

**INTERNAL ONLY**  
**ISLHD POLICY**  
**COVER SHEET**



<b>NAME OF DOCUMENT</b>	Security Incident Management
<b>TYPE OF DOCUMENT</b>	Policy
<b>DOCUMENT NUMBER</b>	ISLHD CORP PD 59
<b>DATE OF PUBLICATION</b>	August 2019
<b>RISK RATING</b>	Low
<b>REVIEW DATE</b>	August 2024
<b>FORMER REFERENCE(S)</b>	None
<b>EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR</b>	ISLHD Chief Information Officer
<b>AUTHOR</b>	Program Manager ICT Security & Strategy
<b>KEY TERMS</b>	Information security, policy, standard, confidentiality, integrity, availability, privacy, classification, electronic information, compliance
<b>FUNCTIONAL GROUP OR HUB</b>	District Policies
<b>NSQHS STANDARD</b>	Standard 1
<b>SUMMARY</b>	This document provides the principles and guidance in responding to an Information Security Incident at the Illawarra-Shoalhaven Local Health District.

**COMPLIANCE WITH THIS DOCUMENT IS MANDATORY**

This document is the intellectual property of Illawarra Shoalhaven Local Health District. Content cannot be duplicated without permission.

Feedback about this document can be sent to: [ISLHD-CorporateGovernance@health.nsw.gov.au](mailto:ISLHD-CorporateGovernance@health.nsw.gov.au)

---

**Security Incident Management**

**ISLHD CORP PD 59**

---

**1. POLICY STATEMENT**

Illawarra-Shoalhaven Local Health District (ISLHD) has a regulatory obligation in relation to the management of information security incidents. Information security incidents are to be reported to the LHD executive and incident management must meet approved practices.

The Security Incident Management Policy is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

This ensures that when an incident occurs, swift mitigation and remediation ensues minimising the damage caused to ISLHD and its stakeholders.

**2. AIMS**

The purpose of the Security Incident Management Policy is to provide the principles and controls used to manage information security incidents.

This policy applies to all members of ISLHD who manage digital systems, including industrial automation and controls systems (IACS) and medical devices.

Assistance and guidance can be sought by contacting Health ICT (HICT) by logging a call with the eHealth State Wide Service Desk (SWSD) or via [SARA](#).

**3. TARGET AUDIENCE**

This Policy applies to all parties including permanent, temporary and casual staff of Illawarra-Shoalhaven Local Health District, staff seconded from other organisations and contingent workers including labour hire, service providers, professional services contractors and consultants, who may utilise ISLHD digital infrastructure and/or access ISLHD systems and applications (including systems provided by external providers such as eHealth) with respect to the security and privacy of information.

**4. INFORMATION SECURITY INCIDENT SCOPE**

Information security incidents must be reported promptly to the eHealth State Wide Service Desk (SWSD) and responded to in a quick, effective and orderly manner in order to reduce the negative effect of the incident, to mitigate the damage, inform policy and mitigate future risks.

Managers of digital systems must ensure that all staff that are called upon to respond and support an incident, be made aware of their roles and responsibilities prior to an incident occurring.

Key information about information security incidents, including the impact of the incident (financial or otherwise), must be formally recorded and the records must be analysed in order to assess the effectiveness of information security controls. The following principles must be adhered to so that incidents and risks are managed appropriately.

- New risks identified as a result of an incident must be assigned to the relevant risk owner and unacceptable risks must be mitigated promptly.

---

## Security Incident Management

## ISLHD CORP PD 59

---

- Staff that are called upon to respond to an Information Security Incident procedure must be trained in digital evidence collection, retention, and presentation, in accordance with Federal and State legislative or regulatory obligations.
- Incidents that are considered serious must be reported to the appropriate external authorities where relevant by authorised individuals. A serious incident is defined by the impact to the business as outlined in the [NSW MoH Risk Matrix](#) and by the [Office of the Australian Information Commissioner \(OAIC\)](#) data breach scheme.

### 4.1 Responsibilities

The identification and designation of responsible staff for systems managed for ISLHD ICT shall be the responsibility of the ISLHD CIO or delegate and for systems that are self-managed, by the department manager including systems that are operated on behalf of departments by vendors or managed service suppliers.

#### Department Manager

The department manager is accountable for;

- a) Development and implementation of a Security Response Plan (SRP);
- b) Management oversight of the response team during an information security incident;
- c) Engaging of Health ICT (HICT) to assist during the incident;
- d) Management of the collaboration between the response team for the department(s), and
- e) Issuing communications of the systems status during an incident.

A department manager may delegate some of all of the responsibilities during an incident.

#### Team Responsibilities;

The response team is accountable for;

- a) Execution of the Security Response Plan (SRP) to incidents that are identified as having a security component; and
- b) Co-ordination and collaboration with members of their department and HICT to resolve the incident.

#### ISLHD Staff and Contractors Responsibilities

The following are the minimum set of responsibilities and controls regarding incidents involving digital systems;

- a) All staff of ISLHD are responsible for reporting actual or suspected Information Security Incidents to the eHealth State Wide Service Desk as soon as possible.
- b) Contractors using the ISLHD's information systems and services must note and report any significant information security weaknesses in those systems or

---

## Security Incident Management

## ISLHD CORP PD 59

---

services that they become aware of. A call can be logged with the eHealth State Wide Service Desk.

- c) The responsibility and actions for responding to information security incidents must be as set out in an Information Security Incident Management Procedure regardless of whether they are locally managed or by HICT.
- d) The responsibility for reporting serious information security incidents to external authorities lies with the Senior Information Risk Owner unless otherwise delegated. As serious incident is determined by using the [NSW Ministry of Health Risk Management Policy and Framework - PD2015\\_043](#).

### 4.2 Compliance

Compliance with this policy should form part of any contract with a third party that may involve access to ISLHD networks or digital systems. Failure by contractors to comply with Section 4.1 of this policy may constitute an actionable breach of contract.

### 4.3 Contact Information

The Security Response Plan (SRP) must include contact information for dedicated team members to be available during non-business hours, should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to the department. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

### 4.4 Triage

The SRP must define triage steps to be coordinated with the security incident management team with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

### 4.5 Identified Mitigations and Testing

The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

### 4.6 Mitigation and Remediation Timelines

The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to department, District and staff. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

## 5. DOCUMENTATION

The following documents may assist in providing guidance with digital systems incident management.

- [Information Security Policy - ISLHD CORP PD 38](#)
- [HICT Incident Management Procedure](#)

---

## Security Incident Management

## ISLHD CORP PD 59

---

- [HICT Critical Incident Procedure](#)

### 6. EXEMPTIONS

Any exemptions to the Security Incident Management policy must be approved by the Chief Information Officer (CIO) or HICT Deputy Director after undergoing a risk assessment. Written approval for exemption must be completed through a Brief and must be recorded within the Document Management System (i.e. Content Manager) as per the ISLHD Records Management Standard.

### 7. DEFINITIONS

#### Information Security Incident

An Information Security Incident is the occurrence or development of an unwanted or unexpected situation which indicates either of the following:

- A possible breach of an information security framework policy; or
- A failure of information security controls which have a probability of compromising department operations.

Examples of information security incidents include (but are not limited to):

- Direct loss or theft of Classified Information (e.g. loss of a USB or thumb drive, unauthorised download of data);
- Loss or theft of equipment used to store Classified Information (e.g. laptop, smartphone, USB stick);
- Accidental or unauthorised disclosure of 'Confidential' or 'Highly Confidential' Classified Information (e.g. via misaddressed email correspondence or incorrect system permissions/filter failure);
- Corruption or unauthorised modification of vital records (e.g. alteration of master records);
- Computer system or equipment compromise (e.g. virus, malware, denial of service attack);
- Compromised IT user account (e.g. spoofing, hacking, shared password); or
- Break in at a location holding Classified Information or containing critical information processing equipment such as servers.

A serious Information Security Incident is an incident whose impact, if unmanaged, has the potential to reach moderate or above on the Risk Measurement Criteria in the [NSW Ministry of Health Risk Management Policy and Framework - PD2015\\_043](#).

Classified Information is information that is confidential, highly confidential or requires enhanced protection to ensure integrity or availability due to its nature. Further explanations of these classifications can be found in ISLHD's Data Information Classification policy.

---

**Security Incident Management**

**ISLHD CORP PD 59**

---

**8. AUDIT**

The NSW Government has mandated via the [NSW Government Cyber Security Policy](#) that audits are to be conducted annually and the outcomes of the audit be reported to the district CIO where a risk assessment can be conducted on the non-compliances to determine the mitigation actions.

**9. REFERENCE DOCUMENTS**

The following documents are referenced in this policy:

**Legislation, Policies and Guidelines**

- [Information Security Policy – ISLHD CORP PD 38](#)
- [NSW Government Cyber Security Policy](#)
- [NSW Ministry of Health Policy Directive PD2013\\_033 - Electronic Information Security Policy – NSW Health](#)
- [NSW Ministry of Health Risk Management Policy and Framework - PD2015\\_043](#)

**9.1 Standards**

- ISO/IEC 27035:2016 Information technology - Security Techniques - Information Security Incident Management
- [NIST Special Publication 800-61 Rev 2 Computer Security Incident Handling Guide](#)
- ISO/IEC 27001:2013 Information Technology - Security Techniques - Information Security Management Systems
- ISO/IEC 27002:2013. Information Technology - Security Techniques - Code of Practice for Information Security Management
- ISO/IEC 31000 Risk Management - Principles and Guidelines

**10. Revision & Approval History**

Date	Revision	Author	Approval
February 2019	0	Program Manager ICT Security & Strategy	<b>Approval/Date:</b> ISLHD Chief Information Officer
July 2019	0	Program Manager ICT Security & Strategy	<b>Approval/Date:</b> Corporate Policy Recommendation Committee - July 2019
August 2019	0	Program Manager ICT Security & Strategy	<b>Approval/Date:</b> ISLHD Chief Information Officer – August 2019