# ACCESS 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.
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 ................................................................. 4
2. REFERENCE DOCUMENTS .................................................................................. 4
3. POLICY .............................................................................................................. 4
   3.1 DEFINITIONS .............................................................................................. 4
   3.2 SCOPE OF WORK .......................................................................................... 4
   3.3 LOGGING AND TRACKING .............................................................................. 4
   3.4 ACCESS HANDLING ....................................................................................... 5
   3.5 MEASUREMENT ............................................................................................ 5
4. PROCESS ............................................................................................................ 6
   4.1 RECEIVE REQUEST ....................................................................................... 7
   4.2 VERIFICATION .............................................................................................. 7
   4.3 PROVIDE RIGHTS .......................................................................................... 7
   4.4 CHECK AND MONITOR IDENTITY STATUS ......................................................... 7
   4.5 LOG AND TRACK ACCESS .............................................................................. 7
   4.6 REMOVE OR RESTRICT RIGHTS ..................................................................... 8
5. ROLES AND RESPONSIBILITIES ......................................................................... 8
   5.1 ACCESS MANAGER ....................................................................................... 8
   5.2 SERVICE DESK STAFF .................................................................................. 8
   5.3 TECHNICAL OPERATOR AND APPLICATION ANALYST/ARCHITECT .................... 8
   5.4 IT OPERATOR ................................................................................................. 8
6. MEASUREMENT AND METRICS ........................................................................... 8
   6.1 MEASUREMENT ............................................................................................. 8
   6.2 METRICS ...................................................................................................... 9
6.3. CRITICAL SUCCESS FACTORS (CSF) AND KEY PERFORMANCE INDICATORS (KPI) .................................................. 9
7. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT ........................................................................... 9
8. VALIDITY AND DOCUMENT MANAGEMENT ....................................................................................................... 10
9. APPENDICES .......................................................................................................................................................... 10
1. Purpose, scope and users

The aim of this document is to define the purpose, scope, principles and activities of the Access 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

- Information Security Process
- Information Security Policy
- Incident Management Process
- Change Management Process
- IT Operations Function
- Technical Management Function
- Applications Management Function
- Service Desk Function
- Service Catalogue Management Process

3. Policy

Access Management is the process that grants authorized users’ rights to use a service while preventing access to non-authorized users. Access Management includes information security policies and actions.

**Access Management activities are performed by Technical and Application Management functions.**

A list of services that users can access are documented in Service Catalogue Management Process.

3.1 Definitions

Configuration Item (CI) - CIs are service assets that need to be managed in order to deliver IT services.

3.2 Scope of work


3.3 Logging and Tracking
While carrying out Access Management activities, accesses are logged and tracked using [...]. Logs need to be kept as described in the basis of this document “Managing records kept on the basis of this document" for auditing, compliance or forensic purposes.

Unauthorized access is handled in the following way: [...].

### 3.4 Access handling

[role description] is responsible to establish and maintain communication with [human resource function], ensuring that all personnel changes are integrated in access rights management.

Security events (of informational and/or exceptional type) arise during the processing of access. Security events are handled based on [...].

Security events that need to be reported by the access management process are assigned to [role description].

Security events are communicated by [role description], in the form of reports, on a daily basis to [Access Manager].

[role description] is responsible to disseminate and inform staff involved in the access management process.

### 3.5 Measurement

[role description] is responsible to generate and evaluate access reports on a monthly basis. The reports must be evaluated every month, by [Chief Information Security Officer], for improvement by [role description].
4. Process
4.1. Receive request

Access (or restriction) can be requested through:
- Change request (Standard change or new services)
- Service request
- Manager request
- Application script or request

4.2. Verification

Access management checks access to the service request from two perspectives:
- User identity – [Information security policy] defines valid identification methodology used by access management.
- [Regulatory or compliance]: Additionally to the user’s request, access management uses the following verification mechanisms:
  - [...]

4.3. Provide rights

[Role description] holds responsibility for execution of access requests. [Organization name] uses [...]

to execute access requests.

Conflicts in regard to access rights can be reported by:
- Related incidents
- Business processes described by [Access Manager], of impacted roles and groups as well as for follow-up see Conflicts and Exceptions in Appendix.

[Access Manager] is responsible for document, exceptions; see Conflicts and Exceptions in Appendix.

4.4. Check and monitor identity status

[Tool name] is used to check and monitor identity status. [Access Manager] is responsible to ensure tool availability.

4.5. Log and track access

[Access Manager] is responsible to:
- Ensure that granted access rights are properly used by monitoring activities of all operational processes

Comment [BV21]: This is an example. Adapt to your own situation.

Comment [BV22]: Enter the name of the policy.

Comment [BV23]: Example of verification mechanisms:
- Human Resources notification about new employee and request for new user identity and resources needed
- [...]

Comment [BV24]: This can be done by Access Manager or by CISO. Adapt to your own organizational setup.

Comment [BV25]: e.g. Technical Manager, Application Manager, Service Manager, Request Fulfillment Manager, etc.

Comment [BV26]: e.g. Service request, automated tool (enter tool name)...etc.

Comment [BV27]: ...
4.6. Remove or restrict rights

[Application and Technical Management roles] are responsible to remove or restrict access rights.

5. Roles and responsibilities

5.1. Access Manager

[job title] assigns the Access Manager role.

Responsibilities of Access Manager:

- Overall responsibility for carrying out activities within the scope of Access Management
- Coordinates with other Access Management roles
- Plans and manages tasks needed to support Access Management process
- Responsible for reporting and information management
- Develops and maintains access management process and procedures

5.2. Service Desk staff

Service Desk staff is used as a means to request access to a service, communicate with users and detect incidents related to access rights. The Service Desk is described in the document “Service Desk Function.”

5.3. Technical operator and Application analyst/architect

The Technical operator and Application will be handled by the Access Management process. The Technical operator and Application analyst/architect are defined in the document “Technical Management Function” and “Application Management Function.”

5.4. IT operator

Operational access management tasks are performed by the IT operator, who is defined in the document “IT Operations Management Function.”

6. Measurement and metrics

6.1. Measurement
Reports showing all access requests in a defined period are available. [role description] is responsible to produce reports.

6.2. Metrics

Metrics reports are produced monthly, with quarterly and yearly summaries. Metrics to be reported:

- Total number of access requests
- **Breakdown of access requests by categories**
- Number and percentage of the access requests that triggered an incident
- Breakdown of access request by time of day, to help prevent peaks and ensure matching of resources

Reports are grouped into the following categories:

- Access request category
- **Breakdown of access requests by categories**
- Location

6.3. 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>It is ensured that confidentiality, integrity and availability are provided according to the Information Security Policy.</td>
<td>Percentage of incidents that include access attempt issues</td>
</tr>
<tr>
<td>Provide access to the system on a timely basis based on SLA/OLA parameters.</td>
<td>Number of audit findings that discovered excessive access rights for current users, users who changed roles, or who left the organization</td>
</tr>
<tr>
<td>Percentage of access requests that were responded to within SLA/OLA parameters.</td>
<td>Percentage of access requests that were responded to within SLA/OLA</td>
</tr>
</tbody>
</table>

7. 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>Service Request Record (in electronic form)</td>
<td>[tool name]</td>
<td>[job title]</td>
<td>Technical operator and Application analyst/architect can update the record</td>
<td>Service Request Records are kept for 5 years and then archived.</td>
</tr>
<tr>
<td>Request for</td>
<td>[tool name]</td>
<td>[job title]</td>
<td>Technical operator and</td>
<td>Request for</td>
</tr>
</tbody>
</table>

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

This document is valid as of [date].

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

### 9. Appendices

- Appendix 1 Conflicts and Exceptions

[job title]

[name]

[signature]

---

Comment [BV35]: Change if needed.

Comment [BV36]: Overall responsibility for Service Request Records. Usually Request Fulfillment Manager.

Comment [BV37]: Change if needed.

Comment [BV38]: Example: for current year (YTD) – in [tool name], otherwise archived in [tool name or place of archive].

Comment [BV39]: This is only a recommendation; adjust frequency as appropriate.

Comment [BV40]: Only necessary if the Procedure for Document Control prescribes that paper documents must be signed.