Incident Management Departmental Policy
Health Sciences Center

![UNM Health Sciences Center logo]

Document Control

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Date</th>
<th>Action or change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rick Adcock</td>
<td>1.00</td>
<td>6/10/15</td>
<td>Final Version</td>
</tr>
</tbody>
</table>
Table of Contents

Purpose of this Departmental Policy ................................................................. 1
Policy Objectives ............................................................................................. 1
Scope .................................................................................................................. 1
Policy .................................................................................................................. 1
Exceptions ......................................................................................................... 2
Policy Compliance and Monitoring ................................................................. 2
Policy Review .................................................................................................... 2
Definitions ......................................................................................................... 2
Supporting Documentation ............................................................................... 2
Acceptance ....................................................................................................... 3
Incident Management Departmental Policy

Purpose of this Departmental Policy
The purpose of this policy is to ensure that any incidents affecting the daily operations of the Health Sciences Center's (HSC) distributed IT environment are managed through an established process. The HSC will utilize a best practice ITIL framework for the implementation of Incident Management within HSC IT departments.

Incident Management is the process that defines how HSC IT departments track, respond, and resolve workforce member issues related to the use and access to enterprise IT services. The goal of Incident Management is to restore workforce members' use and access to enterprise IT services to normal operation within agreed service level targets.

Policy Objectives
- Minimize the amount of potential workforce member "down-time."
- Ensure that HSC IT departments use standardized methods and procedures for the efficient and prompt handling of all reported incidents that negatively affect workforce member access and use of enterprise IT services.
- Ensure that incidents are recorded, evaluated, and resolved in a controlled and timely manner.

Scope
This policy applies to all workforce members utilizing the HSC enterprise IT services. Therefore, the scope of the Incident Management Policy includes the following:
- All IT-supported HSC locations including UNM Hospitals and clinics, HSC academic and research departments, UNM Medical Group, and the Sandoval Regional Medical Center
- All environments subject to the Incident Management Policy determined by the ITSM Steering Committee
- HSC-owned Incidents (e.g., Incidents recorded and managed to closure by HSC IT personnel)
All items not specifically listed within the Scope section are deemed "Out-of-Scope."

Policy
The following policy is established for Incident Management:
1. All HSC IT organizations must use the currently approved documented incident management process and will be report, record, manage, and appropriately communicate through the HSC’s approved Incident Management tool.
2. All HSC IT Managers are responsible for ensuring the Incident Management Process is followed.
3. Upon resolution of an incident, the end user will be notified that the incident has been resolved and restored to normal business function. Once the incident has been resolved, the user will have three (3) business days to reopen the incident.
4. This policy will complement and not supersede compliance policies such as those associated with the Major Incident/Problem Response process.
Incident Management Departmental Policy

Exceptions
Any requests for exceptions to this policy must be submitted in writing and will be reviewed on a case-by-case basis. Exceptions shall be permitted only after documented approval from the ITSM Steering Committee.

Policy Compliance and Monitoring
Incidents will be reviewed on a periodic basis by the Incident Management Process Owner to audit policy compliance to ensure that this policy, along with associated procedures, guidelines, and standards comprising the Incident Management Process, are adhered to.

Policy Review
The Incident Management Policy will be reviewed on the following basis:
- Annually, by the Incident Management Process Owner
- Upon an update to the Incident Management Process and/or tool
- Upon request of the ITSM Steering Committee

Definitions
- **Incident**: An interruption to an IT service or reduction in the quality of an IT service impacting the ability of a workforce member to use technology in support of their work effort.
- **Incident Management**: The process responsible for managing the lifecycle of all incidents. The objective is to restore normal operations within agreed service level targets with the least possible impact on either the business or the user.
- **Incident Manager**: The person or group that is assigned the responsibility of managing the lifecycle of an incident, as defined within the Incident Management process.
- **Incident Management Process**: The process used to report issues with the access and use of enterprise services through the HSC's Service Request Management tool where the incident will be assessed, managed, and resolved within service level targets.
- **IT Service**: An IT service is made up of a combination of information technology, people, and processes. A customer-facing IT service directly supports the business processes of one or more customers and its service level targets should be defined in a service level agreement.
- **ITSM Steering Committee**: An executive body responsible for the guidance and direction of IT Service Management.

Supporting Documentation
- Incident Management Procedures
- HSC IT Security Policy HSC-240 IT Security Incident Response
Incident Management Departmental Policy

Acceptance
The undersigned have reviewed this document and approve its contents and agree to enforce this policy in their organization, including determining appropriate corrective action for non-compliance.

Incident Management Departmental Policy APPROVAL

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Matt Braun</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executive Director, Information Technology, SRMC</td>
<td>[Signature]</td>
<td>6/15/15</td>
</tr>
<tr>
<td><strong>Holly Shipp Buchanan</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIO, Administration and Academic Systems, UNM HSC</td>
<td>[Signature]</td>
<td>6-10-15</td>
</tr>
<tr>
<td><strong>Randy Ferguson</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Director, Information Technology CRTC</td>
<td>[Signature]</td>
<td>6-16-15</td>
</tr>
<tr>
<td><strong>Glen Jormigan</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator Information Technology, UNM Hospitals</td>
<td>[Signature]</td>
<td>6/11/2015</td>
</tr>
<tr>
<td><strong>Dick Weeda</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Technology Director UNMMG</td>
<td>[Signature]</td>
<td>6/11/2015</td>
</tr>
</tbody>
</table>