SYSTEMS ACCESS MANAGEMENT

SAM TEAM

“HOW TO”

MANUAL

- A MANUAL FOR SECURITY MANAGERS -

SECURITY OPERATIONS, VANDERBILT UNIVERSITY INFORMATION TECHNOLOGY
SAM TEAM MEMBERS:
SYLVIA BUFORD-THOMPSON, MANAGER
TEAM MEMBERS: CHRISS GARVIN, ANGELA KING, PHOEBE ROSS
EMAIL: SYSTEMS.ACCESS@VANDERBILT.EDU   PHONE: 615.322.5630
# TABLE OF CONTENTS

**PART I**

**SECTION I:**
I. Interaction Between Security Managers and the SAM Team... *Pg. 4*
II. Systems Access Online Request Form Review... *Pg. 5*
III. VUMC User Management Tool for Security Letter Printing and User Auditing/Verification Process (List of Active Users)... *Pg. 13*

**SECTION II:**
Medipac Security Maintenance... *Pg. 16*

**SECTION III:**
Frequently Asked Questions (FAQ)... *Pgs. 24-25*
Helpful Links... *Pg. 25*
Security Manager Role Defined... *Pg. 26*

**PART II**
Eprocurement Process for SecurID Tokens
PART I
I. Interaction Between Security Managers and the SAM Team

II. Systems Access Online Request Form Review

III. VUMC User Management Tool for Security Letter Printing and User Auditing/Verification Process (List of Active Users)
I. Interaction Between the SAM Team and the Security Managers

Role of the SAM Team

The Systems Access Management Team (SAM) is the team responsible for granting, modifying, and deleting access to clinical applications; assigning, reassigning, and disabling SecurID tokens; managing and training security managers/token managers.

Each department/unit has a designated primary and secondary security manager who is responsible for requesting, modifying, and deleting clinical application access for users within their department/unit. In the requesting of clinical application access, the SAM Team works directly with the security manager verses working directly with the user. (See page 26 for full description of the Security Manager role.)

How are Clinical Applications Accessed?

Clinical applications are accessed with either a RACF ID and RACF password or a VuNet ID and Epassword. The RACF ID is the userid security managers obtain from the SAM Team. VuNet IDs and VuNet ID issues are handled through the AccessVu Team of Information Technology.

Example of a RACF ID and VuNet ID:

User: Jane L Doe  
- RACF ID: DOEX4AB (7 characters in length)  
- VuNet ID: doejl

What Applications Can Be Requested From the SAM Team:

- Medipac (Production, Training, Test,)  
  SAM team only grants the menu option. Functions are granted by the security manager.)
- Epic  
  (SAM team only grants the link to Epic; access is granted by VMG Training.)
- DB2/QMF
- General Ledger Production and Training  
  (Access must be further approved by Matthew McGlasson or Mary S. Robinson of Finance)
- MyHealth at Vanderbilt (Administrative Tool)  
  (Access must be further approved by Sue Muse)
- VORS (OR Schedule)
- Pacs Web
- Impax/Impax Cardiology/Imagecast  
  (Account Setup done by the IMPAX Team)
- Phillips Web View (CCT/VUH/VCH)
- TRMS (Total Report Management Systems)
- EBedboard
- Quill (Clinical Outpatient Notes Entry System)
- OPOC (Outpatient Orders with Compliance)
- RxStar (Prescription Writer)
- Starchart/Starpanel
- WizOrder
- PMM
- MaxSys (Utilization Management System)
- PHG EasyAdmin
- Acudose
- Teletracker
- POU (Point of Use)
- POS VERIFIER
II. Review of the Systems Access Online Request Form

What is the Systems Access Online Form?

The systems access online form is the form used to request, modify, and delete clinical application access as well as request user name changes, transfers, and SecurId tokens.

**Only security managers have accessibility to the online request form**

How Can I Access the Online Form?

The online form is located at the URL: https://samprod.mc.vanderbilt.edu/sam

Enter your VuNet ID/Epassword in lower case to login

After login, you will then be taken to the home page of the online request form.
**Helpful Link: Search History**
The Search History option allows you to review the history of requests submitted for a particular user.

Below is a partial listing of applications, status, requestor, etc. submitted for the VuNet ID: abc123. This list can be sorted by “Application” or the “Created On” columns. If you want to see if a certain application has been submitted for the user, simply choose the application from the drop down menu.

Click “Home” to return to the main entry screen.
**Scenario 1:** New user Jane Doe, doej, is coming into the Burn Unit and needs access to Medipac (Production), VORS, EBedboard, Starchart/Starpanel, WizOrder, PMM, PHG Armband, Acudose, POU, and Teletracker.

1). Enter the VuNet ID of the person you are requesting. Be sure the VuNet ID is entered correctly. (VuNet IDs entered incorrectly will result in the request being denied.)

**VuNet ID Tidbit: The PII (Personal Identifiable Information) must be entered on the VuNet account (this information includes the user’s social and birth date.) The SAM Team uses the PII information as unique identifiers. If this information is not entered, the online request will be denied. A denial message will be sent to the requesting security manager with reasoning for the denial.

2). If the user has an up-to-date confidentiality agreement on file, Check the “I confirm that an up-to-date Confidentiality Agreement is on file” box.

3). The Director/Manager must approve this request. If so, check the “I confirm the Director has approved this request” box.

**Both boxes must be checked. If not, you will receive one of the two messages:**

Before clicking “Submit Request” you will notice a display table listed below.

As you begin submitting online requests, your requests will be listed in the table. Any request you submit will be housed in this table regardless if the user is active/inactive, transferred, etc.

The table shows the VuNet ID, User Name, Department, Pending Requests, Submitted Date, Requestor and can be sorted by either of these fields. Pending Requests simply shows the number of applications you have requested that are still “pending”. Once processed by the SAM Team this number will display as 0.
Let’s go back and click the “Submit Request” button.

You will notice that you have received the error message:

Because the SAM Team no longer receives a direct feed from Human Resources, the above message will be received. You can click “OK” to manually enter the User’s Information (i.e. Name, Title, Birth Date, etc). Please be sure to complete all fields.

**Nature of Requests:**
With the online form you are able to:

- Request Access (for new users)
- Change/Update Existing Access (for existing users with existing clinical application access)
- Change Name and/or Title
- Transfer (Users coming into a new department)
Nature of Requests (cont.)

- Delete (Inactivate Users)
- SecurID Token (Request, Reassign, and Disable SecurID Tokens)

**Nature of Request: Request Access (By default “Request Access” is already checked)**

Enter the information under the **EMPLOYEE INFORMATION** Section. You do not have to enter the Employee’s RACF ID. This information will be provided to you.

► **Questions: Is this a Provider? Yes /No**  
**Is this Provider Credentialed? Yes/ No**

These questions must be answered for all requests. Provider refers to MDs, Credentialed NPs, Residents, and Fellows. Please submit the request only if the users are credentialed (non-credentialing may result in the request being denied). Research MDs and NPs can be submitted pre-credentialing, however, NPs must be submitted as a Nurse. If the users are non-credentialed employees simply choose “No” to “Is this a Provider?”

Under **ACCESS REQUESTED** you will see the columns: “Add Request” (You will also see columns “Cancel Request” and “Change Request.” These options are grayed out.)

*Remember our Scenario 1: New user Jane Doe, doej, is coming into the Burn Unit and needs access to Medipac (Production), VORS, EBedboard, Starchart/Starpanel, WizOrder, PMM, PHG Armband, Acudose, POU, Teletracker.*

In order to request these clinical applications, scroll down to each application and check the “Add” box. See the online form for Medipac, VORS, etc. Applications such as Starchart/Starpanel, WizOrder, PMM, AcuDose, etc. require additional information.
**Starchart/Starpanel:**
Non-VU Employee Section: This section is to be checked if the user is a non-Vanderbilt employee. Some Non-VU employees are given restricted access. In these cases, either “RestrictPanel” or “Restrict” should be checked. A date in which the Starchart/Starpanel access is due to expire should also be noted in the expiration date field. An email will be sent to the security manager the morning of the indicated date.

**WizOrder:** The Role, Department, and Wiz Privileges should also be entered.

**PMM:** The SAM Team only grants access to Clinical Requisitioners, all other roles should go through the Materials Management Team.

*See the online form for other applications that require additional information.*

Once you have selected all needed applications click the “Submit Requests” button.

If you have users that need the exact access, click the button, “Make Same Request for Next User”. You will then only need to enter the user’s VuNet ID and Employee Information. The applications will be pre-checked for you. You will however need to check “Make Same Request for Next User” each time.

If you are not ready to submit the request and would like to save what you have done for a later time, click the “Save Draft” button. Save draft only saves the request in draft mode. Requests in “draft” mode are not seen by the SAM Team until the requests are submitted.

After submission if a request needs to be canceled, simply go back into the online form, select the user, select “Cancel” beside the application that should be canceled, and click the “Submit Request” button. (Request can only be canceled if the SAM Team has not processed the request.)

**Nature of Request: Change/Update Existing Access**

This option is used to request/modify existing user’s access. The last action performed for the user will be automatically checked under Nature of Request.

If you need to grant additional access, check “Add” beside the needed application.
**Nature of Request: Change In Name and/or Title**
This option is used to request a user’s name change or title change.

**If a name is changed, the name must be changed first in Human Resources before the name associated with the RACF ID can be changed.**

Name Changes: Enter the former name and the current name (Changed To).
Title Changes: Enter the former title and the current title (Changed To).

**Nature of Request: Transfers**
This option is used to request access for users that are transferring into the security manager’s area.

**If users are transferring out of the area, a delete request must be submitted verses a transfer request.**

Transfer Information: Enter the user’s old department, new department, new center number, and old and new unit change (if applicable).

Under Nature of Request, you may also check “Change/Update Existing Access” once the transfer information is entered. You will also need to:

1) Click “Add” to any applications needed that have not been previously requested.
2) Click “Change” to any applications needed that have been previously requested by the former security manager.
3) Place in comment field “Please delete applications: (list any applications previously requested by the former security manager that is no longer needed for the current job role).
   Example: “Please delete Medipac and Bedboard access”
1) Submit request when finished.

**If only the transfer option is submitted, please note all previous applications requested will be removed, the form will now appear blank. You will need to request again all needed clinical applications.**
Nature of Request: Delete Access
This option is used to request the inactivation of a user.

Select “Delete” beside all known applications the user has access to. If unknown the “Search History” is a good option to use. If nothing is found in the Search History you may check “Delete All.”

“Delete All” means the SAM Team has to check each application to verify the user is removed.

Nature of Request: SecurID Token Request Only
This option is used to request SecurID Tokens which are devices that allow remote entry into Starchart/Starpanel. Users must have access to Starchart/Starpanel before a token can be granted. Tokens have a lifespan of three years after which they will no longer work. The expiration date and the serial number are both listed on the back of the token. The cost of the SecurID Token is $75.00.

Note: SecurID token requests can not be submitted in conjunction with any of the other request options under Nature of Request.

You can request a New token or existing tokens can be Reassigned or Disabled.

“Request a SecurID Token *(Enter eProcurement Order # below)*:
SecurID token ordering is a two step process. The token has to first be paid for through eProcurement (see Part II: Eprocurement Process for Ordering Tokens.) After the eProcurement order is approved and the email confirmation is sent and received, the online system access request should be submitted.

“Reassign an Existing SecurID Token and Disable An Existing SecurID Token*:
Any token with continued lifespan and no longer used by the original assignee can be reassigned to another user. Any token that has been lost or damaged should be disabled. The same information is needed when completing the Reassign and Disable token section. If the previous assignee is unknown the security/token manager may phone the Help Desk. **Remember, the expiration date and serial number is listed on the back of the token.**

Click “Submit Request” after the information is entered.
III. Security Letter Printing and Active User Review

URL Location: https://10.109.11.191/login.php

When a RACF ID is created and the online request has been fully processed, the security manager receives an automated email of the completion. Included within the email is a link to the VUM User Website to print the user’s security letter. The security letter includes the user’s RACF ID, initial password, and password reset stipulations. This letter should be given or faxed directly to the user, not emailed.

* Tip: Users are currently allowed to log into a clinical workstation with their VuNet or their RACF ID.

After entering the website URL you may receive the website certificate error, if so click “Continue to this website (not recommended).”

Log into the VUM website with your RACF ID and your RACF password. If your RACF ID is revoked or you do not remember your password, please contact the Help Desk (343-4357).

User Letter Printing:
To print security letters, in the “User Letters for Security Administrator” column, check the name of the user to be printed and click “Print” in the “To Print User Letters” column.

*If you are allowed to view the security letters of your backup security manager, that security manager’s name must be selected first from the “Select Security Administrator” column.
**User Auditing/Verification Process (List of Active Users):**
This option lists the name, RACF ID, and VuNet ID of all active users assigned to the RACF ID of a particular security manager.

Bi-Annually security managers are asked to review their list of active users. Security Managers are sent an email with instructions on how to run the active user list and asked to verify, a) whether the listed users are still within their department/unit, b) all users have the correct applications needed for their current job role, c) all transferred users have been inactivated or removed from your list; d) all users within Medipac have been verified (Medipac security maintenance covered in Section II.).

**If transferred users are still within Vanderbilt, the old and new security manager can coordinate the transfer so the user will not lose access.**

To run the list of Active Users, click the “List Active User” link and enter your RACF ID. The system may take a minute to run. Once finished you will see a list of users under the RACF ID entered.

---

**Reprint Security Letter Option:**
If for some reason you will need to reprint a Security Letter that was once in your queue, simply click the “Reprint User Letter” link and enter the user’s social security number.

---
SECTION II

Medipac Security Maintenance
Section II: Medipac Security Maintenance

When Medipac access is needed, the Security Manager submits an online systems access request form. Although the request form is submitted, this only grants the user the link to Medipac on his/her login menu. The security manager has granted the actual Medipac functions through Medipac security maintenance.

Medipac is accessed through the 3270 Mainframe Emulator (Reflections or the VUMC login menu) where you will login with your RACF ID and your RACF ID password (Your RACF ID and your RACF ID password is the same ID and password combination used to access your security letters.)

Medipac has three regions, most users work within Medipac (the production live region), MEDP3M (Training region), and MEDP3T (Test region). 

Permission has to be granted by the Informatics Medipac Team Director before a user is approved for Medipac Test.

Enter S or X beside Medipac or you can type Medipac on the command line.
Enter S or X beside “TECHNICAL FUNCTIONS”. You will also notice at the bottom there is PAV 1. There are five Pavilions within Medipac. Currently we are entering this user to access the Medipac Pavilion of VUH. More about Pavilions in the FAQ Section, Page 25.

**MASTER MENU**

<table>
<thead>
<tr>
<th>MEDIPAC RELEASE 17</th>
<th>PROFILE MAINTENANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCHK GENERATE CHECK DIGIT</td>
<td>PEXT PROFILE EXTENSIONS</td>
</tr>
<tr>
<td>PTMG PATIENT MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td>MEDI PATIENT ACCOUNTING</td>
<td></td>
</tr>
<tr>
<td>MRAS MEDICAL RECORDS</td>
<td>ADSC ADS CLASS EXERCISE</td>
</tr>
<tr>
<td>CTRK CHART TRACKING</td>
<td>TURR TUMOR REGISTRY</td>
</tr>
<tr>
<td>S TECH TECHNICAL FUNCTIONS</td>
<td>TRAM TRAUMA REGISTRY</td>
</tr>
<tr>
<td></td>
<td>CICS STAND ALONE CICS</td>
</tr>
<tr>
<td>INBOUND INTERFACE PROC.</td>
<td></td>
</tr>
<tr>
<td>ZIIP IIP TOOLKIT UTILITIES</td>
<td></td>
</tr>
<tr>
<td>INSURANCE ELIGIBILITY</td>
<td></td>
</tr>
<tr>
<td>EINO ELIGIBILITY INQUIRY</td>
<td></td>
</tr>
<tr>
<td>INTE INTEGRATION</td>
<td></td>
</tr>
</tbody>
</table>

Pavilion Change Accepted

**CLEAR-EXIT**

KU030PC Page 01-of-01 User Id

**TECHNICAL FUNCTIONS**

<table>
<thead>
<tr>
<th>SECURITY MANAGEMENT</th>
<th>SYSF ENQUEUE MONITOR (MRO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>S SECIM SECURITY MAINTENANCE</td>
<td>SYSP PM ENQUEUE MONITOR</td>
</tr>
<tr>
<td>SECII SECURITY INQUIRY</td>
<td>SYSA PA ENQUEUE MONITOR</td>
</tr>
<tr>
<td>SECP SECURITY PASSWORD RESET</td>
<td>SYST SYSTEM STATUS INQ/UPDATE</td>
</tr>
<tr>
<td>CASM CASHIER MAINTENANCE</td>
<td>MQGE A.T.Q. PROCESSING</td>
</tr>
<tr>
<td>CAGM GUARANTOR CASHIER MAINT</td>
<td>RTAM REAL TIME ARCHIVE MONITOR</td>
</tr>
<tr>
<td>TRGM TERMINAL SECURITY</td>
<td>DPRF PROFILE (TS) PURGE</td>
</tr>
</tbody>
</table>

**ADD A NEW MEDIPAC USER:**

Enter either the RACF ID or the user’s four letter department code and hit the [enter] key.

<table>
<thead>
<tr>
<th>SECURITY MAINTENANCE</th>
<th>VANDERBILT MEDICAL CENTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER SECURITY SEARCH CRITERIA</td>
<td></td>
</tr>
</tbody>
</table>

User Id:
Department: acsd
This will bring up a listing of users within your department/unit that are set up with Medipac functions. What you will see is the User ID, Dept, Name, and Initials.

Click the **F9 key** to add a new user.

**Enter the User’s Security Information:**

- **User ID** = the user’s RACF ID
- **Password /Re-enter New Password** = abc123
- **Name** = Last Name, First Name
- **Initials** = the last three characters of the user’s RACF ID

To “Keep the Same Functions As” allows you to model the new Medipac user after an existing Medipac user. Tab to the space beside the **Y** and enter the model’s RACF ID. Hit [enter] to accept. **If you receive the error message that the initials must be unique simply add a # or $ as the first initial. Ex. #2a.**
MODIFY AN EXISTING USER:
From the Security Record Selection Screen place an S or X beside the UserID of the person to be modified.

Place a M on the line “FUNCTION SELECTION STATUS” and hit the [enter] key.

This will take you to the user’s Master Menu.

The master menu shows what functions the user has access to. These functions will be identified by having a three digit number in front of the function name and function description.
From the example we see the user has Patient Management, Patient Accounting, Medical Records, and Chart Tracking functions. The numbers are listed in sequence of 5 and will be listed on the user’s menu in the order they are numbered.

Page forward using the F8 key to see what functions under the master menu items the user has.

If we page forward to the Chart Tracking Menu we will see that DUKE12A has CTRA, CTRO, CTLI, and LOCI functions.

If you want to add additional functions, simply add a number not already used beside the function. If you want to remove a function simply delete the number beside the function.

Hit the F9 key to accept.
Ex. Adding additional function CPRI to appear after CTRA and removing function LOCI

Notice that 006 was entered beside CPRI and 020 was removed from LOCI.

**Tip:** When adding additional functions never use a number that is already listed. Doing so will remove access from the previous function.

Hit F9 to accept.

If after saving you receive the message **FUNCTION Number must be numeric** and a 0 is placed beside the function removed, simply hit the [end] key and hit F9 again.
DELETE AN EXISTING USER:
From the Security Record Selection Screen place a “D” beside the user you wish to delete and hit the [enter] key.

The system will give you the message: **WARNING—Press enter to confirm delete of this User ID**

Simply hit [enter] to confirm.
I. Frequently Asked Questions

II. Helpful Links

III. Security Manager Role and Responsibilities Described
Frequently Asked Questions

► Q. What is a VSA Administrator and how do I become one?
A. VuNet Services Administrators (VSAs) can assist users with dealing with their VuNet Ids, resetting Epasswords, modifying personal options, and other facets of managing a VuNet account.

In order to become a VSA you must: 1) Submit an application which is found at: http://its.vanderbilt.edu/files/documents/vsa_app.pdf

► Q. How do you appoint or remove a security manager?
A. The Security Manager’s Appointment and Removal form may be found at the following links:

► Q. What is the difference between a RACF ID and a VuNet ID?
A. A RACF ID (Resource Access Control Facility) ID is used to access applications such as Medipac, Epic, and POS Verifier/Estimator. This ID, 7 characters in length, includes 6 alphas and 1 numeric. RACF IDs are generated by the SAM Team and may be used to access the clinical workstation.

A VuNet ID is also used to access clinical workstations as well as email and C2HR. VuNet IDs are also handled by Information Technology. More information on ITS can be found here: its.vanderbilt.edu

► Q. Since users can log into the clinical workstation with a VuNet ID do we still need to request RACF IDs?
A. Yes, RACF IDs still need to be created and are used behind the scenes for application account setup.

► Q. What happens when I have a revoked RACF ID or an inactive VuNet ID?
A. Revoked RACF IDs may be resumed by the Help Desk, ext. 615.343.3457. Revoked/Inactive VuNet IDs may be handled by ITS, ext. 615.343.9999

► Q. I have received the “Systems Access Request(s) processed” email but no security letter is listed in my queue to print.
A. Security letters are only created for new and re-activated users. If a user has a current active RACF ID no new security letter will be generated.

► Q. How do I print a Security Letter?

► Q. I have users who need access to VPIMS but it is not listed on the SAM online request form. How can users get setup?
A. The SAM Team only grants access to the OR Scheduler (VORS). Please contact the Help Desk for access to VPIMS.
► **Q. What is a SecurID Token?**

**A.** A SecurID Token is an electronic device that allows access to Starchart/Starpanel outside of a VPN connection or a Virtual Terminal connection. The SecurID token generates dynamic passwords used in conjunction with the user’s VuNet ID and token pin number.

► **Q. How do I get a token and how much does it cost?**

**A.** The token ordering process and cost is explained in Section III Eprocurement Process for Ordering Token Section. You will also find a FAQ section on page 16.

► **Q. What are the different Medipac Pavilions?**

**A.** Pavilion 1 is VUH; Pavilion 3: Children’s, Pavilion 4: Heart and Vascular Institute; Pavilion 5: Psychiatric Hospital; Pavilion 7: Bill Wilkerson Center.

---

**Helpful Links**

► Systems Access Online Request Form (Log in with your VUNET ID and Epassword):  
[https://samprod.mc.vanderbilt.edu/sam/Access.aspx](https://samprod.mc.vanderbilt.edu/sam/Access.aspx)

► Website to print Security Letters and Check Listing of Active Users (Log in with your RACF ID and RACF ID Password):  

**Websites:**

► Systems Access Management:  

► Help Desk:  
[http://helpdesk.mc.vanderbilt.edu](http://helpdesk.mc.vanderbilt.edu)

► Information Technology:  
[lt.vanderbilt.edu](lt.vanderbilt.edu)

► AccessVU:  
[http://www.vanderbilt.edu/accessvu/](http://www.vanderbilt.edu/accessvu/)

► ITS Product Page for SecurID Tokens:  
[https://its.vanderbilt.edu/services/rsa-securid-tokens](https://its.vanderbilt.edu/services/rsa-securid-tokens)

► Eprocurement Ordering Process Tutorial:  
[http://its.vanderbilt.edu/files/web_files/RSA_SecurID_eProcurement_tutorial.pdf](http://its.vanderbilt.edu/files/web_files/RSA_SecurID_eProcurement_tutorial.pdf)
Security Manager Role and Responsibilities

- Maintain an understanding of Vanderbilt standards and policies regarding information security, confidentiality, and privacy and communicate these to individuals within my department.

- Assist the organization in identifying, classifying, and securing confidential and restricted information.

- Orient and train the faculty, staff, and trainees within my department on security awareness in general and security procedures that should be followed in direct relation to their job duties.

- Monitor compliance with information security policies and procedures, referring ongoing problems to the Information Privacy and Security Office.

- Monitor the process of granting system access to users within my department to ensure that appropriate information access levels and security clearances are maintained when transfers, changes in job functions, and terminations occur. This includes:
  - Creating and maintaining a current process map for all employee types regarding the process for notification of changes to employee status.
  - Creating and maintaining a list of active PAF responsible persons within the area served.
  - Creating and maintaining a list of departmental systems operators/owners that need to be notified when an employee status changes. Refer to policy IM 10-30.19 Authorization and Access to Electronic Systems and Applications Section IV: Specific Information, Item D: Modification of Access.
  - Maintain flow of information to and from department systems operators/owners that need notification of changes to employee status.

- Identify potential exposures and risks to the confidentiality, integrity, and availability of information and make recommendations to my Department Head or the Information Privacy and Security Office (when appropriate) to mitigate the risks.

- Alert the Information Privacy and Security Office to changes in the patient-care, business, and computer systems environments in the organization that would have an impact on the information security program.

- Train another individual in the department to act as an ISM backup, in case of emergency or absence.