



Records Management Policy & Procedure

1. Purpose

This document is in addition to and supports the Department of Attorney General and Justice Records Management Policy and Procedures and ensures compliance to ISO/IEC 27001 Information Security Management, ISO 9001 Quality Management Systems and RTO standard requirements. It provides information on the creation, maintenance, proper use, management of and access to student records required by BFCSA as a Registered Training Organisation.

This policy and procedure combines and supersedes the following documents:

- Student Records Management Policy & Procedure 2009 v1.1 (CIMS/TRIM : D09/074003)
- Administration Records Management Policy & Procedure 2008 v 1.0 (CIMS/TRIM:D09/073999)

2. Scope

A record is a document that states a result achieved or provides evidence of an activity performed such as an assessment result. Records are historic in nature and are therefore static in nature, providing evidence that some business event has occurred and has an unchangeable outcome at that point in time such as an enrolment in a course, on a specific date and time.

A document that is other than a record, such as a participant guide or a procedure that evolves as new information is available and requires changes to be managed, is not covered by this policy. The user should refer to the Creating & Controlling Documents Policy.

This document covers the management of all BFCSA learner records and other records related to training and assessment at or on behalf of BFCSA, including: identification, storage, protection, retrieval, retention and disposition. The management of records includes:

- creation and registration (identification & storage)
- access (protection)
- movement and retrieval (retrieval & retention)
- storage and disposal (disposition)

3. Definitions

ASQA	– Australian Skills Quality Authority
BFCSA	– Brush Farm Corrective Services Academy
CSNSW	– Corrective Services New South Wales
Ephemeral records	– those of little value and only needing to be kept for a limited or short period such as hours or days
ISO/IEC 27001	– Information Security Management standard
ISO 9001:2008	– International Standard for a Quality Management System
LMS	– Learning Management System
L&SD	– Learning and Staff Development
RTO	– Registered Training Organisation
SIS	– Student Information System

4. Policy Statement

As required by the Department of Attorney General and Justice Records Management Policy and Procedures 2013, will systematically collect and store data on learners' participation, assessment, and progress as part of its procedures for the creation, use, access, retrieval and disposal of all records.

Warning! – Uncontrolled when printed! The current version of this document is held in TRIM.

This is also in accordance with BFCSA standards as a Registered Training Organisation and certified to an ISO9001:2008, Quality Management Systems standard.

BFCSA in compliance with the VET Quality Framework *and RTO Standards for Continuing Registration* ensures that the management system is responsive to the needs of participants, customers and stakeholders. This includes ensuring that:

- 1 records are managed for accuracy and integrity;
- 2 staff understand and meet their record-keeping and record management responsibilities; and
- 3 learners have timely access to current and accurate records of their participation and progress.

In addition, the Government Information (Public Access) Act 2009 (GIPA Act), enables employees to access files containing personal information, including training files. Participants in training courses conducted by BFCSA will have access on request to their training records as a means of ascertaining their progress and ensuring the contents are complete, accurate, and up-to-date and not misleading.

5. Responsibility

It is the responsibility of the Director, Learning & Culture to ensure that policy documents are regularly reviewed and the most current approved version is available online.

The Director, Learning & Culture will ensure that BFCSA procedures covering creation, storage, access, removal/movement and labelling of records, file covers and transport containers promote the integrity and confidentiality of the organisation's information.

It is the responsibility of all Unit Managers to ensure that all documents produced or revised by their unit complies with this policy.

6. Legislative Context

Copyright Act 1968
Government Information (Public Access) Act 2009 (GIPA Act),
National Vocational Education and Training Regulator Act 2011
Privacy and Personal Information Protection Act 1998
Privacy Amendment (Enhancing Privacy Protection) Act 2012
State Records Act 1998

7. Changes and Updates

All policies and procedures are subject to ongoing revision to reflect systems improvements. All online documentation is considered to be the current version.

8. Monitoring and Evaluation

This policy will be reviewed three years from the date of implementation, or earlier should a review be warranted.

9. Associated Documents

DAG&J Records Management Policy and Procedures 2013, D12/637168 & D07/42418
Intellectual Property Management Framework for the NSW Public Sector, NSW Premier's Department 2005
AS/NZS ISO 9001:2008 Standard for Quality Management System
Standards for NVR Registered Training Organisations 2011
CIMS User Guide 38, CIMS TRIM D12/002167
Creating & Controlling Documents Policy and Procedure, CIMS TRIM D09/073984
Shared Drive User Guide, CIMS, TRIM: D09/271414
Archiving Procedure, D08/122193

Warning! – Uncontrolled when printed! The current version of this document is held in TRIM.

Shared Drive Business Rules, CIMS TRIM: D09/058944
BFCSA Visual Standards, CIMS TRIM: D09/067228
Appeals Policy and Procedure, CIMS TRIM 009/073982
CSNSW Electronic Mail Policy 2008, CIMS TRIM D08/121159
Assessment Policy & Procedure, CIMS TRIM D09/329877
Recognition Policy & Procedure, CIMS TRIM D09/073985

10. Procedures

10.1. Creation and registration of records

The Student Information System (SIS) and Learning Management System (LMS) are databases used to store learners' participation, assessment, recognition and qualification issue records as well as records of prior and/or external training and professional development.

In addition, other records such as policies & procedures, manuals, guides, curriculum documents, organisational charts, business plans, marketing material and other similar documents are stored in TRIM.

All documents are to be created using the organisations agreed naming conventions (refer to CSNSW Electronic Mail Policy and DAG&J Records Management Policy for further information). Document names are to be meaningful to an outsider and not use non-approved acronyms. 'BFCSA' is the only Academy-use acronym approved for use in TRIM.

10.2. User Guides for SIS & LMS

User guides for SIS/LMS are available for various business uses In TRIM 09/14593 and via help in the LMS.

10.3. Electronic storage

All work related documents (including emails and loose-leaf hard copy documents) are to be managed in CIMS-TRIM. NO work related documents are to be stored in either MS Outlook or on network drives such as M:\, L:\ or D:\ or on portable devices such as USB sticks or laptops.

The only exception to this is draft policies which may be stored in an approved folder on M:\ (e.g., Policy in Draft folder) pending finalisation.

There are to be NO password restrictions placed on any work related document. The copyright of all work belongs to CSNSW and should not be attributed to any individual or Unit staff member.

The staff member who first receives information from inside or outside the Agency (CSNSW) (e.g. a document – either hard or soft copy – or an email) is responsible for capturing this record in CIMS-TRIM.

The creation of files (and associated access rights) is restricted to the BFCSA CIMS-TRIM Administrator. The process and procedure is detailed in the Creating and Controlling Documents Policy and Procedure.

10.4. Participant access to personal files

All participants are to have access to their personal training files for the purpose of monitoring their own progress and ensuring accuracy of content.

Warning! – Uncontrolled when printed! The current version of this document is held in TRIM.

10.4.1 Notice

Participants wishing to view their training records will provide a written request to the appropriate Unit Manager. The Unit Manager will arrange for the participant to view their records within seven working days of receiving the request, after notifying the Director Learning & Culture.

10.4.2 Viewing documents

The participant will be able to view their own records only in the presence of or with the permission of the Training Unit Manager or his or her delegate. The Training Unit Manager will ensure that the participant does not have access to information relating to another participant. Only a copy of their record or a viewing of their own record will be made available. A request to view or obtain results of a participant from their Manager or Supervisor or some other interested party must be in writing or e-mail to the Director, Learning & Culture outlining the reason for their enquiry and must satisfy Privacy and Personal Information Protection and not be in any conflict of interest or breach of the CSNSW Guide of Conduct & Ethics. Any doubt should be referred to the Director, Learning & Culture (L&C) CSNSW.

The participant will not be allowed to alter the contents of the file or remove documents.

10.4.3 Challenging the contents

Should the participant disagree with any of the contents of the file, he or she may request a review by submitting a request in writing to the Director, L&C at BFCSA, identifying the document(s) in question and stating the reason. The appropriate Unit Manager will arrange a review within seven working days of receiving the request. In general, the review will be completed within one calendar month. The participant will be informed of the decision in writing. A record cannot be changed or altered unless it is found to be inaccurate, and can only be altered with permission from the Director or his/her nominated delegate. All other issues relating to a participant challenging or disputing a record of results or progress should be referred to the Appeals Policy.

10.5 Retention of Records

BFCSA will retain participants' records for a period of 30 years as per the requirements of the NVR RTO Standards for Continuing Registration.

Unit Managers are responsible for the safety and security of student records related to their unit. They must ensure that all active student records are appropriately maintained and are secure from theft, loss and damage.

10.6 Existing Pre-TRIM Records

Hard copy student records will be stored within each unit at BFCSA for 12 months from the date of the last action. Unit managers must archive these student records annually and transfer records that have not been accessed for 12 months to Corporate Records. All such records are to be placed into approved archive boxes (only) and the contents noted as per CSNSW archive procedures D08/122193.

10.7 New Records

Hard copy student records such as assessment portfolios will be reviewed by the Manager upon

Warning! – Uncontrolled when printed! The current version of this document is held in TRIM.

course completion. All assessment events related to a participant who is/was the subject of funding, will be scanned and saved into the appropriate TRIM container. All other participant records will be assessed regarding the need for sample evidence of assessment completion and where appropriate scanned and placed in TRIM container. The approved naming conventions will be used including the course code and session number. On completion of scanning the Unit Manager will verify all the course documentation has been placed in the correct TRIM container and that the electronic document is identical. (Refer to CIMS User Guide 38 for the management of scanned documents - D12/002167).

Electronic student records will be maintained on SIS or the LMS for a period of 30 years and backed up by CSNSW ICT Division on a daily basis according to the BFCSA Data Back Up/Recovery see section 11.0. The LMS is backed up by the contracting party for the LMS, as outlined in the Master Service Agreement.

A minimum of seven working days' notice must be given for the retrieval of documents in semi-active storage at BFCSA.

10.8 Archiving of Records

The BFCSA Business Services Manager maintains an Archive Scheme for all BFCSA records, comprising:

1. a list of all records created within BFCSA
2. an explanation of what these records contain
3. The records that are stored at BFCSA and their security

The Manager Business Services Unit (BSU) and or the CSNSW Corporate Records Manager may request the transfer of records from BFCSA semi-active storage and from individual units. These records will be packed in accordance with instructions issued by the Manager BSU or the Corporate Records Manager and transferred by secure means. Confidential records, as identified in the Archive Scheme, will be safeguarded.

Records in the care of the Corporate Records Manager may be recalled for use at BFCSA at any time following a request through the IC&T Self Service Portal to Corporate Records. Records will be dispatched promptly through the internal mail system.

Electronic records (e.g. CD's, DVD's etc.) must be archived in the same manner as non-TRIM files as per Archiving Procedure D08/122193.

CSNSW Corporate Records Manager has delegated responsibility for determining appropriate disposal of all departmental, including archived student, records. No record is to be disposed of, either transferred to the State Archives or destroyed, unless approval has been given to do so by the CSNSW Corporate Records Manager.

Records of an ephemeral nature (as defined by DAG&J Records Management Policy) such as raw data collected from Evaluations, which is recorded and captured in summary or other recorded reports, shall be retained for a period of two months after completion of the unit of study, or longer if deemed appropriate by the Training Unit Manager. Such records may then be securely destroyed in accordance with CSNSW Corporate Records Management Policy.

11 0 Data Backup/Recovery

CIMs-TRIM data, SIS data and network data are protected by CSNSW corporate backup system. The management of CSNSW Backup Service is fully outsourced to the external service provider -ac3. The CSNSW backup strategies consist of seven processes:

1. **Backups to Disk:** All primary backups are performed to disk, not tape. To ensure rapid recovery when required, The Disk Backup process provides faster recover timeframe and also

Warning! – Uncontrolled when printed! The current version of this document is held in TRIM.

- offers more flexibility to CSNSW data protection framework.
2. **Tape Backup:** Tape backup is only used for long-term archival purposes to reduce the impact of computer resources during the backup process.
 3. **SAN Integration:** The CommVault backup solution natively integrates with the HDS SAN array data management functions are deployed to ensure backup solution performs in the same standard proactive monitoring and response service levels.
 4. **De-duplication:** To capture opportunities for minimising storage requirements, CommVault uses de-duplication technology to avoid storing duplicate copies of data typically, a 10 to 20 times compression in storage space is achieved.
 5. **Agent-less VM Backups:** CommVault backs up VMware Virtual Machines (VM) using a single agent installed on the vCenter. This enables full VM backup with the ability to restore selected parts of the VM or the whole VM and can reduce recovery times by up to 60%. With no agents installed, there is no load on the VM.
 6. **Incremental Only backups:** The first backup of any data source is a full backup. Thereafter, all subsequent backups are of the incremental changes. 'Synthetic' full backups can be generated for any point in time by determining the most recent copy of all current data files prior to the nominated point in time. It is estimated that this will reduce potential contention on the network between 50 and 60% (based on a weekly full backup and 10% incremental backup daily).
 7. **WAN Bandwidth Management:** Backups performed over WAN connections can have bandwidth management implemented that ensure that WAN links are not flooded when scheduled backups are run.
 8. **The LMS,** LMS data management and data backup and recovery is fully outsourced to Janison Pty Ltd, a third party provider. The data is externally hosted on the Janison server and is protected by their corporate backup system - refer to D13/180880 for details .

12. Contact Details

Any Issues arising from the implementation or process associated with this policy should be referred to BFCSA. Any Issues regarding data storage and recovery should be referred to the Academy Systems Administrator in the Business Unit. The Academy welcomes your feedback, any concerns or interest in improving our system or policy can be referred to the Manager Business Services Unit. Feedback forms are located on the BFCSA website and hard copies in the Academy Reception area.

Warning! – Uncontrolled when printed! The current version of this document is held in TRIM.