Lab Location:	SGAH & WAH	**Date Distributed:**	9/26/2017
Department:	IT & Mgmt	**Due Date:**	10/3/2017
		Implementation:	**10/3/2017**

DESCRIPTION OF REVISION

Name of procedure:
Lab IT Employee Security Requests   SGAH.IT924.1   **Computer Password Request Form AG.F167.3**

Description of change(s):

SOP:
  Section 4: update DI
  Section 5: In section B, clarified DI responsibility for tech and non tech staff
 FORM:
  Add space to record employee ID number & DOB
 	
 This revised SOP and FORM will be implemented on October 3, 2017

Document your compliance with this training update by taking the quiz in the MTS system.

Non-Technical SOP

Title	**Lab IT Employee Security Requests**
Prepared by	Marie Sabonis Date: 9/28/2015
Owner	Marie Sabonis Date: 9/28/2015

Laboratory Approval		
Print Name and Title	**Signature**	**Date**
Refer to the electronic signature page for approval and approval dates.		
Local Issue Date: Local Effective Date:		

Review:		
Print Name	**Signature**	**Date**

Form revised 3/31/00

TABLE OF CONTENTS

1.   **PURPOSE**

To create, activate, modify, or terminate user's security access for staff utilizing the Sunquest Laboratory Information System and any IT related applications/functionality that are required for the employee to perform their job.

2.   **SCOPE**

IT security access is based on the employee's job functions. Sunquest Tech codes are also established based on their job responsibilities.

3.   **RESPONSIBILITY**

Supervisor or manager must complete a Computer Password Request Form for new employees or to make changes to an existing employee's security access.
   a. LIS Staff are responsible for Sunquest security and adding employee to Cerner Master Index file.
   b. Supervisor is responsible to requesting any additional application access needed for the employee.

4.   **DEFINITIONS**

Sunquest - Laboratory Information (Computer) System; LIS

DI (Data Innovations) – Middleware, used for resulting and storing / retrieving specimens

Outlook - Refers to Adventist Healthcare (AHC) email application

FES - Front End System, used for accessioning Microbiology cultures sent to Quest
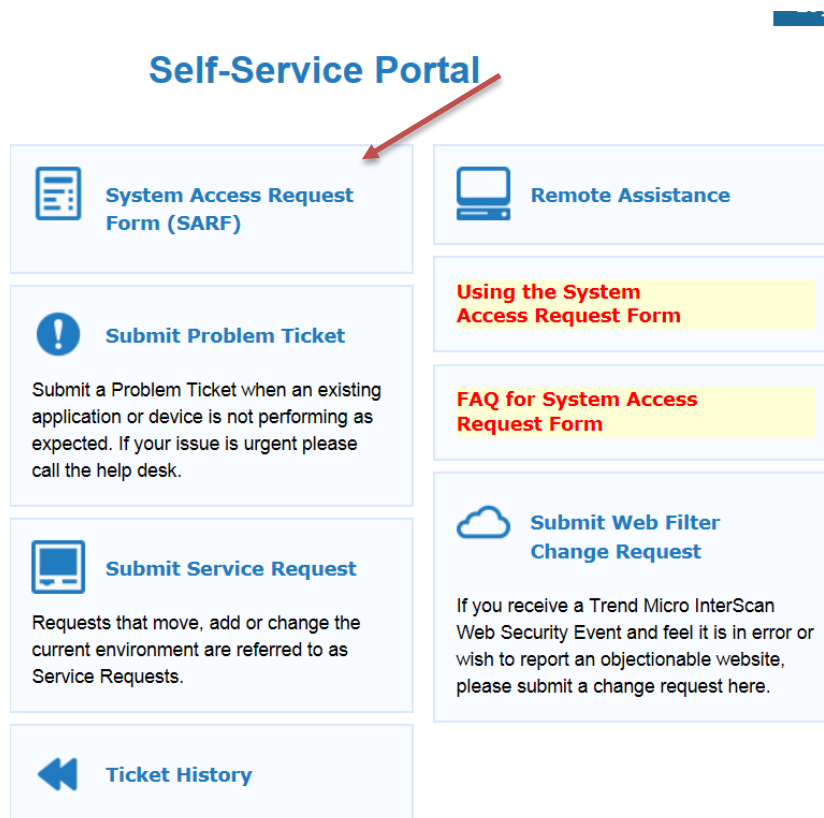
HIS – Hospital Information System

5. **PROCEDURE**

A. **New access or access modification for Non Sunquest applications (HIS access, AHC Outlook, Network access), excluding DI:**

Note: All Technical and Non-Technical Staff must be defined in Cerner. This provides Nursing with the ability to document appropriate lab staff when receiving a telephoned critical result.

- Technical staff must have access to Cerner.
- Non-Technical staff must be added to the Cerner Master Index file, unless Cerner access has been requested. When requesting an addition to the master index file, add the following statement "Please route to CORE team, requesting {insert employee name and DOB] (*specify which is their last name and first name and date of birth*) be added to the Cerner Master Index File." *Example*:

Please route to CORE team, requesting Mary (first name) Smith (last name) 5/1/1980 (DOB) be added to the Cerner Master Index File.

1. An AHC Service Access Request Form (SARF) must be submitted by the supervisor. It is located on the AHC Intranet under Corporate Services/Information Technology. Click on the "Service Request" link and log in using your network log in.
2. Click on "System Access Request Form".
3. Fill out the form and electronically submit it.
4. A ticket will be electronically generated and emailed to you.

Self-Service Portal

System Access Request Form (SARF)

Remote Assistance

Using the System Access Request Form

Submit Problem Ticket

Submit a Problem Ticket when an existing application or device is not performing as expected. If your issue is urgent please call the help desk.

FAQ for System Access Request Form

Submit Service Request

Requests that move, add or change the current environment are referred to as Service Requests.

Submit Web Filter Change Request

If you receive a Trend Micro InterScan Web Security Event and feel it is in error or wish to report an objectionable website, please submit a change request here.

Ticket History

Form revised 3/31/00

B. DI security:

DI is utilized by Technical staff for resulting and storing / retrieving specimens and by Non-Technical staff for storing / retrieving specimens.

Technical Staff: Core Lab Supervisor is responsible for setting up new employees and inactivating terminated employees.

Non-Technical Staff: LIS staff is responsible for setting up new employees and inactivity terminated employees.

C. New access or access modification Sunquest:

1. In order to obtain, change or terminate a security access code, a Computer Password Request form must be completed by the employee's supervisor and forwarded to the LIS staff.

2. Users must change their password when first logging on to the system. In addition, every 180 days (6 months), all Sunquest users are required to change their password. The system automatically asks the user to change the password when the change is due.

3. Functions are given to employees based on their position's duties and responsibilities. The system functions are defined to different security levels based on the area one works.

4. **A security code will be assigned within three working days**. Security agreement is then sent to the requesting supervisor.

5. The security agreement is signed by the new user and returned to the LIS staff for filing in the employee folder.

6. New employee security access will be terminated 7 days after submission to supervisor, if the security agreement is not returned to the LIS staff.

Note: LIS staff is responsible for opening an AHC Service request to have employees added into Cerner. This is not security access for Cerner. The purpose is to add employees to the Cerner database (Cerner Master Index file) so that Nursing can document appropriate lab staff when receiving a telephoned critical result.

D. Access deactivation: Sunquest and DI

1. The Laboratory Supervisor must submit the Computer Password Request Form to the LIS staff indicating when an employee is terminated or transferred to another part of the organization.

Form revised 3/31/00

2. The LIS staff deactivates the access code / user ID within 3 days of notification and the Computer Password Request form is placed in the employee folder.

3. LIS staff is responsible for opening service request to have employee inactivated in the Cerner Master Index file (Cerner Database).

E. LIS Setup: Sunquest

1. Use Function MRP, Option 11 to determine appropriate Tech Code for the individual requiring access. Tech code ranges are as follows:

   - 100-199 and 1000-1999   Lab Administration & LIS
   - 200-299 and 2000-2999   Blood Bank
   - 300-399 and 3000-3999   Customer Support & Phlebotomy
   - 400-499 and 4000-4999   Core Lab
   - 500-599 and 5000-5999   Microbiology
   - 600-699 and 6000-6999   Pathology (600-650 = Pathologists)
   - 700-799 and 7000-7999   Future - do not use
   - 800-899 and 8000-8999   Non Staff/ Interfaces
   - 900-999 and 9000-9999   Future - do not use
   - 10,000-99,999   Respiratory Therapy WAH (set to match user's I-Stat tech code)

2. Use function MA to create a Tech Code for the individual using the next available Tech Code identified on the MRP generated in Step 1.
   - Enter the Tech Code when prompted NAME/CODE/GROUP CODE:
   - Enter the employee's name using the format: Last Name, First Name Middle Name when prompted for NAME:

   Note: See step 4 for Deactivation of Tech Codes.

3. Use function SC to create and maintain accounts for each person that will use the system. Answer the following prompts in the system:

Prompt	System Entry
ACCESS CODE:	• Access codes are generally the user's 1st initial followed by up to 7 characters of their last name. • If the user has network access, use the network login ID as the access code (e.g. Mary Smith's network login ID may be MSMITH2 - define as MSMITH2 on Sunquest.)
TECH CODE/NAME:	• Enter the Tech Code assigned in Step 1
PASSWORD:	• New accounts - press <ENTER> and the system will automatically set the password to equal the ACCESS CODE. THIS IS A ONE TIME OPTION ONLY. • Existing accounts – When staff forgets their password or it isn't working. Reset their password to **ACCESS**. Then process to Expiration date. Password must be between six to twenty (6-20) characters. The characters may be alpha (upper/lower case), numeric or a combination. • After entering the code here, the system will require a second entry to

Prompt	System Entry
	verify the password change. • NOTE: all system passwords (except those defined for 1st time use) are ENCRYPTED.
EXPIRATION DATE:	• New accounts - press <ENTER> and the system will automatically set the password to expire on the next/first usage. (The user will be prompted to change their password the 1st time they use it). • Existing accounts – When resetting the password you must set password expiration to T+1. This way staff are prompted to change their password when they log in.
INITIALS:	• Enter the employee's first and last initials *Example*: Mary Smith = MS
MAILBOX GROUPS:	Enter mailbox groups as appropriate for the individual using commas between groups. Options: • ALL = ALL DEPARTMENTS - except Resp Therapy • BBS = BLOOD BANK SGAH • BBW = BLOOD BANK WAH • CAS = CUSTOMER/PHLEB SGAH • CAW = CUSTOMER/PHLEB WAH • CLS = CORE LAB SGAH • CLW = CORE LAB WAH • *LABS = LAB SGAH ALL* • *LABW = LAB WAH ALL* *Example*: a Core Lab Tech at WAH would be setup as follows: CLW,ALL
SECURITY LEVELS:	Enter security groups and or individual function levels as appropriate using commas between groups. Security Group Codes: • BBLEAD1 1,3,5,7,10,11,40,45 • BBLEAD2 1,3,5,7,10,11,40,45,49 • BBTECH 1,3,5,7,10,11,40 • CUSTSUPT 1,3,5,7 • LEADTECH 1,3,5,7,10,11,20,21 • MICROLEAD 1,3,5,7,10,20,21,30,31,33,34,35 • MSQL 50 • PATH 1,3,5,10,11 • PHLEB 1,3,5,7 • REFLAB 70 • SUPERVISOR 1,3,5,7,10,11,20,21,60 • TECH 1,3,5,7,10,11 *Example*: a Core Lab Tech that also does Reference Lab processing would be entered as follows: TECH,REFLAB
HOSPITAL ID FOR DATA ENTRY:	• Enter a period <.> if the employee has access to all hospitals patient records, or any combination of hospitals separated by commas. *Example*: SGMC,ARH,ABH • Enter SGAH if employee only has access to SGAH patient records • Enter WAH if employee only has access to WAH patient records

SOP ID: SGAH.IT924
SOP version #   1

CONFIDENTIAL: Authorized for internal use only.
Page 6 of 8

Prompt	System Entry
	• Enter ARH if employee only has access to ARH patient records • Enter ABH if employee only has access to ABH patient records
HOSPITAL ID FOR INQUIRY/REPORTS:	• Enter a period <.> if the employee has access to all hospitals patient records • Enter SGAH if employee only has access to SGAH patient records • Enter WAH if employee only has access to WAH patient records • Enter ARH if employee only has access to ARH patient records • Enter ABH if employee only has access to ABH patient records
DEFAULT HOSPITAL ID:	• Enter the HID code of the hospital where the employee is primarily scheduled to work (i.e. WAH or SGAH) • Pressing <ENTER> will leave this option blank and not assign a default hospital ID.
ENTRY MODES FOR DATA ENTRY:	• Enter MODE1
DEFAULT ENTRY MODE:	• Enter MODE1
RESTRICT IR/IQ TO PAT. LOC.:	• Enter any valid MA12 Patient location if the employee is restricted to only view results for patients in that location. • Pressing <ENTER> when setting up an account will leave this option blank and allow the employee access to patients from all locations within their allowable Hospital IDs.
RESTRICT IQ TO PHYS:	• Enter any valid MA13 Physician number if the employee is restricted to only view results for patients from that Physician. • Pressing <ENTER> when setting up an account will leave this option blank and allow the employee access to patients from all physicians within their allowable Hospital IDs.
FOR USE AT LAB LOCATION(S):	• Enter any valid MA6 Lab Location if the employee is restricted to work only within a specified Lab Location. • Pressing <ENTER> when setting up an account will leave this option blank and allow the employee to access the system from any Lab Location.
BLOCK MAILBOX/ERROR DISPLAY:	• At the (M/E/B/<N>) prompt, enter M to block display of mailbox messages, E to block display of system error messages, B to block both mailbox messages AND errors or press <ENTER> to accept the default N not to block messages. NOTE: all staff EXCEPT Customer Support, Lead Techs, Supervisors and LIS staff have this option set to "E"
ALLOW ACCESS TO REAL PATIENT NAME:	• Press <ENTER> to accept the default of N to disallow access to real patient names as this feature is not being used.
SITE ID FOR REMOTE IQ:	• Press <ENTER> to leave this option blank as this feature is not being used at this time.

4. Removal of system access is a two-step process.

   • First, deactivate the Tech Code in Function MA11 by entering a hyphen under the employee's name. The system will display "DEACTIVATED" next to

their name. Note: Tech codes cannot be re-used once assigned as this information is permanently stored in system transaction files (i.e. legal record of which employees performed each transaction in the system).

- Second, delete the user's access code in Function SC by opening their Security file and modifying the account. Enter a hyphen under the TECH CODE/NAME when prompted and respond Y to the prompt "CONFIRM DELETION OF ___:"

5. Additional Security Functions (e.g. security setup reports, setting up new system functions, setting up mailbox groups, and moving functions from one security level to another) may be accessed through function SC. Refer to Sunquest Information Systems Manual: System Operations Monitoring & Troubleshooting, Chapter 12: Security Maintenance for additional information.

6.   RELATED DOCUMENTS
Computer Password Request Form (AG.F167)
LIS Security Agreement (AG.F168)

7.   REFERENCES
None

8.   REVISION HISTORY

Version	Date	Reason for Revision	Revised By	Approved By
0	9/7/17	Header: add WAH Section 4: update DI Section 5: Section B clarified DI responsibility for tech and non tech staff	M Sabonis	M Sabonis

9.   ADDENDA AND APPENDICES
None

Computer Password Request Form

Employee Information	
Last Name	
First Name	
Department	<mark>Quest Employee ID #</mark>
Site	WAH ☐ SGMC ☐ GEC ☐ Quest Employee ☐ Quest Contract ☐ Other (specify)_____
<mark>**Date of Birth**</mark> (Non-Tech staff):	

Request submitted by:			
Last Name		Title	
First Name		Date of request	

Requested Action (mark an X under applicable action)			
Create New Access	Modify Access (specify)	Add Additional Functions	Terminate Access

Complete the applicable sections	
Employee should have access similar to this person	
Sunquest / HIS Access (new employees):	LIS staff performs maintenance on Sunquest For Technical staff: Supervisor opens ticket (AHC Service Request) for Cerner access for employee. For Non-Technical: LIS staff opens ticket to Cerner CORE to have new employee added to the "Cerner Master Index File". Refer to SOP Lab IT Security Request
AHC Outlook or Network Access:	Supervisor of employee submits AHC Security Request form
FES Access:	Supervisor of employee: Refer to Quest SOP WAH.S28 or SGAH.S30 for FES Password requests.
Data Innovations (DI) Access:	Technical staff: Supervisor of employee maintains Non-Technical staff: LIS staff maintains

DO NOT WRITE BELOW THIS LINE - COMPLETED BY LIS PERSONNEL				
LIS Sign on ID				
Completed by: Completed on:				