Monash University Procedure

Procedure Title	Electronic Information Security: Callista Access Procedures
Parent Policy	Electronic Information Security Policy
Date Effective	12-September-2012
Review Date	12-September-2015
Procedure Owner	Chief Information Officer
Category	Operational
Version Number	1.0
Content Enquiries	eSolutions Service Desk
Scope	All campuses in Australia Monash South Africa Monash College Pty Ltd All staff All students
Purpose	Access to the electronic information system (Callista) which stores and processes student personal and academic information is controlled by these procedures.
PROCEDURE STATEMENT	

1. Delegation of Authority

The Chief Information Officer delegates authority to the Director, Student and Education Business Services, to manage Callista Access Security procedures.

Responsibility

Chief Information Officer

2. Authorising access

2.1. Authorised Signatories

- The Director, Student and Education Business Services, will determine a list of delegated signatories who will assume responsibility for the authorising and auditing of appropriate access within their own areas of responsibility.
- Delegated signatories may apply to the Director, Student and Education Business Services, requesting additional signatories, which may be approved at the Director's discretion.
- Delegated signatories are responsible for validating and approving the request for access. As such they assume responsibility for ensuring that the access is appropriate and that the staff member is fully aware of their responsibilities in being granted access to the system.

- The Director, Student and Education Business Services, will provide the Callista Service Desk with the list of the Callista functionality (role/s) and location/s each delegated signatory can approve, and will provide an updated list when there are any amendments to the list of delegated signatories.
- The Callista Service Desk will publish and maintain the list of delegated signatories on the Callista signatory list website.
- A copy of the signatures of the Chief Information Officer, the Director, Student and Education Business Services, and the delegated signatories will be held at the Callista Service Desk.
- Delegated signatories will not be permitted to authorise access for themselves.
- Callista access for the Director, Student and Education Business Services will be authorised by the Chief Information Officer.

Responsibility

Chief Information Officer
Director, Student and Education Business Services
Manager, Callista Service Desk
Delegated signatories

2.2. Eligibility for Access

- Staff of Monash University and any controlled entities to which the Electronic Information Security Policy and Procedures apply, are eligible to be granted access into Callista.
- Access for an entity not included in point 1 above may be approved at the discretion of the Director, Student and Education Business Services.
- The Director, Student and Education Business Services, may enforce an access time restriction for any entity included in point 2.
- The Chief Information Officer, or their nominee, may revoke access in circumstances where inappropriate use is identified.

Responsibility

Staff of Monash University
Director, Student and Education Business Services
Chief Information Officer

2.3. Access Restrictions

- The Director, Student and Education Business Services, shall determine a list of restricted combinations of functions, and the organisational areas to which these apply, for which access will not be granted.
- The Director, Student and Education Business Services, will provide the Callista Service Desk with the list of restrictions.

Responsibility

Director, Student and Education Business Services
Manager, Callista Service Desk

3. Requesting and Activating Access

- The Callista Service Desk will be responsible for activating access and adding or amending roles to Callista accounts.

- To apply for Callista access, a Callista Access form must be completed indicating the functionality (Callista role) for which access is required.
- Access must be approved by a delegated signatory.
- Staff must undertake relevant training prior to having access activated, or demonstrate that relevant training has been undertaken previously.
- A request for Callista Access will be checked to ensure that it has been approved by a delegated signatory and that the staff member has completed the relevant training prior to activating access.
- Until automatic provisioning is established, the Callista Service Desk will check a request for access, along with the functionality already granted, against the list of restricted combinations. If the combination is on the list of restrictions, then the user will be informed that access is refused.

Responsibility

Manager, Callista Service Desk
Staff requesting Callista access

Modification of Access for Staff Members Changing Roles within the University

- Until automated provisioning is established, it is the responsibility of the staff member's manager to inform the Callista Service Desk when a professional staff member with Callista has changed roles within the organisation.
- When a professional staff member changes roles, the Callista Service Desk will revoke any access greater than Inquirer level unless a Callista Access form for the new role is received.

Responsibility

University Manager
Manager, Callista Service Desk

Removal of Access for Staff who have Left the University

- Until automated provisioning is established, on a monthly basis Student Business Support will provide the Callista Service Desk with a list of staff members who have left the University, requesting that access to Callista be deactivated.
- The Callista Service Desk will be responsible for deactivating accounts within an agreed timeframe.

Responsibility

Manager, Student Business Support
Manager, Callista Service Desk

Responsibility for implementation	Information Owners Deputy Vice-Chancellors Vice Presidents Pro Vice-Chancellors and President, Monash South Africa Deans of Faculties
Status	Revised
Approval Body	**Name**: Vice-President (Administration)

Monash University Procedure

	Meeting: n/a **Date**: 12-September-2012 **Agenda item**: n/a
Definitions	**Information Owner**: An individual with the responsibility for coordinating the implementation of this policy and its procedures for a functional area. The Information Owners for administrative, research and education information are listed in the Information Classification Registers. **Information Custodian**: An authorised individual who collects, stores or transmits electronic information pertaining to the university's activities of research, education and administration.
Legislation Mandating Compliance	**Australia:** Privacy and Data Protection Act 2014 No.60 (VIC) Health Records Act 2001 (Vic) - note Health Privacy Principles within Act (Section 19 and Schedule 1) Protected Disclosure Act 2012 No. 85 (VIC) Higher Education Support Act 2003 (Commonwealth) - note Part 5-4 Management of Information, and specifically section 179-10 Use of Personal Information Education Services for Overseas Students Act 2000 (Commonwealth) - specifically The National Code 2007, Standard 3.1(d) Public Records Act 1973 (Vic) Epidemiological Studies (Confidentiality) Act 1981 (Commonwealth) - where relevant to a research project **South Africa:** South African Electronic Communications and Transactions Act 2002 (Act No 25 of 2002) - protects personal information that has been obtained via an electronic medium. South African Protected Disclosures Act 2000 (Act No 26 of 2000)
Related Policies	Electronic Information Security Policy Recordkeeping: Retention and Disposal of University Records Policy
Related Documents	Monash Privacy Compliance Framework