	POLICY Number: 7311-25-010 Title: IT Security Incident Management
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

OVERVIEW

This policy describes the manner in which Saskatoon Health Region (SHR) will identify, contain, investigate, notify, report and remediate IT Security Incidents.

Given the highly confidential nature of the information that SHR creates, transmits, and stores, SHR must be careful to restrict the flow of this information. When this information is compromised (or we suspect it has) a structured investigation and response based on best practices is vital to contain the damage, identify and address security vulnerabilities, and gather the information necessary to manage the incident.

SCOPE

This policy is written from the perspective of investigating the compromise of *electronic* information, which is under the jurisdiction of Information Technology Services. This policy is **not** applicable to the following:

- *Physical Security (e.g. employee safety, theft, vandalism)*
- *Privacy or Confidentiality Breaches* (discussed below), except in the context that such breaches may result from an IT Security Incident.
- *ITS Service Desk Incidents:* Service desk incidents follow the service desk reporting and remediation processes; any specific service desk incident may be escalated to – and resolved by – SHR's IT Security Incident Management process.

DEFINITIONS

Data means information stored in an electronic manner.

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 4.3, below.

IT Security Incident means any real or suspected event or action that could pose a threat to the integrity, availability, or confidentiality of SHR computer systems or computer networks.

Examples of activities that constitute an IT Security Incident include, but are not limited to:

- **Password compromised** – you discover that someone else has access to your account using your password, or others are misusing passwords.
- **Hacking attempt** – certain systems may disable accounts where the wrong password was entered four times. If your account was disabled because someone else was attempting to access it, then an IT Security Incident has occurred.
- **Computer virus infection** – virus infection that was not detected and cleaned automatically.
- **Computer files missing** – unexplained deletion of any file.
- **Unexplained changes to system data/configuration** – any unexplained change to data.
- **Theft/loss of IT equipment** – a theft or loss is an IT Security Incident if it means that information is lost or made available to others.
- **Unauthorized people using** or attempting to use IT equipment.
- **Unauthorized people gaining access** to protected IT areas.
- **New vulnerabilities and exploits** discovered in existing IT systems.
- **Violations** to other SHR IT policies

NOTE: *IT Security Incidents may result in a Privacy/Confidentiality Breach, discussed below.*

IT Security Vulnerability means a weakness in the design, implementation, operation or internal controls of a process or IT system or service that could be exploited to violate system security.

Phishing means a type of fraud or scam whereby a user is sent an unsolicited but legitimate-looking email that appears to come from a well-known and trustworthy web site or company; this email asks for personal information, financial information or user account credentials (i.e. username & password). The sender of these emails is "fishing" for information that can be used for identity or financial theft, or to acquire unauthorized access to online systems or information. Most such emails attempt to create a sense of urgency, and many provide the user with something to click on (e.g. a link to a fake site designed to mimic a company's legitimate web site).

Privacy/Confidentiality Breach means the unauthorized collection, use, disclosure or disposal *of personal health information*. Activities are considered "unauthorized" if they contravene any provision of The Health Information Protection Act (HIPA). Although breaches can be intentional or unintentional, the majority of breaches take place inadvertently.

Examples of activities that constitute a Privacy or Confidentiality Breach include, but are not limited to:

- Looking at a family member's chart to see how they are doing

- Talking about patients with friends outside of work
- Misplacing a file folder containing personal health information.
- Confidential material unsecured in a public area
- An employee not logging off a patient information database when away from his/her computer.

Privacy/Confidentiality breaches must be reported to SHR's Privacy Office. For more information on how to report a breach, as well as recommended actions that should be taken based on the breach's severity, see Departments >> Privacy & Access >> Breach Reporting on the SHR InfoNet.

SHR staff means employees, affiliate employees, practitioner staff, professional staff, students and contractors.

Spam means irrelevant, inappropriate, and/or unsolicited electronic mail messages sent on the Internet, usually to large numbers of recipients and often with the purpose of soliciting new business.

1. PURPOSE

The purpose of this policy is to:

1.1. Provide a policy framework for responding to IT Security Incidents in accordance with legislative and policy requirements;

1.2. Prepare employees and contractors to recognize and acknowledge when an IT Security Incident has occurred;

1.3. Create a single point of contact for the investigation and management of all IT Security Incidents in order to avoid miscommunications; secondary points of contact will be used where sensitivity require it.

1.4. Enhance SHR's reputation through the use of a professional approach in quickly resolving and appropriately communicating IT Security Incidents when they occur.

2. PRINCIPLES

2.1. SHR incorporates privacy protection and accountability for privacy into all aspects of its operations, to ensure that every program and project complies with applicable legislation, including *The Health Information Protection Act* (HIPA) and *The Local Authority Freedom Of Information and Protection of Privacy Act* (LA FOIP).

2.2. Administrative, technical and physical safeguards are required to protect personal health information against theft, loss and unauthorized access to or use, disclosure or modification of the information.[1]

3. POLICY

3.1. All actual, potential or suspected IT Security Incidents will be reported and responded to based on SHR's IT Security Incident Management Framework (see procedure).

[1] HIPA s.16.

3.1.1. All SHR staff will inform their immediate managers of any observed, potential or suspected IT Security Incidents, vulnerabilities, or threats to systems or services provided by SHR as quickly as possible. If management is not available, staff are to contact the ITS Service Desk with this information

3.1.2. Managers or supervisors (or, if not available, the reporting individual) will immediately submit an IT Security Incident Report form (see Appendix B) when an actual, potential, or suspected IT Security Incident occurs.

3.1.3. **Emergencies**

If an IT Security Incident's impact is anticipated to be serious or critical, or timely response is required, the incident reporter or their manager shall contact ITS Service Desk directly. *If in doubt, call the ITS Service Desk.*

3.1.4. All SHR staff will contact the ITS Service Desk with any information regarding software malfunctions or support issues. Staff can also report phishing attempts or spam (see Definitions, above) directly to the ITS Service Desk. (In both cases, an IT Security Incident Report form is not required.)

3.2. All IT Security Incidents will be documented (logged and tracked) by the designated triage officer for the purposes of:

- Protecting the safety of individuals;
- Protecting information assets (i.e. sensitive and personal/personal health information) of the organization and individuals;
- Quality improvement; and
- Limiting and mitigating enterprise risk.

3.3. Under no circumstances will parties not explicitly authorized by ITS attempt to prove a suspected IT security vulnerability, as this could result in potential damage to the confidentiality, integrity, or availability of the system or its data.

4. ROLES AND RESPONSIBILITIES

4.1. All Staff

4.1.1. Be aware of possible IT Security Incidents or policy violations and report them to their own supervisor, or to the supervisor of the employee who may have been involved with the incident. If management is not available, they are to contact the ITS Service Desk with this information.

4.2. Directors, Site Leaders and Managers

4.2.1. Refer users to published materials and elearning to assist with interpretation of SHR policies as they relate to security of information technology resources. If further clarification is required, contact SHR's IT GRC group.

4.2.2. Assess whether a violation has occurred. Consult with the following on their decision:

- SHR's IT GRC group

- The manager of SHR's ITS Service Desk
- SHR'S Human Resources service team

4.2.3. Responsible/accountable for implementing recommendations that result from an incident investigation

4.3. **SHR IT Governance, Risk and Compliance (GRC)**

4.3.1. Provide technical support to confirm if an information technology resource has been accessed inappropriately, and assist in identifying and implementing technical options to prevent subsequent violations and security exposures.

4.3.2. Completes an IT Security Incident Report form outlining details of the incident and their suggestions to mitigate future risk.

- Once complete, this form will be signed by the appropriate Director along with the Incident Manager.
- The form will then be filed with SHR's IT GRC group for future reference.

4.3.3. 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.

4.3.4. Provide (or coordinate the provision of) associated expertise to other SHR business units, as well as conduct, oversee, or contribute to investigations of IT Security Incidents; this includes, but is not limited to, actual or suspected violations of regional IT policies and IT standards.

4.4. **Triage Officer**

4.4.1 Assesses whether an IT Security Incident warrants further investigation. If yes, appoints an Incident Manager (below).
4.4.2 Leads investigations regarding suspected or confirmed IT Security Incidents and vulnerabilities, including policy compliance.
4.4.3 Tracks completion of recommendations resulting from an investigation

4.5. **Incident Manager**

4.5.1. Acts as a single point of contact for ITS.
4.5.2. Takes immediate steps to contain/reduce the impact of any IT Security Incident
4.5.3. Leads investigations regarding suspected or confirmed IT Security Incidents and vulnerabilities, including policy compliance.

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 may result in disciplinary action up to and including termination of employment and or privileges if the breach is intentional, major or relates to Personal Health Information.

Human resources will assist with interpretation and application of SHR's policies and processes relating to investigating and addressing behaviour or work performance issues. However, violations of SHR's IT Policies shall be addressed by a user's manager in a manner similar to other types of unacceptable behaviour or work performance issues.

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 13.1, Reporting Privacy and Security Incidents.

Other regional policies that apply to employees who have access to SHR's information technology resources include:

- 7311-30-001 Respect And Dignity
- 7311-10-002 Fraud and Irregularity
- 7311-30-005 Conflict of Interest
- SHR InfoNet:
    - Manager Resources >> Performance Management
    - Human Resources >> Resources >> Corrective Discipline

PROCEDURE Number: 7311-25-010 Title: IT Security Incident Handling	
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

1. PURPOSE

The purpose of this procedure is to:

1.1. Establish the process for reporting IT Security Incidents and vulnerabilities.

1.2. Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation and ongoing management and reporting of IT Security Incidents.

2. PROCEDURE

2.1 It is the responsibility of all individuals who witness, discover or are involved in actual, suspected, or potential IT Security Incident to immediately advise his/her manager or supervisor of the incident.

2.1.1 If unable to reach a manager or supervisor immediately, the individual who identifies an incident contacts the ITS Service Desk.

2.2 The reporting individual or their manager or supervisor will then immediately submit an IT Security Incident Report form (see Appendix B).

2.3 The designated Triage Officer within SHR IT GRC (either the Manager of IT GRC or their delegate) will determine if the IT Security Incident requires further investigation:

2.3.1 If yes, then an Incident Manager will be appointed, as discussed below.

2.3.2 If no, the IT Security Incident will be logged and no further action will be taken.

2.4 The Triage Officer will appoint an Incident Manager to lead the investigation and act as a single point of contact. (The Incident Manager and the Triage Manager may be the same person).

2.4.1 Each incident response will address:

- Identification
- Containment

- Eradication
- Recovery
- Follow-up

2.5 The Incident Manager will take immediate steps to contain/reduce the impact of any IT Security Incident.

2.6 Beyond any immediate containment steps, the Incident Manager will determine the appropriate containment measures to address the particular incident, as well as to prevent similar incidents from occurring, by following SHR's IT Security Incident Management procedures.

2.7 The Incident Manager leads the investigation.

2.7.1 If facts are received during the investigation that change the nature of the incident to include more than one type of incident (e.g. Privacy & Compliance, Human Resources), the Incident Manager will transfer the lead to the Director of Enterprise Risk Management to involve departments or individuals from other areas but will continue to maintain the role of Incident Manager and single point of contact for the information technology aspects of that incident.

2.7.2 If criminal activity is suspected, the incident is referred to the Vice President in charge of SHR's Enterprise Risk Management department for escalation (or, in the absence of this VP, the Director of Information Technology Services/ also known as Chief Security Officer.

2.8 Incident Managers will utilize SHR's Emergency Preparedness Plan's (EPP's) existing Incident Command Activation Triggers to determine if the situation is critical enough to activate SHR's Health Incident Command System (HICS).

2.8.1 If assistance is required (including coordinating with others and mobilizing resources the Incident Manager sets up a determination meeting with key personnel (for example, SLT On Call, EPP On Call, Rural Admin On Call, Site Leader, OLT On Call, Managers On Call) to discuss potential activation of HICS. Determination meetings can occur in person or by teleconference.

2.8.2 For further information, see Departments >> Emergency Preparedness >> Health Incident Command System on the SHR InfoNet.

2.9 Reporting and Recommendation

2.9.1 Upon completion of the investigation, a report and recommendation will be completed by the Incident Manager and will be completed and copied to the designated Triage Officer and (if/as appropriate) the associated business unit.

2.9.2 The appropriate business unit will be responsible for the implementation of any recommendations.

2.9.3 Recommendations are tracked for completion and reporting by the designated Triage Officer.

2.10 Notification

2.10.1 The determination to notify individuals or organizations outside of SHR will be handled by the Incident Manager; all external notifications are subject to the approval of the Director of Communications.

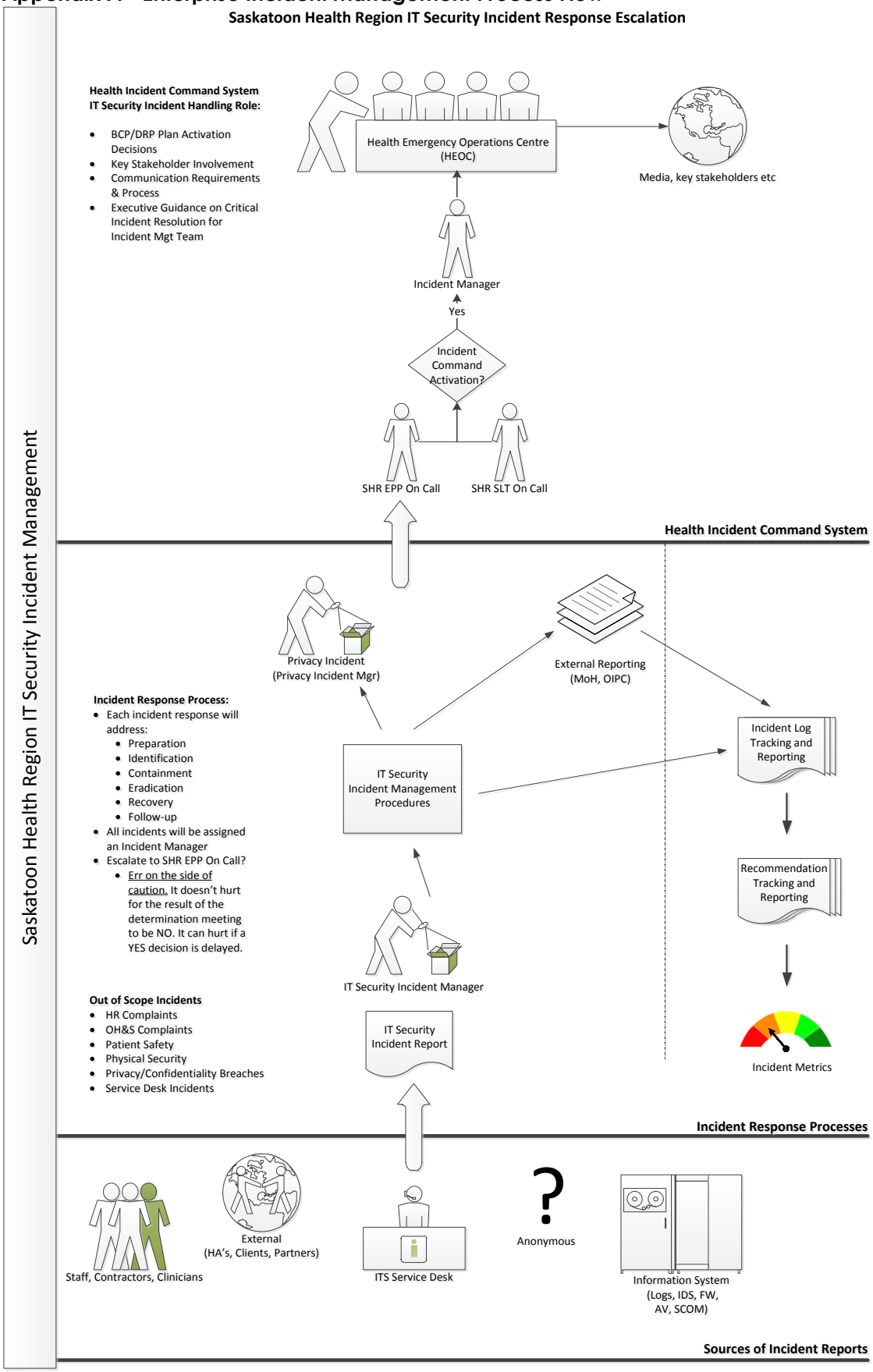
3. PROCEDURE MANAGEMENT

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

4. NON-COMPLIANCE/BREACH

Non-compliance with this procedure may in disciplinary action up to and including termination of employment and/or privileges the breach is intentional, major or relates to personal health information.

Appendix A - Enterprise Incident Management Process Flow



Appendix B - SHR IT Security Incident Report

Please fill in the following details as completely as possible

Date of Report	

PERSON REPORTING THE INCIDENT

Name		**Title**	
Organization			
Department			
Phone		**Cell**	
Email Address			

INCIDENT INFORMATION

Date and Time Incident OCCURRED:	
Date and Time Incident DETECTED:	

Type of Incident: *(check as many as apply)*

- ☐ Unauthorized/improper use
- ☐ Unauthorized Access
- ☐ Computer security hack/attack
- ☐ Breach of regional policy (specify):
- ☐ Other(specify):
- ☐ Theft/loss of laptop or mobile device
- ☐ Theft/loss of portable storage
- ☐ Illegal/improper software

Location where the incident occurred?

Briefly describe the nature/cause of the incident (e.g. facts and physical findings):

How was the incident discovered?

Location where the incident was detected from (if different from where it actually occurred):

Was the appropriate supervisor/manager advised of the incident?*

YES ☐ NO ☐ N/A ☐

***Note: To the extent possible, the reporting individual should immediately advise his or her supervisor/manager of the incident. If the supervisor/manager is not available, the reporting individual is responsible for reporting the incident directly to the ITS Service Desk.**

Please list the names and units of any other SHR staff involved in the incident.

Has the incident been contained? YES ☐ NO ☐ UNSURE ☐

Please describe in detail (e.g. include the who, what, where, when, why and how) any immediate steps taken to contain/reduce the harm of the incident:
(e.g.: locks changed, computer systems shut down, processing stopped, etc.)

IT Applications or Services involved: (e.g. Enovation, PACS, Email)

Technology/Equipment Involved: (e.g. local printers, electronic reader boards, laptops, fax, etc.)

Describe below the types of information involved:
(e.g.: name, address, HSN, personal health information, budget information, etc.)

Was there (or could there have been) personally identifiable information/personal health information included in or affected by the incident?

Personally Identifiable Information ☐ Personal Health Information ☐

"Personally Identifiable Information" (PII) is information about an identifiable individual. It includes, for example, a person's name, address, social insurance number or other identities, financial details or other information about the individual. "Personal Health Information" (PHI) includes information about one's physical or mental health and/or information gathered in the course of receiving a health service from a trustee.

Additional Information: *(Please attach additional pages if needed)*

Once completed please submit this form to:

Attention: IT Governance, Risk & Compliance
Saskatoon Health Region
701 Queen Street, 2nd floor
Saskatoon, SK S7K 0M7
Email: ITSSI@saskatoonhealthregion.ca