

<b>Demo Company Limited</b>		
<b>Organisation of Information Security</b>		
<b>ISO/IEC 27001:2013</b>		
<b>Issue 1</b>	<b>A.6.1.1 Information security roles and responsibilities</b> <b>A.6.1.2 Segregation of duties</b> <b>A.6.1.3 Contact with authorities.</b> <b>A.6.1.4 Contact with special interest groups</b> <b>A.6.1.5 Information security in project management</b>	<b>Authorised By:- Directors of Demo Company Ltd.</b>
<b>Page 1 of 3</b>	<b>Effective Date: 1<sup>st</sup> Nov 2021</b>	<b>Classification:- Internal</b>
<b>Issue Date: 1<sup>st</sup> Nov 2021</b>		<b>Last Review Date: 1<sup>st</sup> Nov 2021</b>

### Scope

This controlled process defines Information security roles and responsibilities, segregation of duties, contact with authorities and special interest groups and Information security in project management.

### Responsibility and Authority

The appointed information security representatives are responsible for the overall management of this process including its correct implementation and regular review.

### Control and Distribution

This process is issued as a controlled document and can only be updated by the authorised information management representative and must include a revision status and traceability of the change process.

A master is retained as part of the information security management system with uncontrolled copies issued at point of use.

### The Process

#### A.6.1.1 Information security roles and responsibilities

The organisational structure details the different levels of roles within the company. Duties and responsibilities are determined within individual job descriptions. Responsibilities include the protection of individual assets and carrying out specific information security duties. Responsibilities include the acceptance of residual risk, where applicable. Authorisation levels are redefined and documented in the **organisation chart**.

Individuals with allocated information security responsibilities remain accountable for delegated tasks. Details of responsibilities are documented as part of ownership of assets as documented in assets management section 8.1.2.



<b>Demo Company Limited</b>		
<b>Organisation of Information Security</b>		
<b>ISO/IEC 27001:2013</b>		
<b>Issue 1</b>	<b>A.6.1.1 Information security roles and responsibilities</b> <b>A.6.1.2 Segregation of duties</b> <b>A.6.1.3 Contact with authorities.</b> <b>A.6.1.4 Contact with special interest groups</b> <b>A.6.1.5 Information security in project management</b>	<b>Authorised By:- Directors of Demo Company Ltd.</b>
<b>Page 3 of 3</b>	<b>Effective Date: 1<sup>st</sup> Nov 2021</b>	<b>Classification:- Internal</b>
<b>Issue Date: 1<sup>st</sup> Nov 2021</b>		<b>Last Review Date: 1<sup>st</sup> Nov 2021</b>

#### **A.6.1.4 Contact with special interest groups**

Special interest groups are detailed within the table above and include membership of forums and or professional associations to ensure appointed persons are up to date with current issues and solutions.

#### **A.6.1.5 Information security in project management**

Project management is the responsibility of xxxxxxxxxxxxxxxx who ensures that risk assessments are carried out as part of the initial planning to process including assessment of potential information security issues. This process should also be addressed following the documented operations security change management detailed in section 12.1.2.

This is documented within the **project management plan** and authorised prior to project implementation.