	POLICY Number: 7311-25-004 Title: Saskatoon Health Region User Account Policy
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: 7311-25-002, 7311-25-003, 7311-75-003 Date Approved: Dec 6, 2006 Date Revised: May 13, 2013 Date Effective: May 30, 2013 Date Reaffirmed: Scope: SHR & Affiliates

Overview

A user account is a SHR User's primary method of uniquely authenticating themselves in order to access the clinical and administrative technology systems and resources required to fulfill their day-to-day responsibilities. In addition to verifying a user's identity, a user account often defines a user's role by limiting the systems that he/she can access, what functions can be performed, and what information the user will be allowed to view, update, and/or delete. It is therefore important that users utilize SHR computing resources responsibly and protect their access from being compromised, as they are solely responsible for all actions performed using their user account.

DEFINITIONS

LOA (Leave Of Absence) means is any extended leave, including, but not limited to illness and maternity leave.

Saskatoon Health Region (SHR) User means a person with an active SHR User Account that allows access to the SHR computer network. A SHR User may include SHR employees, physicians, other healthcare professionals, students, contractors, vendors and any other person who has been approved for an SHR User Account.

Saskatoon Health Region (SHR) User Account means a personal account consisting of an Active Directory username and a password that is granted user access privileges, as specified on the *SHR User Account Application Form*. Privileges may include access to shared files, email and/or systems/applications.

1. PURPOSE

The purpose of this policy is to establish SHR's requirements for SHR Users and SHR User Accounts.

2. PRINCIPLES

2.1 All SHR Users are responsible for the security of SHR systems/applications, resources and information.

2.2 By establishing strong user account requirements, SHR will better secure its information and computing resources against unauthorized use.

3. POLICY

3.1 Access

3.1.1 All SHR Users shall be assigned a SHR User Account to access SHR systems/applications.

3.1.2 The Manager must submit the request using his/her own SHR User/Email Account in order to authenticate the request.

3.1.3 Employees who were hired prior to April 27, 2009 must sign and submit a SHR Confidentiality Agreement (see SHR Policy Privacy and Confidentiality, Appendix A or Privacy InfoNet page, (forms)) to People and Partnerships before their SHR User Account can be created

3.1.3.1 Employees hired after April 27, 2009 will have signed this agreement as part of their employee orientation.

3.1.4 SHR Users shall only retain access rights and privileges relevant to their current roles.

3.1.4.1 SHR Users shall not retain prior rights and privileges unless they have a clear business or clinical need and they have been explicitly authorized to do so.

3.1.5 SHR Users will not have access to their user account while on a LOA. Exceptions to this rule will be evaluated by ITS Security on a case by case basis.

3.1.6 All SHR User Accounts assigned to an individual who has been terminated must be disabled.

3.2 Conduct

3.2.1 All SHR Users are responsible and accountable for all activities conducted through the assigned SHR user account.

3.2.2 SHR Users will strictly adhere to all laws, copyright laws, codes of conduct, SHR privacy and IT policies, the Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP), the Health Information Protection Act (HIPA), the Personal Information Protection and Electronics Document Act, (PIPEDA) and any other applicable federal and/or provincial legislation on privacy and confidentiality including the collection, use, storage and disclosure of personal health information.

3.2.3 SHR Users shall not utilize a SHR User Account or computing device to access, distribute, or display objectionable material, including but not limited to:

- Obscene or pornographic material;
- Hate propaganda or discriminatory material;
- Defamatory and libellous material; and

- Sexually harassing material.

3.2.4 SHR computing resources are provided for SHR business and clinical use. Occasional, limited use of SHR computing resources is acceptable, provided it occurs only on an employee's own time and is otherwise in compliance with SHR policy and codes of conduct. However, SHR Users shall not perform actions such as downloading streaming audio or video, downloading or emailing large files, or storing personal files (e.g. music, photos, software) on SHR computer hard disks or network drives unless there is a clear, defensible SHR business or clinical rationale.

3.3 Privacy and Confidentiality

3.3.1 SHR Users shall have no expectation of privacy. All information stored on SHR computer equipment or accessed via the SHR network is the property of SHR.

3.3.2 LA FOIP (the Local Authority Freedom of Information and Protection of Privacy Act) allows the general public the right to request access to any administrative records in the custody of SHR through a Freedom of Information Request.

3.3.3 ITS reserves the right to actively monitor SHR systems/applications to protect and maintain the integrity of SHR system resources and to ensure SHR User compliance with SHR policy and procedures.

3.4 Security

3.4.1 SHR Users shall not share SHR User Account information and/or password(s). Under no circumstance shall a SHR User allow another individual to use their assigned SHR User Account to access a SHR system/application (see SHR's Password Policy).

3.4.2 SHR Users shall report any unauthorized use (or suspicions thereof) to their Manager.

3.5 Investigations

3.5.1 SHR will investigate unacceptable use or illegal activity that has been reported or detected. During the course of these investigations it may be necessary for the investigative resources to access or confirm evidence of objectionable material as defined in clause 3.2.3 above.

3.5.2 All investigative findings and SHR User activity or audit reports will be sent to an ITS Manager, who will follow up as required with the appropriate law enforcement agency and/or the Care Group/Service Department's Manager. In the event that law enforcement becomes involved, SHR's Director of Risk Management shall be notified.

3.5.3 ITS will not investigate unsubstantiated (spurious 'fishing expedition') requests by a Manager to view SHR User activity.

3.5.4 In confirmed cases of unacceptable use by an SHR User, it is the Manager's responsibility to take measures in accordance with SHR human resources procedures.

3.5.5 SHR and SHR Users will cooperate fully with external investigations where the investigation is related to a SHR User using SHR resources inappropriately.

4. ROLES AND RESPONSIBILITIES

4.1 SHR Users

4.1.1 Access SHR systems/applications only via the SHR User Account assigned to them and for the sole purpose of performing work/business on behalf of SHR.

4.1.2 Are responsible and accountable for all activities conducted on SHR systems/applications by access gained through their assigned SHR User Account.

4.1.3 Take necessary safeguards to prevent unauthorized access to SHR systems/applications through SHR User Accounts.

4.1.4 Immediately report all unauthorized use, or suspicions of unauthorized use, to a Manager.

4.1.5 Secure workstations when leaving them unattended. In cases where users are the sole user of a workstation, the workstation should be locked. For shared workstations, users should log off (not shut down or lock their workstations) as this will both secure the workstation and ensure that the next user has easy access.

4.1.6 Log off of their assigned SHR User Account at the end of a work day/shift.

4.2 Managers

4.2.1 Complete, approve, and submit an Information Technology Services *SHR User Account Application/Termination Form* (UAF), which can be found on the "Forms" page of the ITS InfoNet, for:

- An employee, physician, other healthcare professional, student, contractor, vendor, or other person for whom they are responsible, in order to ***apply*** for a SHR User Account and become a SHR User.
- A SHR User who has been ***terminated***, in order to have their SHR User Account disabled on the date of termination.
- A SHR User who has been ***transferred***, in order to have their associated SHR User Account privileges suitably updated on the date of transfer.

(**Note:** For U of S staff and residents, their designated department/division head or administrator must authorize the UAF. For physicians, their department head assumes this role.)

4.2.2 For new SHR Users, ensure that a SHR Confidentiality Agreement signed by the user has been submitted along with the SHR UAF.

- EXCEPTION: For new employees hired at SHR owned and operated facilities on or after April 27, 2009, SHR confidentiality agreements are signed at the employee's regional orientation.

4.2.3 Notify an applicant when their new SHR User Account has been activated.

4.2.4 Notify ITS Security by email when an existing SHR User's privileges need to be changed or reduced (e.g. when their job role has changed). Once a user's need to access SHR computer systems/applications, resources, or information has

disappeared, this access should be removed or downgraded accordingly.

4.2.5 ***Notify*** ITS Security of a LOA ***prior to*** the start of an LOA, so that the associated SHR User Account can be suspended the same day the LOA commences.

4.3 People and Partnerships

4.3.1 Notify ITS Security ***prior to*** a termination for cause so that the associated SHR User Account(s) can be suspended.

4.4 ITS Security

4.4.1 Create a SHR User Account upon receipt of a duly authorized UAF and confirmation that a signed SHR Confidentiality Agreement is on file for the associated applicant.

4.4.2 Notify the authorizing Manager when a new SHR User Account has been activated, supplying the account's username and temporary password.

4.4.3 Modify existing SHR User Accounts upon receipt of an authorized request with all relevant information from the SHR User's Manager.

4.4.4 Investigate unacceptable use or illegal activity that has been reported or detected.

4.4.5 Disable/suspend a SHR User Account:

- Upon commencement of a SHR User's LOA.
- Upon confirmation of unacceptable use or illegal activity, or if they deem urgent action is required due to SHR information or systems being at risk.
- Prior to a termination when requested by a SHR Manageror People and Partnerships
- Upon receipt of a properly authorized termination request.
- After six months of inactivity.

4.4.6 Back up and delete disabled user accounts after a total of 18 months of inactivity.

5. POLICY MANAGEMENT

The management of this policy including policy education, monitoring, implementation and amendment is the responsibility of the Director, Information Technology Services.

6. NON-COMPLIANCE/BREACH

Non-compliance with this policy will result in a review of the incident. A review for non-compliance may result in disciplinary action, up to and including termination of employment and/or privileges with SHR.

7. REFERENCES

Password Policy
Internet Acceptable Use
Email Acceptable Use
Emailing Personal Health Information

PROCEDURE Number: 7311-25-004 Title: Saskatoon Health Region User Account Policy	
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: 7311-25-002, 7311-25-003, 7311-75-003 Date Approved: Dec 6, 2006 Date Revised: May 13, 2013 Date Effective: May 30, 2013 Date Reaffirmed: Scope: SHR & Affiliates

1. PURPOSE

The purpose of this procedure to establish processes associated with applying for, activating, using, changing, disabling, and terminating SHR User Accounts.

2. PROCEDURE

2.1 Applying for a New User Account

2.1.1 The Manager completes and submits online a *SHR User Account Application/Termination Form* (UAF) ***before*** the employee's first day of employment, to initiate the process.

(**Note:** For U of S staff and residents, their designated department/division head or administrator must authorize the UAF. For physicians, their department head assumes this role.)

2.1.2 The Manager ensures that a SHR Confidentiality Agreement (see SHR Policy Privacy and Confidentiality, Appendix A or Privacy InfoNet page, (forms)) signed by the user has been submitted along with the SHR UAF.

EXCEPTION: For new employees hired at SHR owned and operated facilities on or after April 27, 2009, SHR confidentiality agreements are signed at the employee's regional orientation.

2.2 Creating and Activating a New User Account

2.2.1 ITS Security:

- Confirms that a signed SHR Confidentiality Agreement is on file for the associated applicant.
    - For new employees hired at SHR owned and operated facilities, ITS Security will check with People and Partnerships.
    - Medical Affairs will keep a copy of all physician signed confidentiality agreements. No verification necessary.
    - For all other types of users (unpaid students, volunteers, contractors, employees of SHR affiliates), a signed confidentiality agreement must be

received by ITS Security before a new SHR User Account can be activated.

NOTE: It is the authorizing Manager that is responsible for ensuring that a signed Confidentiality Agreement is acquired and submitted.

- Creates the SHR user account upon receipt of a duly authorized UAF.

  NOTE: A **minimum** of five working days notice is required to create an account. Although ITS Security strives to process requests as quickly as possible, turnaround times may vary based of the number of requests in the queue. For this reason, It is imperative that Managers submit their request as far in advance as possible so new accounts can be created and/or activated prior to an employee's first day of work.

- Assigns a username and temporary password to create a user account. The username and password combination will be used to grant access rights to information resources as requested on the UAF.
- Notifies the authorizing Manager after the user account is activated, with the user's username and temporary password.

2.2.2 Manager:

- Notifies the applicant *of* the account activation.

2.2.3 SHR User:

- Logs in for the first time using the temporary password, and then changes their password when prompted to do so. The new password must conform to the SHR Password Policy.

2.3 Using SHR User Accounts

2.3.1 Workstation Security

Users who leave their workstations unattended ***must*** secure them as follows:

- **Windows XP:**
  - Press the *Ctrl, Alt* and *Delete* keys simultaneously
  - Click the *Lock Workstation* button
  - To unlock the workstation press the *Ctrl, Alt* and *Delete* keys again, then log in to the system to resume work
- **Windows Vista & Windows 7:**
  - Press the *Ctrl*, *Alt* and *Delete* keys simultaneously
  - Click the *Lock this computer* button
  - To unlock the workstation press the *Ctrl*, *Alt* and *Delete* keys again, then log back into the system to resume work

2.3.2 Logging Off of a SHR User Account

At the end of a work day/shift, SHR Users ***must*** log off their SHR User Account as follows:

- **Windows XP, Windows Vista & Windows 7:**
  - Click the *Start* button and select '*Shutdown'*
  - Select '*Log off'* or '*Shutdown'* from the selection list and click the *OK* button

2.4 Changing SHR User Account Privileges

NOTE: A **minimum** of five working days is required to make changes to a user account. Although ITS Security strives to process requests as quickly as possible, turnaround times may vary based of the number of requests in the queue. For this reason, It is imperative that Managers submit their request as far in advance as possible.

2.4.1 When the User's Authorizing Manager Remains the Same

- The Manager emails the request with all relevant information regarding the change to its.security@saskatoonhealthregion.ca (**Note**: A UAF is not required.)

2.4.2 When the User Transfers to a New Position

- If a SHR User transfers to a new job, role, or position, their Manager shall complete the "Transfer" section of the UAF and submit it to ITS Security ***prior to*** the transfer date. This will allow the account access rights to be suitably updated the day of the SHR User's transfer.

2.5 Changing SHR User Account Properties

When a SHR User's information changes (e.g. last name, site, phone number, etc.), the user's Manager(Department Head for physicians)emails the request with all relevant information regarding the required change to its.security@saskatoonhealthregion.ca (**Note:** A UAF is not required.)

2.6 Termination of SHR Users

- The SHR User's Manager completes the "Termination Section" of the UAF and submits it to ITS Security ***prior to*** the termination date. This will ensure the account is disabled the day of the termination.
- In cases of termination for cause, People & Partnerships may assume responsibility for informing ITS Security of a pending termination.

2.7 Locking/Disabling of User Accounts

SHR User Accounts are locked/disabled in the following circumstances:

2.7.1 Account Misuse

- For urgent situations that may pose a security risk and require immediate account suspension, the Manager shall call the ITS Service Desk at 655-8200.
- Otherwise, unauthorized or improper use (or suspicion thereof) may be reported by emailing the ITS Security Investigations account, ITSSI@saskatoonhealthregion.ca.

2.7.2 Leave of Absence (LOA)

- The Manager must notify ITS Security of a LOA ***prior to*** its start date so that the

associated SHR User Account can be suspended the same day the LOA commences.

- The Manager emails all relevant LOA information to its.security@saskatoonhealthregion.ca (**Note:** A UAF is not required.)

2.7.3 If three attempts to access a user account are unsuccessful

- The account is suspended for15 minutes. After 15 minutes, the user may try again.

2.7.4 If they are not accessed for six months

2.8 Reactivating User Accounts

The Manager emails all relevant information to its.security@saskatoonhealthregion.ca to have a user account reactivated. (**Note**: A UAF is not required.)

2.9 Archival/Removal of User Accounts

- After a total of **18** months of inactivity, disabled/terminated user accounts will be backed up and deleted.

3. PROCEDURE MANAGEMENT

The management of this procedure including policy education, monitoring, implementation and amendment is the responsibility of the Director, Information Technology Services.

4. NON-COMPLIANCE/BREACH

Non-compliance with this procedure will result in a review of the incident. A review for non-compliance may result in disciplinary action, up to and including termination of employment and/or privileges with SHR.