**INFORMATION SECURITY POLICY**

<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.
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. DEFINITIONS ...................................................................................................................................... 3
4. OBJECTIVE .......................................................................................................................................... 3
   4.1 INFORMATION SECURITY POLICY .................................................................................................... 3
   4.2 INFORMATION SECURITY REQUIREMENTS ......................................................................................... 4
   4.3 RISK MANAGEMENT .................................................................................................................... 4
   4.4 INFORMATION SECURITY CONTROLS .............................................................................................. 4
   4.5 INTERNAL AUDIT .......................................................................................................................... 5
   4.6 POLICY COMMUNICATION ............................................................................................................ 5
   4.7 SECURITY INCIDENT MANAGEMENT ............................................................................................... 5
5. VALIDITY AND DOCUMENT MANAGEMENT ........................................................................................ 5
1. Purpose, scope and users

The aim of this document is to define the purpose, direction, principles and basic rules for information security.

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

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

- Information Security Management Process
- IT Service Continuity Management Process
- Incident Management Process
- Change Management Process
- ISO 20000-1:2011 clause 6.6

3. Definitions

Confidentiality – characteristic of the information by which it is available only to authorized persons or systems.

Integrity – characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.

Availability – characteristic of the information by which it can be accessed by authorized persons when it is needed.

Information security – preservation of confidentiality, integrity, and availability of information.

Information Security Management System – part of overall management processes that takes care of planning, implementing, maintaining, reviewing, and improving the information security.

4. Objective

The objective of Information Security Management is to provide confidentiality, integrity and availability of information assets, organization’s assets and services.

[role description] is responsible to review existing goals for Information Security Management and set new ones.

4.1 Information Security Policy
The Information Security Policy is a guideline which provides rules for use and misuse of [organization name]'s information security.

[role description] authorizes the [Information Security Policy]

[organization name] uses the following specific policies:

4.2 Information security requirements

Information security activities comply with the following legal and regulatory requirements relevant to the organization in the field of information security, as well as with contractual obligations.

- List of service requirements:
  - [list]
- List of company and regulatory requirements
  - [list]
- List of contractual obligations:
  - [list]

Legal and regulatory requirements and contractual obligations relevant to the organization in the field of information security that are not addressed in the Service Level Requirements are listed in the Service Level Requirements; see Service Level Requirements in Appendix of Service Level Management Process.

4.3 Risk Management

[role description] is responsible to identify information security risks and to prepare Risk Assessment and Treatment Plan (see Risk Assessment and Treatment Plan in Appendix of IT Service Continuity Management Process). Risk level is calculated according to security risk assessment is conducted once a year.

Risk acceptance criteria - Values 1 and 2 indicate acceptable risks, while values 3 and 4 indicate unacceptable risks. Unacceptable risks must be treated. Treatment measures are entered in the Risk Assessment and Treatment Plan (see Risk Assessment and Treatment Plan in Appendix of IT Service Continuity Management Process).

4.4 Information security controls

[organization name] has implemented and operates physical, administrative and technical information security controls. [role description] is responsible for ensuring that:

- Security controls are identified and documented – see Risk Assessment and Treatment Plan in Appendix of IT Service Continuity Management Process
- Security controls contain risk description which controls relate
- Security controls contain description of operation and maintenance
Effectiveness of controls

The Internal Audit Report (see Internal Audit Report in Appendix) contains necessary actions.

The Communication Procedure is defined in document “Communication Procedure.”

[role description] is responsible to:

- [organization name] information or services
- document, agree and implement information security controls with these external organizations.

4.5 Internal Audit

An internal [once a year] – see Annual Internal Audit in Internal Audit. [role description] appoints an auditor.

[role description] ensures the results of the audit are used in the Internal Audit Report (see Annual Internal Audit Report in Internal Audit). [Continual Service Improvement Manager] reviews the audit results and defines opportunity for improvement (see Service Improvement Plan Appendix of the Continual Service Improvement Process).

[Information Security Manager] is responsible to follow and manage resolution of internal audit findings; see Corrective and Preventive Action Form in Corrective and Preventive Action and see Annual Internal Audit Report in Internal Audit.

4.6 Policy communication

[role description] has to ensure that all employees of [organization name], as well as appropriate external parties, are familiar with this policy and the importance of conforming to the policy.

Communication procedure is defined in document Communication Procedure.

4.7 Security incident management

Security [role description] is defined by the incident Management process. Information security incidents are prioritized as [...]. [role description] defines priorities for information security incidents and communicates them to [Incident Manager].

[role description] analyzes

Information security incidents are reviewed and improvement identified by [Information Security Manager].

5. Validity and document management

This document is valid as of [date].
Owner of this document is [job title], who must update and [frequency] at least once a year.

[Top management] approves this policy.

[job title]

[name]

[signature]

Comment [BV22]: Appropriate role in top management.
Comment [BV23]: This is only a recommendation; adjust frequency as appropriate.
Comment [BV24]: Only necessary if the Procedure for Document Control prescribes that paper documents must be signed.

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