Data Access Form

Purpose

Support the sharing of authoritative organisational data across CSU technology solutions and to ensure:

- same data and rules are referenced by all system where applicable
- correct data has been matched to business need and context
- support implementing data quality controls of availability, accuracy, correct, consistent, complete, fit for purpose
- data security classification is known to inform required security controls
- visibility of data shared between CSU Systems to support internal and external auditing obligations

Data Access Approval Phases

1. **Initial Approval to Use:** Initial approval to allow change activity to progress investigation of identified data needs. First approval phase includes use within named target system & Developer access to identified source data for the purpose of inclusion within design, development and testing of the associated change activity and governance. This includes both development and QA environments, associated Test Team.
   Timing: Within change activity, prior to or at commencement of associated design activity. For example in an agile approach, this may be within Definition of Ready requirement, Solution Overview or a 'story' within a sprint.
2. **Production Ready Approval:** Formal notice has been provided to Data Custodian that unit & user acceptance testing satisfactorily completed, security controls & new integration interface/s are production ready. On the source Data Custodian's signoff, this includes approval for Developer access to respective system production database/tables/files to complete changes in scope.
   Timing: Within change activity, at completion of testing, prior to RFC for production implementation and release. For example in an agile approach, this may be within Definition of Done requirement or a 'story' within a sprint.

User Guide

For further information on how to complete a data access form refer to the supplementary user guide.

Document Version Status & Revision History

Version	Author	Source Custodian	Target Custodian	Request Date	Revision Item / Section

Section 1

Target System

CSU System Name	
Org Unit	
Data Custodian Contact	
Site Physical Location	
Site Contact/Vendor	
System Primary Function	
System Access Controls	*<CSU authentication>*
Link to system documentation	
Change Activity and Contact	

Target System User Group Definitions (disclosure)

System User Group	User Group Description	Access Type	Access Method	Membership Mgt
<eg. CSU staff, HR staff, Faculty Admin>				

Data & Source System/s - Overview

Source System	**<system 1>**	**<System 2>**	**<System 3>**	**<System n>**
Org Unit				
System Custodian				
Data Custodian				
Data Set 1				
Security Level				
Feature/Function/s				
Purpose				
Scope of Records				
Data Set *2*				
Security Level				
Feature/Function/s				
Purpose				
Scope of Records				

Data Set n				
Security Level				
Feature/Function/s				
Purpose				
Scope of Records				

Data Notes

<Section available to capture any notes on data to be considered in design, development, testing. As advised from Source Custodian or from the projects perspective.>

Restricted Data Sets

School of Policing & Australian Graduate School of Policing & Security (AGSPS) Student Data	**Response**
1. Are policing, Goulburn, Manly or AGSPS student data within scope of data request?	*YES / NO*
2. Are policing, Goulburn, Manly or AGSPS course or subject related data in scope?	*YES / NO*
3. If yes, who within the School of Policing & Australian Graduate School of Policing & Security (AGSPS) has formally sanctioned?	*<N/A or add note/ reference to formal approval>*

Section 2

Source System Data Custodian – Approval

Approval includes use within Target system & Developer access to identified source data for the purpose of inclusion within design, development and testing. This includes both development and QA environments.

Source System	***<system 1>***	***<System 2>***	***<System n>***
Data Custodian	**<enter name>**	**<enter name>**	**<enter name>**
Phase 1 - Initial Approval to Use	*Approval includes use within Target system & Developer access to identified source data for the purpose of inclusion within design, development and testing. This includes both development and QA environments.*		
1. Initial Approval to Use	Yes / No	Yes / No	Yes / No
Link to Approval Email			
Initial Approval Date			
Any exclusions or known issues			
Nominated Source Testing Contact or Tester			
Additional Notes			
Phase 2 - Production Ready Approval	*When formal notice has been provided to Data Custodian that unit & user acceptance testing satisfactorily completed & new integration interface/s are production ready. On the Data Custodian's signoff, this includes approval for Developer access to respective system production database/tables/files to migrate changes in scope to production environment.*		
Appendix A complete	Yes / No	Yes / No	Yes / No
Testing Successfully completed	Yes / No	Yes / No	Yes / No
2. Production Ready Approval	Yes / No	Yes / No	Yes / No
Production Ready Approval Date			
Link to Approval Email			
Additional Notes			
Disclaimer: It is the responsibility of the Target System Custodian (c/-Project Manager) to ensure the data sourced from the authoritative source system is correctly matched for the requirements of the target system, confirmed through unit & user acceptance testing for all business use cases in scope.			

Appendix A: Source System/s Data Extract Details

Instruction:

Task - For each source system in scope copy and complete an appendix A entry for a summary of implementation details for the requested data.

Timing - Complete as early as possible and prior to seeking approval for phase 2, production ready approval.

Source System 1: <enter name>

Data Description

Master Data Attribute	Source System	Source Table	Source Table Field	Security Class.	Master Data Object	Target System table/field	Scope of Data Records	Data Tranformation	Access Type	Extract Type	Extract Timing	Data Path *(see key appendix B)*
Data Set 1												
Data Set n												

Target System Extract Rule

Shared (Master) Data Object	Extraction Rule – for record set to be used in target system

Enterprise Identity Data in Scope

List any IGMS identity data in scope.

		Scope of Use	
Identity Attribute	**Purpose & Use**	**Lookup Value**	**Stored Data**
		Y or N	*Y or N*

Enterprise (Identity) Groups in Scope

List any enterprise groups and memberships to be applied within the scope of this data set where used:

- *as a data record extraction criteria e.g. only Academic Staff timesheet records; and/or*
- *for provisioning user access to a system e.g. provisioning only Academic staff access to a Research Repository*

		Scope of Use	
Enterprise Group	**Additional Filter Rule (if applicable)**	**User Access Provisioning**	**Data Set Criteria**
IGMS enterprise group name OR if new, describe briefly	*Only where applicable eg. only Bathurst campus staff*	*Y or N*	*Y or N*

Data Lifecycle Management – Lifecycle Quality Controls

Describe target system method to manage source data lifecycle changes eg. create, updates, inactive, deletions, archive, disposal.

- Complete for each change type when known and prior to request for production approval.

Source Record Changes	Target System - Data Lifecycle Management
Data Set 1 – *<label>*	
New	
Updates	
Inactive	
De-identified	
Deletion	
Data Set n – <label>	
New	
Updates	
Inactive	
De-identified	

Deletion	

Appendix B: References

Data Description

Master Data

Master Data Definitions: Master Data Resources Catalogue

Security Class.

Data Security Classifications: http://www.csu.edu.au/division/dit/eal/portfolios/information/docs/Data_Security_Classification_Scheme1.pdf

Data Path Legend

igms - Identity & Group Management System
mw - middleware, term used to describe CSU data integration technology solution.
mdc - Master Data Cache, a database that stores a copy of master data.
source - the determined originating authoritative data source.
target - the system to access & use authoritative data.
API – Application program interface (API), a method of allowing communication between two systems.
CSV – comma separated values file which allows data to be saved in a table structured format

Add additional items if necessary

User Guide: Data Access Form

This document is a supplementary guide to completing the ***Data Access Form***. There are two parts to the user guide.

Part 1 – provides an overview of why of a data access form is used, along with a brief outline of when, who, and how.

Part 2 – Following the layout of the data access form, provides a brief description of expected details required to complete the form. User guide notes are represented as *blue italic text*.

Part 1 – Overview

Purpose

Support sharing of authoritative organisational data across CSU technology solutions and to ensure:

- same data and rules are referenced by all system where applicable
- correct data has been matched to business need and context
- support implementing data quality controls of availability, accuracy, correct, consistent, complete, fit for purpose
- data security classification is known to inform required security controls
- visibility of data shared between CSU Systems to support internal and external auditing obligations

Data Access Approval Phases

1. **Initial Approval to Use:** Initial approval to allow change activity to progress investigation of identified data needs. First approval phase includes use within named target system & Developer access to identified source data for the purpose of inclusion within design, development and testing of the associated change activity and governance. This includes both development and QA environments, associated Test Team.

   Timing: Within change activity, prior to or at commencement of associated design activity. For example in an agile approach, this may be within Definition of Ready requirement, Solution Overview or a 'story' within a sprint.
2. **Production Ready Approval:** Formal notice has been provided to Data Custodian that unit & user acceptance testing satisfactorily completed, security controls & new integration interface/s are production ready. On the source Data Custodian's signoff, this includes approval for Developer access to respective system production database/tables/files to complete changes in scope.

   Timing: Within change activity, at completion of testing, prior to RFC for production implementation and release. For example in an agile approach, this may be within Definition of Done requirement or a 'story' within a sprint.

Responsibilities

- **Accountability**
  Change Manager or Business Owner (requiring access to data) are accountable for ensuring a data access request is completed.
- **Responsibility**
  Responsibility for preparing a data access request will depend on the type of change activity. Within a project, it will be the Business Analyst with input from Principal Designer/Technical Lead. Outside a project, an appropriate Business Stakeholder involved within the change such as a Process Owner, Systems Officer or Data Custodian.
- **Data Custodians**
  A Data Custodian is a nominated trustee responsible for a specified information or data set with regards to quality, availability and protection according to relevant University business requirements, policy and legislative compliance. In the context of data sharing there is a source and target data custodian:
    - **Source Data Custodian** is the custodian associated with data requested to be shared to another system or solution. For delivering on data sharing capability, contributes knowledge on the purpose, meaning, rules, lifecycle management processes, protection, etc. for the requested (source) data in scope.
    - **Target Data Custodian** is the custodian associated with the system or solution that would like to access and use data from another system. For delivering on data sharing capability, contributes knowledge on the required data need, how it will be managed and protected within the other (target) system.

  The data access form is completed by a representative of the Target Data Custodian and access approved by the relevant Source Data Custodian representative.
- **Information Architect**
  Supports data access approval process primarily in preparation of requests, communication with source data custodians and maintaining a central register of data access agreements.

Instruction

Initial Approval to Use – Complete section 1 of the form with information as known at the early requirements or design phase of the change activity. Appendix A can be completed if additional details are known, however not mandatory at this phase but useful if details can be shared early with the respective source Data Custodian. The Information Architect is available to support the preparation of approval requests, please contact if required. Send completed form to respective Data Custodian with request for initial approval to use and any feedback.

Register Outcome - On receipt of feedback and approval response from each Data Custodian, update section 2 with relevant details in the Approval summary table and forwarded a copy to the Information Architect. This then becomes an internal record of a Data Access Agreement for initial approval to share data between nominated CSU systems.

Production Ready Approval – From the Check if any updates required to request and appendix A has been completed for each source system. Confirm all relevant testing has been successfully completed. Update document version and forward to respective Data Custodian/s with request for approval to move to production.

Register Outcome - On receipt of feedback and approval response from Data Custodian/s, update section 2 with relevant details in the approval summary table and forwarded a copy to the Information Architect. This then becomes an internal record of a Data Access Agreement for approval to share data in the production environment between nominated CSU systems.

Accessing Data for Analytical Purposes

If data access is required purely for analytical purposes, complete the ***Analytics Data Access Form*** instead.

Part 2 – Completing the Form

First step is to save a copy of the form, to save as a draft Data Access Agreement (DAA) document.

Apply the following document naming convention: DAA source target yyyymmdd.docx

Source: short name of source system (if multiple source systems, initially use key source system. Source label will ratified on submission.)

Target: short name of target system

yyyymmdd is the current date

Document Version Status & Revision History

Version	Author	Source Custodian	Target Custodian	Request Date	Revision Item / Section
	Requesters Name	*Data Custodian for source system*	*Data Custodian for target system*		

The same form will be used for stage 1 initial approval and stage 2 production ready approval. For each approval stage, capture document changes by adding a new row, increment version number and capture details of change and, or approval phase.

Section 1

Target System

CSU System Name	*CSU name of target system*
Org Unit	*Organisational Unit that owns/manages target system*
Data Custodian Contact	*Data Custodian for target system*
Site Physical Location	*Externally Hosted name Campus/City, State, Country. Internally hosted named CSU Data Centre Sydney or campus location*
Site Contact/Vendor	*Name of Vendor or Internal Contact*
System Primary Function	*Brief description of primary function e.g. events management*
System Access Controls	*Local system based access management &/OR (enterprise) CSU authentication &/OR public/open access, etc.*
Link to system documentation	*If available, documentation that provides more detail on target system solution*
Change Activity and Contact	*Name of project or change activity and contact person*

Target System User Group Definitions (disclosure)

System User Group	User Group Description	Access Type	Access Method	Membership Mgt
Group name e.g. CSU staff, HR staff, Faculty Admin. *One row for each group. Add more rows if required.*	*Brief description of membership rule*	*Read, Write, Update, Delete*	*Public, authenticated, single sign-on, local account, etc.*	*Provisioned enterprise group (IGMS) OR target system local management group*

Data & Source System/s – Overview

Instruction – can add or subtract columns to match number of source systems in scope. If more than four, may be more manageable to capture on a second request form.

Source System	*Enter CSU name of source system*	**<System 2>**	**<System 3>**	**<System n>**
Org Unit	*Organisational Unit that owns/manages source system*			
System Officer	*Name of system officer for source system*			
Data Custodian	*Name of Data Custodian for source system*			
Data Set 1	*Name of data set required e.g. program enrolments*			
Security Level	*Enter security classification of data set e.g. highly confidential, confidential/private, internal, public*			

Feature/Function/s	*Brief description of target system function for which data will be used e.g. event management*			
Purpose	*Brief description how data will be used e.g. to identify potential participants for planning purposes.*			
Scope of Records	*Describe scope of records required e.g. current, future, only Bathurst program enrolments for required session.*			

Optional – Can copy in an additional set of rows to accommodate more data sets. Equally, can remove unused rows.

Data Set *2*				
Security Level				
Feature/Function/s				
Purpose				
Scope of Records				

Data Notes

<Section available to capture any notes on data to be considered in design, development, testing. As advised from Source Custodian or from the projects perspective.>

Restricted Data Sets

School of Policing & Australian Graduate School of Policing & Security (AGSPS) Student Data	**Response**
1. Are policing, Goulburn, Manly or AGSPS student data within scope of data request?	*YES / NO*
2. Are policing, Goulburn, Manly or AGSPS course or subject related data in scope?	*YES / NO*
3. If yes, who within the School of Policing & Australian Graduate School of Policing & Security (AGSPS) has formally sanctioned?	*Enter N/A or add note with reference to formal approval document e.g. email, minutes.*

Section 2

Source System Data Custodian – Approval

Approval includes use within Target system & Developer access to identified source data for the purpose of inclusion within design, development and testing. This includes both development and QA environments.

Source System	*Enter Source system name as per Section 1 entry*	***<System 2>***	***<System n>***
Data Custodian	*Enter Data Custodian name as per Section 1 entry*	**<enter name>**	**<enter name>**
Phase 1 - Initial Approval to Use	*Approval includes use within Target system & Developer access to identified source data for the purpose of inclusion within design, development and testing. This includes both development and QA environments.*		
1. Initial Approval to Use	Yes / No		Yes / No
Link to Approval Email			
Initial Approval Date			
Any exclusions or known issues			
Nominated Source Testing Contact or Tester			
Additional Notes			
Phase 2 - Production Ready Approval	*When formal notice has been provided to Data Custodian that unit & user acceptance testing satisfactorily completed & new integration interface/s are production ready. On the Data Custodian's signoff, this includes approval for Developer access to respective system production database/tables/files to migrate changes in scope to production environment.*		
Appendix A complete	Yes / No – provide appropriate response	Yes / No	Yes / No
Testing Successfully completed	Yes / No – provide appropriate response & link to test outcome report/s	Yes / No	Yes / No
2. Production Ready Approval	Yes / No		Yes / No
Production Ready Approval Date			
Link to Approval Email			
Additional Notes			
Disclaimer: It is the responsibility of the Target System Custodian (c/-Project Manager) to ensure the data sourced from the authoritative source system is correctly matched for the requirements of the target system, confirmed through unit & user acceptance testing for all business use cases in scope.			

This section will be completed by Information Architect or Data Custodian

This section will be completed by Information Architect or Data Custodian

Appendix A: Source System/s Data Extract Details

Instruction:

Task - *For each source system in scope copy and complete a data mapping table summary of implementation details for the requested data.*

Timing - *Complete as early as possible and prior to seeking approval for phase 2, production ready approval.*

Source Data Mappings

Data Mapping Table

Master Data Attribute	Source System	Source Table	Source Table Field	**Security Class.**	Master Data Object	Target System table/field	Scope of Data Records	Data Tranformation	Access Type	Extract Type	Extract Timing	Data Path *(see key **appendix B**)*
Data Set 1 – Enter name of data set as per section 1												
Program Code	*Banner Student*	SGBSTDN	SGBSTDN_PROGRAM_1	*Level 2*	*Program Enrolment*	*Research Master*	*All current RHDS records*	*n/a*	*read*	*push*	*Scheduled 4am daily*	*Source -> mw -> Target*

Guide to required entry items for each of the above fields within the data mapping table.

Master Data Attribute	*Select from master data definitions, if does not currently exist, leave blank & include a note.*
Source System	*Extract from master data definitions, if does not currently exist, add identified source system*
Source Table	*Extract from master data definitions, if does not currently exist, add identified source system table/file*
Source Table Field	*Extract from master data definitions, if does not currently exist, add identified source system table field*
Security Class.	*Extract from master data definitions, if does not currently exist, indicate security level (Highly Confidential, Confidential/Private, Internal, Public.)*
Master Data Object	*Select from master data definitions, if does not currently exist, leave blank & include a note.*
Target System table/field	*Specify target system schema/table/field*

Scope of Data Records	*Brief description e.g. current records, current & future, future, past & current*
Data Transformation	*Brief note on any transformation of source data e.g. xyz123 to xyz-123*
Access Type	*E.g. read, write, update, delete, read & update, read & create, lookup only (not stored)*
Extract Type	*E.g. Pull on demand, triggered push, …*
Extract Timing	*On update (near real-time), periodic batch transfer, daily update cycle, specified schedule*
Data Path	*Simple description required using appendix A legend ie.* source - igms - mw – target. *Note, can add to legend if required.*

Target System Extract Rule

Shared (Master) Data Object	Extraction Rule – for record set to be used in target system
List entry for each master data object above, if does not currently exist, include note to show link to above new data set.	*Brief, plain English description of extraction/filter rule. If filter is based on an identity grouping, please note to refer to table below.*
E.g. 1. Subject Enrolment	*Only current active enrolments for Wagga internal subjects*
E.g. 2. NEW – Staff Image	*Only staff images with category of 'official' & status of 'current'*

Enterprise Identity Data in Scope

List any IGMS identity data in scope.

A CSU Identity record within IGMS holds the identity attributes of CSU_ID, first name, second name, last name, title, gender, date of birth, email, preferred name (where applicable).

CSU_ID. *When sharing CSU identity records between CSU systems/applications, the unique identifier to be shared is the CSU_ID. Identity identifiers local to an application should not be shared to other applications, e.g. pidm. CSU_D is used for the purpose of maintaining integrity between CSU applications but not for display or disclosure on system or application end user interfaces.*

		Scope of Use	
Identity Attribute	**Purpose & Use**	**Lookup Value**	**Stored Data**
Add name of identity attribute	*Brief note on why attribute required and how it is used within target system*	*Y or N*	*Y or N*
E.g. Date of Birth	*Required as student event management function needs to check participants are over 18.*	*Y*	*N*

Enterprise (Identity) Groups in Scope

List any enterprise groups and memberships to be applied within the scope of this data set where used:

- *as a data record extraction criteria e.g. only Academic Staff timesheet records; and/or*
- *for provisioning user access to a system e.g. provisioning only Academic staff access to a Research Repository*

		Scope of Use	
Enterprise Group	Additional Filter Rule (if applicable)	User Access Provisioning	Data Set Criteria
IGMS enterprise group name OR if new, describe briefly	*Only where applicable eg. only Bathurst campus staff*	*Y or N – i.e. is the group rule to be used for user access of target system*	*Y or N – i.e. is the group rule to be applied to the data set criteria*
E.g. Current Student	*Restricted to only students enrolled for Bathurst internal program*	*N*	*Y*

Data Lifecycle Management – Lifecycle Quality Controls

Describe target system method to manage source data lifecycle changes eg. create, updates, inactive, deletions, archive, disposal.

- Complete for each change type when known and prior to request for production approval.

Source Record Changes	Target System - Data Lifecycle Management
Data Set 1 – *Enter same label to data set 1 as in section 1 of form*	
New	*Brief, plain English description eg. will create new record in target system*
Updates	*Brief, plain English description eg. will keep history & create new record for update in target system*
Inactive	*Brief, plain English description eg. will deactivate in target system record*
De-identified	*Brief, plain English description eg. will de-identify in target system record*
Deletion	*Brief, plain English description eg. will delete in target system*
Data Set n – <label>	
New	
Updates	
Inactive	
De-identified	
Deletion	

Appendix B: References

Data Description

Master Data

Master Data Definitions: Master Data Resources Catalogue

Security Class.

Data Security Classifications: http://www.csu.edu.au/division/dit/eal/portfolios/information/docs/Data_Security_Classification_Scheme1.pdf

Data Path Legend

igms - Identity & Group Management System
mw - middleware, term used to describe CSU data integration technology solution.
mdc - Master Data Cache, a database that stores a copy of master data.
source - the determined originating authoritative data source.
target - the system to access & use authoritative data.
API – Application program interface (API), a method of allowing communication between two systems.
CSV – comma separated values file which allows data to be saved in a table structured format

Add additional items if necessary