IBI AUSTRALIA INVESTMENT BANKING INSTITUTE

Records Management and Security Procedure

policy@ibi.edu.au

www.ibi.edu.au

Records Management and Security Procedure

1.0 Overview

Senior management of have a legal responsibility to protect the organisation's physical and electronic records (including IT infrastructure) and the information IBI holds.

The creating, securing and retention of records is part of IBI's overall knowledge management system.

IBI keeps records to:

- provide an historical record of IBI's operations, activities and decision-making;
- provide evidence of business transactions and decisions, for purposes of accountability;
- enable IBI to find the right information easily and comprehensively;
- enable IBI to meet its legal and regulatory requirements for data management and reporting.

2.0 Types of records

2.1 Student records (Paradigm)

A separate paper-based file is created for each student and an electronic record is also created in the student database myIBI Portal. The paper and electronic student files combined are known as the "student record".

The Registrar maintains student records.

The student record contains as a minimum:

- the completed Application Form;
- enrolment details;
- any agreement with the student;
- any information relating to request for, and granting of credit for prior learning;
- results for each assessment event in a unit of study;
- the final mark and grade for each unit of study;
- details of payments and refunds;
- copies of testamurs and records of results issued;
- any notes made by the academic /administrative staff about the student (including any disciplinary matters).

The entire student record is maintained for a period of at least 2 years from graduation (or when the student otherwise ceases to be a student). Financial records relating to a student are kept for a minimum of 7 years.

Student results for each unit of study are retained indefinitely to enable the re-issue of an award and record of results if required. In the event of IBI's closure, student records will be transferred to the relevant higher education regulator, or as otherwise prescribed by regulation. Students may access information on their files as per the *Privacy and Personal Information Procedures*. Third party access is only permitted when required by law or with the express permission of the student as outlined in the *Privacy and Personal Information Procedures*.

2.2 Staff records

The HR Manager maintains staff records.

Each staff member has a file created and maintained for the purpose of archiving:

- recruitment paperwork;
- employment conditions / letter of offer / employment agreement;
- evidence of the "right to work" in Australia;
- position description;
- evidence of participation in the staff induction process;
- certified copies of qualifications claimed;
- verification of experience;
- professional development activity.

Original documentation must be sighted to verify the authenticity of qualifications. Copies on file must indicate the date sighted and by whom (refer *Staff Recruitment, Induction, Professional Development, Appraisal and Promotion Policy & Procedure*, section 2.5).

Disciplinary action or details of grievances in which the staff member is a complainant or respondent may also be noted in the staff file. Staff may access information on their files on request to the HR Manager. Third party access is only permitted when required by law or with the express permission of the relevant staff member.

2.3 Financial records

The Registrar maintains financial records. Financial records are maintained on MTOB financial management system. Financial records are created, secured, archived and retained consistent with contractual and legal requirements. Financial and contractual records must be kept for a minimum of 7 years.

3.0 Records security and access

IBI takes seriously its obligations under privacy legislation to safeguard all confidential information. IBI will also ensure that anyone acting on its behalf maintains appropriate confidentiality. As such, it is a requirement that records are held in a secure environment and safeguarded against loss, damage or unauthorised access. Only authorised staff will be granted access to student and staff records.

This section should be read in conjunction with IBI's *Privacy and Personal Information Procedures.*

3.1 Electronic records

IBI maintains a secure computer network. Each user has their own password which allows them access to appropriate functions and files within the system.

The IT Manager is responsible for the restriction of access to and security of electronic records.

3.2 Physical records

Physical records are kept in secure areas or locked filing cabinets and access is only available to authorised personnel.

4.0 Version management

In the interests of enhancing knowledge management, IBI has implemented a system for managing the versions of certain documents - refer section 4.4 of the *Quality Assurance Framework*.

5.0 Record retention and disposal

Records will be retained and secured according to the following retention periods:

- General business records (including financial records): 7 years.
- Student records: 2 years after the student ceases to be a student except for enough data to re-issue an award and record of results to be kept in perpetuity.
- Staff records: 5 years after the staff member ceases to be a staff member.

6.0 Security of electronic data

The breakdown of key IT infrastructure, either by mechanical means or human intervention can become a critical incident if proper safeguards are not put in place to ameliorate the impact of such a breakdown.

6.1 Preventions against data loss

In relation to IT Infrastructure IBI ensures that the following preventions are implemented:

- Backups (including software as well as all data information) are sent off-site at regular intervals to facilitate recovery;
- A remote backup facility is utilised to minimise data loss;
- Surge protectors are employed to minimise the effect of power surges on electronic equipment;
- Servers and essential equipment are protected with an Uninterruptible Power Supply (UPS) and/or Backup Generator;
- An effective alarm system and accessible fire extinguishers are installed in the case of a fire;
- Anti-virus software, firewalls and other security measures are employed.

Electronic records are backed up on a regularly basis. On the last day of the month a monthly backup is taken and is kept off-site.

The computer network is maintained by a programmed regimen of maintenance along with ad hoc support as and when required by IT Manager.

6.2 Security safeguards

6.2.1 Protection against in-house intrusions:

IT Manager has implement and range of security measures including

1. Password allocation
2. Login monitoring
3. IT access levels

6.2.2 Protection against external intrusions

IT Manager has implement and range of security measures including

i. Firewalls
ii. Password protection
iii. Electronic keys

6.2.3 In the case that equipment is damaged or data is compromised:

IT manager makes a judgment call on whether the equipment is repaired or used for spares/replacement parts.

7.0 Version history

VERSION CONTROL

Review/ amendment history

Policy Approved by: Chief Executive Officer

Responsible Officer: Chief Executive Officer

Next Policy Review Date: July 2018

Version	Date	Details
1.0	July 2014	Policy issued
2.0	Dec 2014	Updated to reflect Standards for Registered Training Organisations (RTOs) 2015
3.0	April 2015	Updated to reflect NVR 2015 Standards
4.0	April 2016	No material changes
5.0	April 2017	No material changes