# POLICY

## Computer Surveillance Policy

### Purpose
To detail the circumstances in which computer surveillance could be undertaken at Macquarie University.

### Overview
Computer surveillance is a tool that Macquarie University will use from time to time as defined by the [Workplace Surveillance Act 2005](http://www.mq.edu.au/policy/docs/comp_surveillance/policy.html) (‘the Act’). Section 12 of the Act prohibits an employer from carrying out computer surveillance of its employees at work unless it is carried out in accordance with a policy on computer surveillance. This Policy must be notified to employees in advance in such a way that it is reasonable to assume that the employee is aware of and understands the Policy.

Adopting and promulgating this Policy constitutes the provision of the notice under the Act.

**DEFINITION**
**Computer Surveillance**: surveillance, including by means of software or other equipment, that monitors or records the information input or output, or other use, of a computer (including, but not limited to, local or hard drive, public network, internet and email and other electronic technologies).

### Scope
The policy applies to all employees, contractors, consultants and visitors who are given access to the University's computer systems.

### Policy
The University will conduct ongoing and intermittent computer surveillance for the purposes of:
- protecting its assets, property and finances from suspected unlawful activity or activities which are in breach of University policy or Rules
- its business and operational requirements
- protecting its reputation
- compliance with legislative requirements
- meeting the expectations of its stakeholders and the general public

**AUTHORISATION**
The Director, Human Resources (HR) and the Chief Information Officer (CIO) are both authorised to conduct computer surveillance. Joint approval must be given before surveillance can proceed. Either officer can delegate authority to another senior officer.

An information technology (IT) user can agree to computer surveillance being undertaken.
METHOD OF SURVEILLANCE
Computer surveillance will be carried out by all means available to the University which can include:

- accessing University email accounts or emails
- accessing files
- accessing work computers, including computer activity logs
- recording internet usage (including sites and pages visited, files downloaded, video and audio files accessed and data input)
- and accessing these records

BLOCKING EMAILS, INTERNET ACCESS OR SOFTWARE APPLICATIONS
Computer surveillance may prevent, or cause to be prevented:

- delivery of an email sent to or by an IT user
- access to an internet website
- access to software applications

The IT user will be notified of any email that has not been delivered as soon as practicable. The exception is where:

- the email was a commercial electronic message within the meaning of the *Spam Act 2003* (Cth)
- the content of the email or any attachment to the email would or might have resulted in an unauthorised interference with, damage to or operation of a computer or computer network operated by the employer or of any program run by or data stored on such a computer or computer network
- the email or any attachment to the email would be regarded by reasonable persons as being, in all circumstances menacing, harassing or offensive, or
- the University was not aware (and could not reasonably be expected to be aware) of the identity of the IT user who sent the email or that the email was sent by an IT user

The University will not prevent, or cause to be prevented, delivery of an email or access to a website merely because:

- the email was sent by or on behalf of an industrial organisation of employees or an officer of such an organisation or
- the website or email contains information relating to industrial matters [within the meaning of the *Industrial Relations Act 1996* (NSW)].

USE OF INFORMATION MONITORED AND COLLECTED
The Director, HR, or the CIO can authorise any person to analyse computer activity or computer surveillance records obtained in accordance with this Policy, unless:

- there is reasonable cause to suspect misconduct or serious misconduct, or
- there is agreement to the use of the computer surveillance records for a documented and agreed purpose (such as assessing the workload).
COMPLIANCE AND BREACHES
The University may commence applicable disciplinary procedures if a person to whom this policy applies breaches this policy (or any of its related procedures).

<table>
<thead>
<tr>
<th>Contact Officer</th>
<th>Risk Manager, Information Technology Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Approved</td>
<td>22 July 2010</td>
</tr>
<tr>
<td>Approval Authority</td>
<td>Deputy Vice-Chancellor and Chief Operating Officer</td>
</tr>
<tr>
<td>Date of Commencement</td>
<td>22 July 2010</td>
</tr>
<tr>
<td>Amendment Dates</td>
<td>September 2011 – clarification to authorisation required for analysis of surveillance records</td>
</tr>
<tr>
<td>Date for Next Review</td>
<td>July 2013</td>
</tr>
<tr>
<td>Policies/Rules Superseded by this Policy</td>
<td>Computer Surveillance Policy (ITS004) – 22 March 2007</td>
</tr>
<tr>
<td>Keywords</td>
<td>Computer, Surveillance, Workplace, Email, Electronic</td>
</tr>
</tbody>
</table>