1. Statement

The Director-General of the Department of Health or their specified delegate and the Hospital and Health Service (HHS) Chief Executive or their specified delegate, may authorise monitoring of an employee’s email account where there are concerns about the security or compliance with the email account.

The Director-General of the Department of Health or their approved delegate and the HHS Chief Executive or their approved delegate, may authorise access to an employee’s email account where access to the employee’s email account is required for operational reasons.

2. Scope

Compliance with this standard is mandatory.

Email use shall be compliant with the law, including legislation, whole-of-government policy, Department of Health policy, HHS policy or the Code of Conduct for the Queensland Public Service.

This standard applies to all employees, contractors, consultants, agency staff, locums, students and volunteers within the Department of Health divisions, HHSs, agencies and commercialised business units and in this document, the term ‘employee’ applies to these people.

Hospital and Health Services and the Department of Health are custodians of records that contain information. HHSs and the department have obligations under the Public Records Act 2002 in relation to managing the records in each of their custodies. Irrespective of the entity that is the custodian of the records, the State owns the records and the Director-General is the agent of the State for the purpose of controlling those records. The Director-General can direct the HHSs to give access to departmental employee email accounts.

This standard applies to employee emails ‘accessible’ to the ‘intended recipient’ under the Telecommunications (Interception and Access) Act 1979 (Cth).

This standard does not address automated electronic scanning of emails sent to Queensland Health email addresses for the purposes of performing ‘network protection duties’ under the Telecommunications (Interception and Access) Act 1979 (Cth). Examples of this could include scanning for viruses, security threats or flooding attacks and inappropriate content such as pornography, sexually explicit or obscene material.

3. Requirements

3.1 Employee email monitoring

Where there are concerns in relation to a Department of Health or HHS employee’s email account about security or compliance with the law, including legislation, whole of government policy, Department of Health policy, HHS policy or the Code of Conduct for the Queensland Public Service, all requests for manual monitoring of the employee’s email account must be authorised by the Director-General Department of Health or the HHS Chief Executive or their specified delegate prior to the monitoring occurring.

Specified delegates are:

- Department of Health Chief Human Resources Officer
- Department of Health Chief Legal Counsel
- HHS Executive Member nominated by the HHS Chief Executive
• ‘Health service investigators’, as defined in the Hospital and Health Boards Act 2011, appointed under an instrument of delegation authorising the activity in relation to the investigation.

The authorisation for email monitoring is to be issued by the Director-General Department of Health or the HHS Chief Executive, or their specified delegate, to Integrated Application Services. The authorisation is to be in writing or by way of email.

3.2 Reporting concerns about employee email use and content

Where there are concerns in relation to a Department of Health employee’s email account about security or compliance with the law, divisional human resources representatives, the Chief Human Resources Officer, the Chief Legal Counsel or Ethical Standards Unit are the appropriate contacts for supervisors and managers.

Where there are concerns in relation to a HHS employee’s email account about security or compliance with the law, HHS human resources representatives and the HHS Executive Member nominated by the HHS Chief Executive are the appropriate contacts for supervisors and managers.

In relation to considering whether use is authorised or unauthorised, the Use of ICT Services Standard has examples of authorised and unauthorised conduct.

3.3 Email access for operational reasons

Where access is required to a Department of Health employee’s email account for operational reasons, other than email monitoring for security or compliance, the request for access to the employee’s email account must be authorised by the Director-General Department of Health or approved delegates.

Approved delegates for the Department of Health are those persons performing the function and duties of the roles so listed in the Department of Health HR Delegations Manual August 2015 (or as amended from time to time) at a level Band 5 delegation or above.

Where access is required to a Hospital and Health Services employee’s email account for operational reasons, other than email monitoring for security or compliance, the request for access to the employee’s email account must be authorised by the HHS Chief Executive or their approved delegate determined at the HHS level.

The authorisation for email access is to be issued by the Director-General Department of Health or the HHS Chief Executive, or their approved delegates, to Integrated Application Services. The authorisation is to be in writing or by way of email.

Operational reasons may include, but are not limited to, when an officer is on leave or absent from the workplace and arrangements for on-forwarding or referring incoming emails are not in place (usually unplanned leave); when an officer has separated from Queensland Health; or in accordance with any requirement of law.

A staff member email account may contain ‘personal information’ as defined in the Information Privacy Act 2009 (IP Act). Any person authorised to access a staff member’s email account must ensure they do so in accordance with the requirements of the National Privacy Principles (NPPs) contained within the IP Act. The NPPs are rules about how the department must handle all personal information including the collection, storage, use and disclosure of personal information.

4. Legislation

• Telecommunications (Interception and Access) Act 1979 (Cth)
• Telecommunications Interception Act 2009
• Public Records Act 2002
• Information Privacy Act 2009
5. Supporting documents

- *Email monitoring and the Telecommunications (Interception and Access) Act guideline*
- *Use of ICT Services policy*
- *Use of ICT Services standard*
- *Queensland Government Information Security Classification Framework*
- *Code of Conduct for the Queensland Public Service*

6. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved delegate</td>
<td>Is the delegate approved to authorise the monitoring of an employee’s email account where there are concerns about the security or compliance with the email account</td>
</tr>
<tr>
<td>Email</td>
<td>Electronic mail (email)</td>
</tr>
<tr>
<td>Email Monitoring</td>
<td>Scanning, accessing, reading or otherwise determining the content of email sent to or from an email account other than by way of automated scanning for the purposes of performing ‘network protection duties’ under the <em>Telecommunications (Interception and Access) Act 1979</em> (Cth).</td>
</tr>
<tr>
<td>Specified delegate</td>
<td>Is the delegate specified to approve access to an employee’s email account for operational purposes</td>
</tr>
</tbody>
</table>

7. Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>16/09/2015</td>
<td>Director-General approval</td>
</tr>
<tr>
<td>1.1</td>
<td>10/05/2016</td>
<td>Director-General approval</td>
</tr>
</tbody>
</table>