UNM HEALTH SCIENCES CENTER	Applies To: All HSC Responsible Department: KMIT Operations Council Revised:

Title: **HSC IT Major Incident Reviews**	**Procedure**

Patient Age Group:	(X) N/A	( ) All Ages	( ) Newborns	( ) Pediatric	( ) Adult

DESCRIPTION/OVERVIEW

In keeping with industry best practices and in order to maintain the security of HSC and UNMH IT systems, the Health Sciences Library and Informatics Center (HSLIC) and UNM Hospitals Information Technology department (UNMH IT) conduct reviews after major incidents that disrupt IT services at the Health Sciences Center (HSC). The purpose of these reviews is to provide an opportunity for IT personnel involved in the incident to discuss how this incident was handled, both what went right and what didn't, and to collectively learn from the incident toward improving IT services provided to the HSC and the security of those services.

This procedure is limited to HSC IT incidents. UNM IT also has a major review process, and the HSC will participate in UNM IT's process for incidents where they are the lead service owner.

REFERENCES

Not applicable.

AREAS OF RESPONSIBILITY

The HSLIC Program Operations Director facilitates HSC IT Major Incident Reviews. Members of the Knowledge Management and IT (KMIT) Operations Council are responsible for identifying and requesting reviews. The KMIT Operations Council examines all IT Major Incident Review documents and determines the priority of any cross-unit projects that arise as a result of the review.

PROCEDURE

Following an IT incident, any member of the KMIT Operations Council may contact the HSC IT Major Incident Review facilitator and request a review. Ideally, an HSC IT Major Incident Review should be conducted soon after the incident has been resolved. However, a review can be conducted at any time, and KMIT Operations Council members may request a review a month or more after the incident if he/she judges the review to still provide value. For incidents with regulatory and/or security implications, the HSC CIO will obtain approval of the HSC Incident Commander for the specific protocol and the optimum timing to conduct the review.

The request for a review will include the names of all parties who should be invited to the review. Consulting with other KMIT Operations Council members involved in the incident to determine who to include in the review is highly recommended. In general, review participants should include all staff directly involved in identifying and resolving the incident, an IT security representative, and help desk managers who fielded inquiries and communicated to the HSC community about the incident. In the case of IT incidents with regulatory and/or security implications, the HSC HIPAA Security and Privacy Officers and the appropriate HSC University Counsel will also be included as participants in the review.

After a request has been made, the review facilitator, in most cases the HSLIC Program Operations Director, will determine a time and location for the review and send a meeting appointment to all participants. The appointment will include the incident being reviewed and a copy of the HSC IT Major Incident Review template, attached to this procedure as Appendix 1. The facilitator will make reasonable efforts to accommodate the schedules of all participants in the review, giving priority to the person calling the review, as well as the HSC HIPAA Security Officer and HSC University Counsel in the case of reviews involving regulatory issues.

The KMIT Operations Council member who requested the review will develop a preliminary time line of the incident and submit to the review facilitator in advance of the review. This will help the facilitator more efficiently use the review meeting.

In general, the reviews will be one to one-and-a-half hours in length. If possible, they will be held in rooms equipped with LCD projectors so participants can view the HSC IT Major Incident Review template as the facilitator works with the group to complete it. The facilitator is responsible for moving the participants through the sections of the template and keeping accurate notes of the content for each section.

For reviews involving regulatory and/or security issues, the HSC CIO will consult with the designated HSC Incident Commander to determine the specific protocol to be used, but in general, all participants will be asked to sign a Confidentiality of Information Agreement form (Appendix 2), which will be collected by the facilitator and given to the HSC University Counsel attending the review.

After the review, the facilitator will complete the template and email a draft copy to all participants for revision with a deadline for submitting changes. The facilitator will incorporate the revisions and resend the revised draft to all participants in the event of significant, substantive changes to the document. The facilitator can elect to also send a draft of the review to the HSC or UNMH CIO if appropriate. In the case of reviews involving regulatory issues, the facilitator will use a secure document collaboration tool and have participants make revisions to the document using a limited-access folder in SharePoint.

In general, the facilitator will include the review on a future meeting agenda of the KMIT Operations Council. The KMIT Operations Council will examine the document, make any additional revisions and determines the priority of any cross-departmental projects that arise as a result of the review. For reviews involving regulatory issues, the review will be sent to the appropriate compliance officers after it has been reviewed by the KMIT Operations Council. For reviews involving other IT departments, the facilitator will send the final copy of the review to the person requesting the review and/or the departmental IT manager.

Copies of all reviews will be kept on a secure HSC SharePoint site. Reviews involving regulatory issues will be kept in folders for each individual review with access limited to the participants involved in the review and other appropriate compliance officers.

DEFINITIONS

Not applicable.

SUMMARY OF CHANGES

In June 2011, a security analyst was added to the list of regular participants in a review. In September 2012, the name of the procedure was changed to HSC IT Major Incident Review Procedure, and the procedure was modified to include submission of a preliminary time line for the incident before the review meeting.

RESOURCES/TRAINING

Resource/Dept	Contact Information
HSLIC Program Operations Director	272-0691, sbowler-hill@salud.unm.edu

DOCUMENT APPROVAL & TRACKING

Item	Contact	Date	Approval
Owner	Sally Bowler-Hill, HSLIC Program Operations Director		
Committee(s)	KMIT Operations Council		
Official Approver	Associate Vice President for Knowledge Management & IT, HSC CIO		
Official Signature		[Day/Mo/Year]	
2nd Approver (Optional)	UNMH CIO		
Signature		[Day/Mo/Year]	
Effective Date		December 2010	
Origination Date		12/2010	

ATTACHMENTS

Appendix 1: HSC IT Major Incident Review Template
Appendix 2: Confidentiality of Information Agreement

Major Incident Review	Review Date:	Help.UNM Record #:
Incident name:	Incident date(s):	

Attendees:
Roles absent:

1. **Succinct overview of events. Include tickets opened and closed:**
   a.

2. **2-3 Sentence Summary of Events**

3. **Is root cause known?**

Description	Primary	Secondary
Human Error		
Procedure Failure		
Computing Hardware		
Networking Hardware (Voice or Data)		
Vendor Application		
UNM-built Application		
Utility Software (database, job scheduling, etc.).		
Systems Software (rules, configuration, OS, etc.)		
Facility (power, HVAC, water, alarms, etc.)		
Vendor Service		
Security Incident		
Unknown		

4. **Lead Service Owner for Root Cause Analysis:**

5. **Those things that were done correctly (including Incident process questions):**
   a.

6. **Those things that could be done better in the future:**
   a.

Item	Next Steps, Project to Prioritize or Done?	Groups

7. How to prevent recurrence:

a.

Item	Next Steps, Project to Prioritize or Done?	Groups

Appendix 2

HSC Compliance Office
Confidentiality of Information Agreement
Last revised: March 10, 2010

It is the policy of the University of New Mexico Health Sciences Center Compliance Office to protect the confidentiality of all compliance information gathered in the course of an investigation and/or preparation for compliance committee reports, regardless of form or source. You are being asked to sign this form because your participation on/under the direction of the Executive Compliance Committee (ECC) and/or IT Security Council (ITSC) provides you with access to information, whether communicated verbally or contained in files, data and/or other systems, that may not be shared with others; this information is referred to collectively as "confidential information."

Your permission to access and use information in the course of your association with the ECC and/or ITSC is subject to your agreement to strictly adhere to the following terms and conditions:

1. I acknowledge and agree that the maintenance of the confidentiality and integrity of all confidential information is a central requirement of my function with the ECC and/or ITSC, and any unauthorized disclosure or alteration of confidential information would harm the University and potentially cause substantial damage to rights of those individuals with protected rights of privacy, including students, employees and patients.
2. I will only use confidential information in a manner consistent with my authorized access and the duties and responsibilities of my position.
3. I will not provide or release confidential information to any individual or entity without proper authorization and or unless as required by law.
4. I will not make copies of any records or data except as required in performance of my duties.
5. I will destroy any confidential information for which I no longer have an official business use in a manner appropriate to the medium and consistent with University policy.
6. I understand and agree that my obligation to maintain confidentiality will continue even after my disassociation with the ECC and/or ITSC.

My signature below signifies that I have carefully read and agree to the terms and conditions of this Confidentiality of Information Agreement and acknowledge that my continued participation with the ECC and/or ITSC is dependent upon my strict adherence to all of its terms and requirements.

Print Name: _____

Signature: _____

Date: _____