it. Possible categories include:

|  |  |
| --- | --- |
| **Impact Category** | **Explanation** |
| Major | A change that impacts a massive group of users or a mission-critical system (e.g. change to the inventory module of the ERP system). The change involves downtime of a system or service. |
| Significant | A change that affects a high percentage of users (e.g. a change affecting a group within a department or a specific group of users). The change may involve downtime of an important system or service. |
| Minor | A change that impacts a non-critical system and a small number of users (e.g. change to a non-critical application used by a small team). |

1. **Change authorization and prioritization.** At this point, the organization needs to determine a course of action for the RFC (i.e. change priority, approve, reject, or defer).Who makes this decision **depends upon the priority and the impact category** of the change:

* If the RFC has immediate (urgent) priority, the change manager must escalate it as soon as possible to the CAB/EC for urgent evaluation (see the roles and responsibilities section for a list of CAB/EC members).
* If the RFC is categorized as minor, the change manager can evaluate and decide himself/herself without involving anyone else.
* All other RFCs must be addressed by the CAB during its monthly meeting.

Once decisions are made, the change manager is responsible for updating the [Change Master Log](http://www.infotech.com/research/change-master-log-template) and for communicating the decision to the initial requestor.

If the RFC is approved, the CAB needs to decide when the RFC will be developed and when it will be implemented in production. Business units are usually competing for scarce IT resources. As a result, getting consensus about which requests will be developed first is challenging. The best way to make this decision is to establish a rating/voting system based on an agreed upon set of criteria. An example of criteria is:

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteria** | **Weight** | **Description** | **Values** |
| Assigned Priority | 40% | How critical are the business needs that this change aims to meet? | 3 = High 2 = Medium 1 = Low |
| Tangible Benefits | 40% | Does this change lead to cost reductions, time reductions, or sales increases? | 3 = Clear and measurable returns 2 = Time reductions 1 = Returns unclear, difficult to measure |
| Effort | 20% | What is the level of effort to implement this change? | 3 = Little effort, less than 1 week 2 = Medium effort, 1-4 weeks 1 = Large effort, over 4 weeks |

1. **Change development.** In this step, theRFCenters the development phase. The IT management team (applications or/and infrastructure) assigns resources to develop the change.
2. **Change implementation (according to ITIL, the accountability for this step resides with the release management function).** Once the change is developed and tested, the change manager will work with the IT Operations manager and the user community to schedule the implementation. All of the following activities must be completed before introducing a change in production:

* Technical tests performed and signed off (e.g. Component integration test (CIT), system acceptance test (SAT)).
* User acceptance test (UAT) completed and signed off.
* IT Operations manager has approved the implementation of the change in the production environment.
* Business owner(s) of the system has/have approved the implementation of the change in the production environment.
* End-user training completed.
* Support personnel training completed.
* Service level agreements (SLA) have been properly modified if necessary.
* End-user and technical documentation have been properly modified if necessary.
* Assessment of impact on business continuity and contingency plans.

Once an implementation date and time has been determined, the change manager must update the [Forward Schedule of Changes](http://www.infotech.com/research/forward-schedule-of-changes-template) (FSC) and communicate it to the enterprise (e.g. post it on the Intranet).

1. **Post-implementation review.** The change manager will perform a post-implementation review one month after the change implementation. This review will evaluate the following aspects of the change:

* Did the change meet its objectives?
* Are users satisfied with the results?
* Has the change created any unexpected side-effects to existing applications or infrastructure?
* Did the implementation plan work correctly? Was the implementation completed on time and within budget?
* If the back-out plan was utilized, did it work correctly?
* What are the lessons learned from this implementation?

Upon completion of the review, the change manager will document findings and report back to the CAB if required.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.