Appendix 1

Data Breach Preparation and Response Plan

Maintain information privacy and security

JCU, its staff and affiliates have an ongoing obligation to take reasonable steps to handle personal information in accordance with the University's Information Privacy and Records Management policies, Acceptable Use of ICT policy and broader Queensland and Commonwealth Government legislation on information privacy that may change from time to time. This includes protecting personal information from misuse, interference and loss and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information.

Step 1. Contain

The first step is to contain a suspected or known breach where possible. This means taking immediate steps to limit further access or distribution of the affected personal information – this will be by different mechanism if in hard copy or physical form (eg drive or USB) than if sent by email or posted on websites or other digital media. Staff should immediately notify their supervisor and contact the Information Privacy Officer to alert them to a potential breach, providing as much detail as possible on how the breach occurred, what was the information, who might be affected and what immediate action was taken to contain the breach.

Step 2. Assess

Information Privacy Officer conducts an assessment on whether the information is likely to result in serious harm to any of the individuals whose information was involved, and consider remedial action. This will be undertaken in consultation with the Information Security and Risk Specialist or Manager Records as appropriate. If an eligible data breach under the NDB Scheme, the Chief of Staff is to be notified and the Notifiable Data Breach Response Team is constituted.

Take remedial action

Where possible steps to reduce potential harm to individuals should be undertaken. This includes recovering lost information before it is accessed or changing access controls on compromised records or systems. If remedial action is successful in reducing the likelihood of serious harm, then notification to the OAIC is not required.

NO — **Is serious harm likely?** — **YES**

Step 3. Notify

The Chief of Staff is to prepare a statement for the Commissioner (using the OAIC form) that contains: a description of the eligible data breach; the kind or kinds of information involved in the eligible data breach; and what steps the entity recommends that individuals take in response
JCU must also notify affected individuals:

- Option 1 – Notify all individuals;
- Option 2 – Notify only those individuals at risk of serious harm; or if neither options is practicable:
- Option 3 – Publish notification (for example, if the entity does not have up-to-date contact details for individuals, JCU may provide a copy of the statement on the website and take reasonable steps to publicise the statement. This statement and notification may include an apology and explanation what is being done about the breach.

Step 4. Review

Review the incident and take action to prevent further breaches and improve personal information handling practices. This will include the completion of a Lessons Learned Report may include

- a security review including a root cause analysis of the data breach;
- a prevention plan to prevent similar incidents in future;
- audits to ensure the prevention plan is implemented;
- a review of policies and procedures and changes to reflect the lessons learned from the review;
- changes to staff selection and training practices; and
- a review of service delivery partners that were involved in the breach.

JCU may also have a requirement to report the incident to other relevant bodies including policy, ASIC, APRA or the ATO, the Australian Cyber Security Centre or TEQSA.