**Roles and**

**Responsibilities in ISO 27001**

## Purpose

By the criteria of ISO 27001, Optimized Solution created and put into place an information security management system. The list of teams and their duties for carrying out the ISMS are described in this paper.

## Top Management

* Outlining a business plan.
* Outlining ISMS's objectives.
* Outlining the area that ISMS should cover
* Exercise leadership in putting the Information Security Management System into place.
* Defining the organization's strategy while taking into account the policies and data protection measures in place.
* Outlining the necessary positions and determining the tasks for the open roles.
* Supplying necessary resources.
* defining the budget and approving the budget.
* Participating actively in ISMS management reviews and improvement processes

## Information Security Officer

* Defining and offering ISMS supervision.
* Coordinating actions associated with ISMS.
* Contact the relevant authorities and parties to express your interest in ISMS.
* Coordinate every step of the ISMS procedure.

## Data Protection Officer

* y outlining the jobs under ISO 27001, including their tasks and areas of responsibility.
* Possess the authority to appoint people to open positions.
* Give the people the training they need about the roles that have been given to them.
* When it's necessary to let users know that a certain person is in charge of a particular area of material, do so.
* Long-term competence profiles for a particular role.

## IT Administrator

* Outlining the necessary security precautions.
* Putting the necessary security measures into place.
* Participate actively as a technical expert in the risk analysis process.
* Maintaining the IT resources that are accessible.
* coordinating IT system availability.
* React to security issues and threats that are directed at the company.
* Always work to raise employees' awareness of cyber security.

## Employee/Contractor

## Must abide by all policies and guidelines set forth by the organization.

## Work through the organization's awareness training.

## Should abide by and follow rules like.

## Information Security Policy

## Policy for Information Classification

## Asset Acceptable Use Policy

## Network and Service Policy for Access

## The Policy on Password Management

## Internal Auditor

* Participate actively in audits and management procedures.
* Creating documentation and audit reports.
* distributing audit paperwork and reports.
* Creating an audit criterion to raise the standard of the auditing procedure.
* Creating and enhancing management systems inside the company.