**Roles and**

**Responsibilities in ISO 27001**

Version:

Date:

Classification

Document Control

|  |  |  |
| --- | --- | --- |
| 1. | Document Title: |  |
| 2. | Date of Release: |  |
| 3. | Documents superseded: |  |
| 4. | Version No.: |  |
| 5. | Document Owner: |  |
| 6. | Document Author(s): |  |

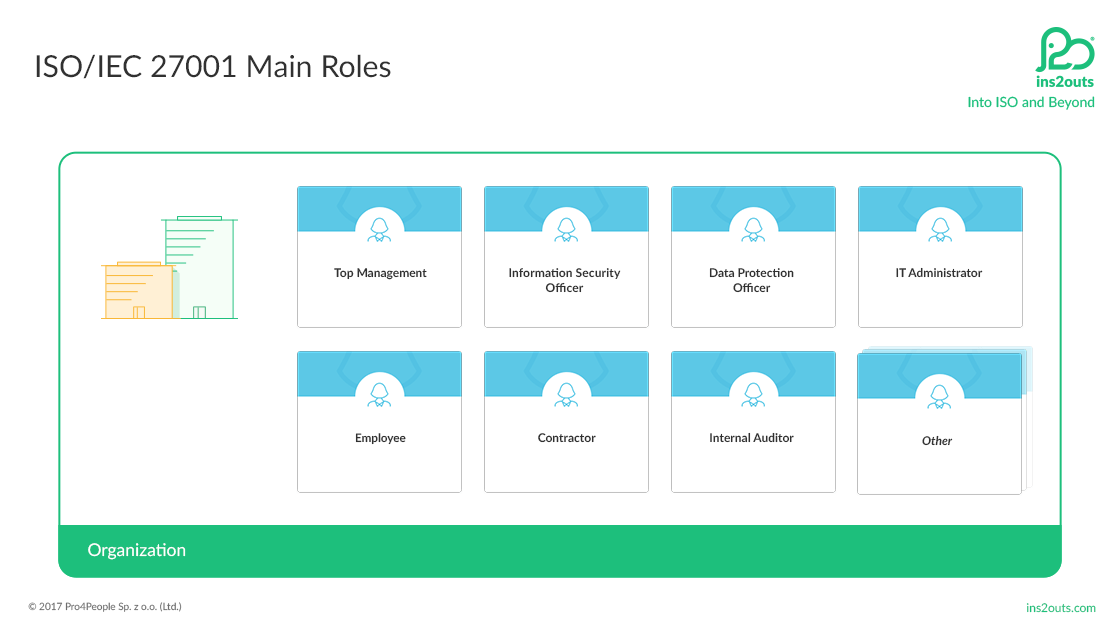
Document Approvers

|  |  |  |  |
| --- | --- | --- | --- |
| S. No. | Approver | Approved Through Nominee | Nominee Contact |
|  |  |  |  |

Document Change Approvals

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Section / Page No. | Description of Amendment | Reason for Amendment | New Version No. and Effective Date | Amendment done by | Approved by |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Purpose

\_\_\_**organization name**\_ has developed and implemented an information security management system in accordance with the requirements of the international standard ISO 27001. This document outlines the list of teams and their responsibilities for effective implementation of the ISMS.

## Top Management

* Defining organizational strategy.
* Defining the purpose of the ISMS.
* Define the scope to be covered by the ISMS
* Demonstrate leadership in implementing information security management systems
* Define organizational strategy, taking into account data protection mechanisms and available policies.
* Define required roles and assign responsibilities to available roles.
* Providing necessary resources.
* Budget determination and budget approval.
* Active participation in management review and improvement processes for ISMS

## Information Security Officer

* Define and monitor your ISMS.
* Coordination of activities related to ISMS.
* Contact authorities and interested parties in the ISMS.
* Provide coordination of the entire ISMS process.

**Data Protection Officer**

* Full definition of ISO 27001 roles and their assigned responsibilities and scope.
* You have the right to assign individuals to available roles.
* Provide individuals with the necessary training relevant to their assigned roles.
* Notify users when they need to be notified of content in spaces that a particular person is responsible for.
* Provide long-term, role-specific proficiency profiles.

**IT Administrators**

* Defining required security measures.
* Implementation of necessary security measures.
* Actively participate in the risk analysis process as a subject matter expert.
* Maintaining available IT resources.
* Management of IT system availability.
* Respond to security threats and incidents targeting your organization.
* Always strive to increase cyber security awareness among your employees.

**Employees/Contractors**

* You must comply with the rules and regulations available in your organization.
* You must work in accordance with your organization's awareness training.
* You must abide by and comply with policies such as:

1. Information Security Policy

2. Information Classification Policy

3. Acceptable Uses of Asset Policy

4. Network and Network Service Access Policy

5. Password Management Policy

## Internal Auditor

* Actively participate in exams and exam administration processes.
* Create audit reports and documents.
* Distribution of test reports and documentation.
* Developing review criteria to improve the quality of the review process.
* Developing and improving management systems within the organization.