Saskatoon Health Region	**POLICY** Number: 7311-25-009 Title: IT Systems – Monitoring, Access and Use
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: Date Approved: July 31, 2014 Date Revised: Date Effective: August 1, 2014 Date Reaffirmed: Scope: SHR & Affiliates

Any PRINTED version of this document is only accurate up to the date of printing. Saskatoon Health Region (SHR) cannot guarantee the currency or accuracy of any printed policy. Always refer to the Policies and Procedures website for the most current versions of documents in effect. SHR accepts no responsibility for use of this material by any person or organization not associated with SHR. No part of this document may be reproduced in any form for publication without permission of SHR.

OVERVIEW Saskatoon Health Region's clinical and business processes are highly dependent on information technology systems and services. Tracking the activity of system users helps protect the confidentiality and integrity of electronically stored information by providing a mechanism to detect unauthorized or improper information access. Tracking system changes and system activity helps ensure the integrity and availability of the systems themselves by ensuring that changes to a system are authorized, system errors and problems are detected and diagnosed effectively, and malicious or suspicious information systems activity can be detected, contained, and investigated.

NOTE: This policy covers SHR's enterprise systems, applications, and databases. Microsoft Access databases are not within scope of this policy, as general protection of the information that they contain can be achieved by restricting access to the database itself. However, it is highly recommended that SHR business units do not store information critical to business or clinical processes in Microsoft Access databases in a permanent or long-term manner, as this technology does not support multiple users, large volumes of data, or robust logging and monitoring of user activity.

DEFINITION

Data Center means a secure physical area that contains the computer servers, storage, and network gear necessary to provide shared, highly available IT applications and services, including the storage, processing, and retrieval of electronic information (i.e. data). Data centers are expected to include physical access controls, environmental controls, redundant or backup power supplies, and redundant data communication connections.

IT GRC means the Information Technology Governance, Risk, and Compliance group within SHR's Information Technology Services (ITS) department. This group's roles and responsibilities are described in section 4.1, below.

Threat Risk Assessment means identifying the threats or vulnerabilities faced by a specific IT asset of value, determining the risk (i.e. likelihood and impact) of each threat, and developing protective and proactive measures to mitigate or eliminate these threats.

Issues that could prompt a Threat Risk Assessment could include (but are not limited to): whether an application stores personal health information; whether an IT system or service and/or its data are being hosted by a third party; whether the proposed implementation of a system adequately accounts for the high availability expectations (e.g. 24x7) of its user base; whether the system or its vendor are located outside of Canada; whether the system utilizes hardware and software technologies that match SHR's existing IT standards; whether the IT system or service will be accessible from the Internet; and whether the system will adequately scale to meet the growing demands and storage needs of its users over time. For other examples of potential issues to consider during a Threat Risk Assessment, please refer to Appendix A.

1. PURPOSE

The purpose of this policy is to establish requirements for SHR auditing, monitoring, and reviewing controls for Information Technology (IT) Resources.

2. PRINCIPLES

2.1 Physical access to secure SHR data processing areas such as data centers is subject to logging, auditing, and review.

2.2 IT controls are required to:

- Help SHR protect and maintain the security of information and IT Resources
- Aid in determining compliance with (and measuring the effectiveness of) SHR's Privacy policies and processes
- Aid in determining compliance with (and measuring the effectiveness of) SHR's IT Security policies, processes, and standards.

2.3 SHR is required to comply with the Freedom of Information and Protection of Privacy Act (FOIP) and the Health Information Protection Act (HIPA).

3. POLICY

3.1 IT SYSTEM MONITORING

3.1.1 All systems/applications that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions will record and retain audit-logging information sufficient to determine:

- the activity that was performed;
- the account or system that performed the activity, including where or on what system the activity was performed;
- the system the activity was performed on;
- the time that the activity was performed;
- the tools that were used to perform the activity;
- the status (such as success vs. failure), outcome, or result of the activity.

3.1.2 Legacy (existing) systems/applications that cannot conform to all SHR ITS monitoring and logging standards (3.1.5, 3.1.6 and 3.2 below) must meet as many as possible. However, the responsible business unit must put all such systems/applications on an upgrade/replacement path such that these shortcomings are addressed as part of the next major release cycle.

3.1.3 New systems/applications that are being considered for SHR use shall be evaluated *prior to* purchase to verify whether or not they are capable of meeting the standards for auditing, monitoring, and reviewing of system, network, and user activity as outlined in this policy. This includes including relevant evaluation criteria in any associated RFPs. When in doubt, the services of SHR Information Technology Services or a reputable external contractor with expertise in this field shall be engaged for advice and assistance.

3.1.4 Implementation of new systems/applications that do not meet the auditing and monitoring requirements outlined by this policy may be refused until such time as they are brought into compliance.

3.1.5 Security controls, audit trails, and activity logs will be used for IT resources during automated and manual processes. Monitoring of IT resources shall include, but is not limited to:

- Creating, reading, updating, or deleting confidential information, including confidential authentication information such as passwords;
- Creating, updating, or deleting information not covered in the first bullet point, above;
- User authentication and authorization for activities covered in the first and second bullet points, above, such as user login and logout;
- Controlling access to software that monitors or modifies network configurations or devices;
- Equipment maintenance records of suspected or actual equipment faults and maintenance activities;
- Fault logs and reports;
- Internet use;
- External network connections and remote access networks;
- Entry control logs recording entry statistics (e.g., name, affiliation, date, and time, et cetera) to SHR IT Resources and data processing facilities;
- Internet audit trails (where required);
- The maintenance of synchronized clock settings;
- Initiating a network connection;
- Accepting a network connection;
- Granting, modifying, or revoking access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;

- ➢ System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
- ➢ Application process aborts, failures, or abnormal ends, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
- ➢ Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or antispyware system.

3.1.6 To maintain the integrity and availability of information systems, IT personnel (and, as appropriate, business unit IT system support personnel) will maintain either manual or automated system logs of their activities. Personnel logs shall be subject to regular independent checks against operating procedures to ensure that adequate processes are logged and that the procedures are being followed. Logs shall include, but are not limited to:

- System starting and finishing times;
- System errors or warnings identified and corrective actions taken;
- When automated paging of errors is used, a record of the time an error occurred, when the page was sent, and the pager/cell phone number;
- Confirmation of the correct handling and classification of data files and computer output; and
- The name or User ID of the individual making the log entry.

3.1.7 Electronic access controls shall be employed to protect IT Resources in accordance with existing SHR electronic information access control and SHR IT security standards. Electronic access privileges are monitored and audited to detect potential vulnerabilities or access privilege abuse.

3.1.8 ITS will ensure that controls are in place for the monitoring and early detection of malicious network activity.

3.2 FORMATTING AND STORAGE

3.2.1 The system of logging and auditing will ensure the integrity of the logs and support enterprise-level analysis and reporting. Mechanisms that support these goals include but are not limited to the following:

- Event Logs collected by a centralized log management system;
- Logs in a well documented format sent via syslog, syslog-ng, or syslog reliable network protocols to a centralized log management system;
- Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and

- Other open logging mechanisms supporting the above requirements such as those based on CheckPoint OpSec, ArcSight CEF, and IDMEF.

3.3 IT SYSTEM AUDITING

3.3.1 SHR's IT GRC group will develop system audit controls, including maintenance of audit trails for employee access attempts to intranet, internet, applications, browsing and directories.

3.3.2 All audit tools will be protected to safeguard integrity and to prevent misuse.

3.3.3 Contractors shall maintain a log of all access to SHR information and IT resources, including all successful and unsuccessful requests for physical, environmental, or electronic access. This log shall be made available, upon request, to SHR's IT GRC group for auditing purposes.

3.3.4 At the request of SHR's IT GRC group, the business unit that owns an SHR IT system shall perform audits of the systems for which they are responsible. Investigations may be requested based on reports or suspicions of wrongdoing, when existing risks, controls, policies, or regulations have changed, as a follow-up to previous audits to ensure that recommendations have been complied with, or as the result of a random or periodic spot audit program. The Principles of Investigations (see SHR's Fraud procedure) will be followed.

3.4 REVIEWING

3.4.1 Logs will be protected to maintain integrity and to prevent unauthorized access. Logged information may be filtered by ITS to ensure that only relevant Information is reviewed.

3.4.2 The individual(s) reviewing the log shall have a segregation of duties from the activities being monitored.

3.4.3 Logs of faults and errors for information systems and services will be reviewed by the parties responsible for the availability and maintenance of that system to ensure faults have been satisfactorily resolved and corrective actions taken.

3.5 THREAT-RISK ASSESSMENT

3.5.1 IT systems or services that store, transmit or process confidential information (as defined by SHR's Information Classification, Labeling, and Handling policy) or face the public Internet, require a threat risk assessment prior to their initial acquisition, prior to significant system upgrades, and periodically as the regulatory or threat landscape changes over time.

- ➢ If a threat-risk assessment is required, contact ITS for advice and expertise, or engage the services of a reputable third party firm.
- ➢ The outcome or objective of a threat and risk assessment is to provide recommendations that maximize the protection of

confidentiality, integrity and availability while still providing functionality and usability.[1]

3.6 SECURITY RESPONSE

3.6.1 SHR has established security response processes to minimize damage from IT Security Incidents see SHR policy: IT Security Incident Management. To monitor responses to Information Security Incidents and learn from such Incidents, audit trails and relevant Information will be collected for:

- Problem analysis;
- Use in arbitration, civil or criminal proceedings; and
- Negotiating for compensation from software and service providers, and other contractors.

3.7 ENTERPRISE DATABASE MANAGEMENT (excludes MS Access)

3.7.1 All enterprise database discrepancies such as lost records or potential security exposures will be reported to the SHR IT GRC group immediately.

3.7.2 IT GRC shall periodically verify that logical and physical database consistency checks have been performed.

3.7.3 Changes made to all enterprise databases shall be tracked in accordance with the SHR ITS Change Management processes.

4. ROLES AND RESPONSIBILITIES

4.1 SHR IT Governance, Risk, and Compliance (GRC)

4.1.1 Protect electronic information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction through the implementation, oversight, and monitoring of appropriate administrative, physical, and technical safeguards. This includes providing (or coordinating the provision of) associated expertise to other SHR business units, as well as conducting, overseeing, or contributing to investigations of IT security incidents; this includes, but is not limited to, actual or suspected violations of regional IT policies and IT standards.

4.1.2 Maintain centralized audit trails of SHR checks and controls, including those that are in place for information accesses, changes, additions, and deletions.

4.1.3 Perform periodic computer audits to ensure that software is licensed. Non-approved software shall be removed and reported to the IT GRC group.

4.2 Managers or designates

4.2.1 Ensure new systems/applications that are considered for SHR use are evaluated *prior to* purchase (see 3.1.3, above).

[1] SANS (SysAdmin, Audit, Network, Security) Institute (www.sans.org), “An Overview of Threat and Risk Assessment”

4.2.2 Ensure threat risk assessments are conducted of IT systems or services that store, transmit or process confidential information or face the public Internet when circumstances warrant (see 3.5 above).

4.2.3 Ensure that audit processes are developed and performed for the applications that their business unit owns.

4.3 **ITS and Business Unit IT System Support Personnel**

4.3.1 To the extent possible, utilize security controls, audit trails, and activity logs to monitor the resources of the IT systems that their business unit owns and operates (see 3.1.5, above).

4.3.2 Maintain either manual or automated system logs of their activities (see 3.1.6 above).

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 to this policy by SHR employees or employees of contractors providing services to SHR may lead to disciplinary action including dismissal if the breach is intentional, major or relates to Personal Health Information.

Non-SHR user organizations and application providers will be responsible for implementing similar non-compliance policies for their employees.

7. REFERENCES

Adopted from the eHealth Saskatchewan Security Policy Framework, section 10.10.1, Monitoring System Access and Use.

Appendix A – Issues to Consider When Conducting an IT System Threat Risk Assessment

IT systems or services that store, transmit or process confidential information (as defined by SHR's Information Classification, Labeling, and Handling policy) or face the public Internet require a threat risk assessment prior to their initial acquisition, prior to significant system upgrades, and periodically as the regulatory or threat landscape changes over time. *Many* factors need to be considered in order to understand potential threats to the availability, confidentiality, and integrity of an IT system and the information that it stores. Below is a *partial* list.

Conducting an IT Threat Risk Assessment requires specialized knowledge. If any of the questions below raise a red flag, or if you have any other threat or risk related questions or concerns, please contact SHR Information Technology Services for advice and assistance.

QUESTIONS TO ASK	POTENTIAL THREAT OR RISK
HARDWARE ARCHITECTURE	
Workstation Specifications What are the workstation specifications that are required for this particular system/application? Is there a preferred, or certified, list of manufacturers?	***Any new workstation manufactures may require significant effort for similar certification before the platform would be supported by the Health Region IT staff.*** *The Health Region's currently preferred vendor for PC workstations is Lenovo. The hardware platforms from this vendor have gone through extensive internal certification to confirm the Operating System configuration, hardware drivers, etc. work with the systems/applications that are run within the Health Region.*
Server Specifications What are the server specifications that are required for this particular system/application? Is there a preferred, or certified, list of manufacturers?	***Any new workstation manufactures may require significant effort for similar certification before the platform would be supported by the Health Region IT staff.*** *The Health Region's currently preferred vendor for servers is IBM for Windows, AIX, and Linux based servers and HP for Windows and HP/UX based server. Similar to the workstations above, the hardware platforms from these vendors have gone through extensive internal certification to confirm the Operating System configuration, hardware drivers, etc. work with the systems/applications that are run within the Health Region.*
High Availability What are the workstation and server design considerations to help improve availability of the system/application?	***It's important to understand what techniques are used by this system/application to improve the availability of its workstation and server infrastructure.*** *The Health Region network uses variety techniques to provide a highly available workstation and server infrastructure such as multiple power supplies, RAID, server link aggregation, etc.*
Additional Hardware Information Are there any other pieced of hardware equipment that are required as part of the system/application such as cameras, printers, workstation carts, UPS's, server racks, mobile devices, clinical devices, etc.?	***Deviation from pre-existing standards may cause integration issues or necessitate additional investment in infrastructure or software to manage the hardware properly.*** *For other pieces of hardware the Health Region may have existing standards that would be desirable to follow, such as Lexmark for printers, APC for racks and UPS's, etc. Specialized hardware (typically clinical devices) will need to be examined in detail to ensure that the device can be properly connected to the Health Region network and secured. As well it may need to be evaluated to ensure it fits within any facility constraints.*
NETWORK ARCHITECTURE	
Bandwidth Requirements What are the bandwidth requirements for the application?	***The Health Region has upwards of 80 sites, many of those located in rural communities where high-speed bandwidth is not available.*** *To know what the bandwidth requirements are between the different components such as workstations, database servers, web servers, etc. is*

	critical in predicting what the impact of the system/application will be to the available bandwidth and other systems/applications that may be already running.
SOFTWARE ARCHITECTURE	
Software Update Procedures What are the software update procedures for the operating systems and application?	***The health region has an ongoing program that requires servers to be kept up to date with security and stability related operating system patches.*** *Further, the Health Region has stringent change control procedures which are much easier to navigate if there is a documented update procedure for the application and operating systems that support this system/application.*
SYSTEM/APPLICATION ARCHITECTURE	
Data/Information Location Does the system/application store clinical data/information? Please identify the physical locations in which this data/information is stored. Does the application architecture store information in a separate location not managed by the Health Region, or on separate servers not managed by the Health Region? If so, please provide the location information, and security policies governing the protection of that information.	***In order to evaluate information privacy and security it's important to understand where the data/information is being stored in the system/application.*** *Adhering to national, provincial and municipal legislation necessitates that all data is kept within Canada and preferably within Saskatchewan. As well, if information is being transmitted over public or semi-trusted network infrastructure this may necessitate employment of encryption techniques like VPN.*
Availability What's the expected availability of the system? Have the user's been provided realistic expectations about the system availability considering the maintenance schedule and risk from single points of failure?	***In previous projects it's been the experience that users sometimes are not provide realistic availability information considering the system/application maintenance schedule and potential risks from any inherited by the designed infrastructure.*** *For example, advertising 100% availability for a platform where a server has a single power supply or has a single network connection is most likely not possible due to the inherit risks of the single-points of failure. If either the power supply or network switch failed the system/application would be unavailable.*
System/Application Health Warnings Does the system/application have the ability to monitor components or processes in its architecture and provide any warnings or alerts when there are issues affecting performance?	*It would be very advantageous if the system/application has the ability to monitor its components (like disk storage) or processes and warn the administrators of a potential issue prior to an actual failure.*
SECURITY ARCHITECTURE	
Privacy If the system/application has any identifiable patient information, has the Health Region Privacy department had an opportunity to inspect the system/application? Has a security impact analysis been performed to ensure compliance with Regional, Provincial, and National legislation with respect to privacy and protection	*The privacy and confidentiality of the people served by the Health Region is of paramount concern. Information in this area will show whether vendors know and understand the constraints to which the system/application must adhere to and whether adequate privacy protection techniques have been employed. Further, providing the privacy legislation to which the system/application are required to adhere to shows a level of maturity and expertise that goes a long way to demonstrate sound knowledge of privacy and confidentiality legislation as they apply from different regions of the World.*

of patient information (ie: HIPA (not HIPPA <- this legislation has to do with U.S. Insurance), PIPEDA). Please provide all international privacy legislation that is applicable to this system/application (ie: U.S. Patriot Act if Support services are being performed from or data is stored within the U.S., the German Data Protection Act – Bundesdatenschutzgesetz, etc.)	
Administrative and Service Accounts Do users of the system/application require administrative access to the workstation for it to function properly? Do any service accounts require static passwords?	***Systems/Applications that require users to have administrative access to the workstation are inherently insecure and demonstrate poor security practices.*** *Service or Vendor accounts that are unable to have periodic password changes yet have access to other portions of the Health Region network are a risk to the rest of the Regional systems.*
Authentication Can the system/application use the Health Region Active Directory domain for authentication and security? Does it require its own domain or is the authentication completely internal?	***There are advantages in leveraging the Health Region's Active Directory domain to limit the number of accounts that the user's need to manage.*** *If the system/application requires its own domain this may result in additional IT resources in order to manage and maintain the domain properly. Systems/Applications using internal user security may result in the users needing to manage yet another set of credentials. With the number of applications running within the Health Region the users already manage many security credentials; systems/applications that can leverage existing authentication mechanisms are advantageous.*
Monitoring & Logging Does the system/application record and retain audit information regarding user and system activity?	***From SHR's regional policy on IT Systems – Monitoring Access and Use:*** ***New systems/applications that are being considered for SHR use shall be evaluated prior to purchase to verify whether or not they are capable of meeting the standards for auditing, monitoring, and reviewing of system, network, and user activity as outlined in this policy.*** *This includes including relevant evaluation criteria in any associated RFPs. When in doubt, the services of SHR Information Technology Services or a reputable external contractor with expertise in this field shall be engaged for advice and assistance.* ***Legacy (existing) systems/applications that cannot conform to all SHR ITS monitoring and logging standards must meet as many as possible.*** *The responsible business unit must put all such systems/applications on an upgrade/replacement path such that these shortcomings are addressed as part of the next major release cycle.* *All systems/applications that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions must record and retain audit-logging information sufficient to determine:* • *the activity that was performed;* • *the account or system that performed the activity, including where or on what system the activity was performed;* • *the system the activity was performed on;*

	- *the time that the activity was performed;* - *the tools that were used to perform the activity;* - *the status (such as success vs. failure), outcome, or result of the activity.* *Security controls, audit trails, and activity logs must be used for IT resources during automated and manual processes. Monitoring of IT resources shall include, but is not limited to:* - *Creating, reading, updating, or deleting confidential information, including confidential authentication information such as passwords;* - *Creating, updating, or deleting information not covered in the first bullet point, above;* - *User authentication and authorization for activities covered in the first and second bullet points, above, such as user login and logout;* - *Controlling access to software that monitors or modifies network configurations or devices;* - *Equipment maintenance records of suspected or actual equipment faults and maintenance activities;* - *Fault logs and reports;* - *Internet use;* - *External network connections and remote access networks;* - *Entry control logs recording entry statistics (e.g., name, affiliation, date, and time, et cetera) to SHR IT Resources and data processing facilities;* - *Internet audit trails (where required);* - *The maintenance of synchronized clock settings;* - *Initiating a network connection;* - *Accepting a network connection;* - *Granting, modifying, or revoking access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;* - *System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;* - *Application process aborts, failures, or abnormal ends, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and* - *Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or antispyware system.*
IMPLEMENTATION AND DEPLOYMENT METHODS	
Scope Overlap with Other Projects To the best of your knowledge, are	***The Health Region provides systems/applications to many facilities and delivering services in a common manner across them is critical to supporting these processes and predicting work-flow.*** *Existing processes or functions may already exist across the Health Region that*

there functionality overlaps between this system/application and other systems/applications already running within the Health Region (ie: Digital dashboard displays, staff scheduling, and bed management)?	*are available within this new system/application, but unless this system/application is planned to be deployed throughout the Health Region it will be difficult to justify the use of a particular function if it is not available region-wide.*
OPERATIONS AND SUPPORT	
Disaster Recovery Plan Does the system/application have a documented disaster recovery plan? Do the business units depending on this system/application have business continuity plans in place for when it fails?	***A predefined DR plan helps to eliminate a huge amount of re-work, especially if the information is available at the planning-stage.*** *This could help to suggest placement of servers or other components to help enhance any DR plan.* *Business units that do not have a "down time plan" to cope with when their automated processes and systems fail are at significant risk.*
Disaster Avoidance Does the system/application have architectural components that aid in disaster avoidance or any recommended disaster avoidance plans?	*Analysis of these plans will help to evaluate if they fit within existing disaster avoidance plans and strategies.* ***If there are no architectural components or recommendations for disaster avoidance the Health Region will need to spend time to quantify the cost and likelihood of failure event as it relates to implementation and maintenance.*** *For example, if the server storage is not built in a RAID configuration, what is the impact to the Health Region when a hard drive fails?*
Multiple Instances Does the system/application come with one or multiple instances that could be used for pre-production activities like testing, certification, and training? *Can one of these instances be used for disaster recovery?*	*For larger systems/applications, the ability to have multiple instances running simultaneously is of great value. This way, activities which may affect performance of a production system (like those mentioned above) are run on a separate copy of the system/application.*
SUPPORT AND OPERATIONS	
Remote Access Support Is there a requirement for vendor Support Engineers to have remote access to the devices in the system/application?	*If there is a requirement for vendor remote access, please provide as much detail as possible on the preferred method including details such as (but not limited to),* • *The location of the Support Engineers.* • *What software is providing the remote access* • *What patient information is exposed during remote access activities* • *Authorization processes for remote access.* • *Network transmission paths and routes used for support activities* • *Techniques used to protect the remote access session* • *Privacy and security assessments.* ***Historically vendor access can be a contentious issue, especially when support is provided from outside of Canada. Ensuring adherence to any privacy legislation is critically important and often impacts vendor remote access.*** *The Health Region does have approved methods of remote access, so the information provided here will identify if those methods can be used.*