# INFORMATION SECURITY MANAGEMENT PROCESS

<table>
<thead>
<tr>
<th>Code:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
<td></td>
</tr>
<tr>
<td>Date of version:</td>
<td></td>
</tr>
<tr>
<td>Created by:</td>
<td></td>
</tr>
<tr>
<td>Approved by:</td>
<td></td>
</tr>
<tr>
<td>Confidentiality level:</td>
<td></td>
</tr>
</tbody>
</table>

**Comment [BV1]:** All fields in this document marked by square brackets [ ] must be filled in.

**Comment [BV2]:** The document coding system should be in line with the organization’s existing system for document coding; in case such a system is not in place, this line may be deleted.

©2013 This template may be used by clients of EPPS Ltd. www.20000academy.com in accordance with the License Agreement.
Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Created by</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>xx/xx/2013</td>
<td>0.1</td>
<td>Branimir Valentic</td>
<td>Basic document template</td>
</tr>
</tbody>
</table>

Table of contents

1. PURPOSE, SCOPE AND USERS................................................................. 3
2. REFERENCE DOCUMENTS ........................................................................... 3
3. PROCESS .................................................................................................. 3
4. ROLES AND RESPONSIBILITIES................................................................... 4
   4.1. INFORMATION SECURITY MANAGER..................................................... 4
5. MEASUREMENT AND METRICS ................................................................. 4
   5.1. MEASUREMENT .................................................................................. 4
   5.2. METRICS ......................................................................................... 4
   5.3. CRITICAL SUCCESS FACTORS (CSF) AND KEY PERFORMANCE INDICATORS (KPI) .......................................................... 5
6. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT.................. 5
7. VALIDITY AND DOCUMENT MANAGEMENT............................................. 5
1. Purpose, scope and users

The aim of this document is to define the purpose, scope, principles and activities of the Information Security Management process.

This document is applied to the entire IT Service Management (ITSM) organization.

Users of this document are all employees of [organization name], as well as all external parties who have a role in ITSM.

2. Reference documents

- Incident Management Policy
- Information Security Policy
- ISO/IEC 20000-1:2011 clause 6.6

3. Process

Figure: Information Security Management process activities

Comment [BV3]: ***OPTION***
Replace this with "SMS" if you are implementing ISO 20000.

Comment [BV4]: ***OPTION***
Replace this with "SMS" if you are implementing ISO 20000.

Comment [BV5]: ***OPTION***
Delete this if you are implementing ITIL but not ISO 20000.

Comment [BV6]: Double-click to edit figure and adapt to your own requirements.
Activities of Information Security Management are described in the Information Security Policy. [role description] is responsible to establish and maintain Information Security and make it available to all employees and external suppliers.

4. Roles and responsibilities

4.1. Information Security Manager

Responsibilities of Information Security Manager:
- Overall responsibility for carrying out activities within the scope of the Information Security Management process
- Coordinates with other Service Management roles
- Responsible for reporting and managing information
- Develops and maintains Information Security Policy
- Communicates Information Security Policy
- Develops and documents procedures for operating and maintaining security controls (see Information Security Policy)
- Monitors and manages all security breaches
- Raises awareness, promotes and educates on the topic of information security
- Serves as a focal point for all security issues

5. Measurement and metrics

5.1. Measurement

[role description] is responsible to produce reports.

Reports are sent to the Service Level Manager on a monthly basis.

[role description] is responsible that:
- reports are produced monthly, with quarterly and yearly summaries
- reports are evaluated
- measures for improvement are defined

5.2. Metrics

Metrics reports are produced monthly, with quarterly and yearly summaries. Metrics to be reported:
- Number of security incidents

Comment [BV7]: **OPTION**
Delete this figure if you are implementing ISO 20000 and not ITIL.

Comment [BV8]: Adapt to your own requirement.

Comment [BV9]: Or similar role. Change if needed.

Comment [BV10]:

Comment [BV11]: Example:
Information Security Manager, Continual Service Improvement Manager.

Comment [BV12]: These are usual metrics, change as required.

Comment [BV13]: Final list depends on tool’s possibilities, i.e. requirements.
5.3. Critical Success Factors (CSF) and Key Performance Indicators (KPI)

[role description] is responsible to define CSFs and respective KPIs. Achievements against KPIs are monitored and evaluated by [role description].

<table>
<thead>
<tr>
<th>Critical Success Factor</th>
<th>Key Performance Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>High level of security awareness among end users</td>
<td>Number of security incidents</td>
</tr>
</tbody>
</table>

6. Managing records kept on the basis of this document

<table>
<thead>
<tr>
<th>Record name</th>
<th>Storage location</th>
<th>Person responsible for storage</th>
<th>Controls for record protection</th>
<th>Retention time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Policy</td>
<td>[enter location]</td>
<td>[Information Security Manager]</td>
<td>IT Security Manager</td>
<td>Policy is updated; old version is archived</td>
</tr>
<tr>
<td>Reports</td>
<td>[tool name]</td>
<td>[Change Manager]</td>
<td>Information Security Manager</td>
<td>Reports are kept for [...]</td>
</tr>
</tbody>
</table>

7. Validity and document management

This document is valid as of [date].

Owner of this document is [role description], who must check and, if necessary, update the document at least once a year.