## CSU Data Principles Rationale

<table>
<thead>
<tr>
<th>Version</th>
<th>1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRIM file number</td>
<td>-</td>
</tr>
<tr>
<td>Short description</td>
<td>Provides a more detailed description and rationale for the data principles to be applied in consideration to the capture and management of data (assets) within the organisation. It also identifies the associated data standards that directly support the data principle.</td>
</tr>
<tr>
<td>Relevant to</td>
<td>Officers who have a responsibility in the planning, identification, definition, capture or management of data (assets).</td>
</tr>
<tr>
<td>Authority</td>
<td>This background description and rationale of the data principles have been endorsed by the Enterprise Architecture, Director and CSU Data Governance Committee (DGC)</td>
</tr>
<tr>
<td>Responsible officer</td>
<td>Information Architect</td>
</tr>
<tr>
<td>Responsible office</td>
<td>Enterprise Architecture &amp; Liaison, Division of Information Technology</td>
</tr>
<tr>
<td>Date introduced</td>
<td>September 2010</td>
</tr>
<tr>
<td>Date(s) modified</td>
<td>To be determined.</td>
</tr>
<tr>
<td>Next scheduled review date</td>
<td>To be determined.</td>
</tr>
</tbody>
</table>
| Related University documents | [CSU Enterprise Architecture Principles](#)  
CSU Data Principles  
CSU Data Standards  
[Records Management Policy](#)  
[Digital Records Policy](#)  |
| Related legislation | [State Records Act 1998 (NSW)](#)  
[Privacy Act](#)  |
| Key words | data, principles, standards, data architecture, guidelines, rules |
Data Principles Full Description

**Principle 1: Data Determined by Business Needs**

**Definition**
Data captured and used within the organisation is determined by strategic and operational business needs (function). The ability to articulate explicitly the business requirement, context and purpose is essential to determining the required data. This also provides the necessary information and context to inform on data characteristics such as integrity, source, security, and custodian.

**Rationale**
- The investment in capturing and managing data should be to deliver on specific required business needs otherwise the ability to effectively deliver data to support business operations and share information at an organisational level becomes increasingly complex or impossible.

**Benefits**
- Directly informs and supports the ability to deliver quality data, as the business need will inform on the required quality measures and constraints.
- Informs on data governance requirements.
- Identifies most appropriate Data Custodian.

**Risks**
- Increases risk of data issues occurring across the organisation, if the purpose and use of data elements is not clearly understood and communicated.
- Unnecessary data can become a liability in costs, resources, productivity, etc.

**Associated Data Standards**
- Data Asset
- Defined Purpose & Use
- Data Integrity
- Data Custodian
- Authoritative Source
- Single Capture & Validation
- Security Classification
- Availability Classification
**Principle 2: Right Data Captured, Right Data Used**

**Definition**
The task is to accurately match context, description & purpose of a business requirement (i.e. the data question) to a data element that is available or to be created in order to capture the required data. Inappropriate or inadequate data matching will become liabilities or distractions to the organisation, and not the realisation of data assets.

**Rationale**
- To deliver on operational and strategic business requirements, appropriate data needs must be identified, captured and managed in alignment with requirements in order to effectively support and sustain these business activities.
- The availability of a concise definition of purpose and use of data assets can be achieved by understanding the business requirement (including associated rules) that has determined it as an enterprise data asset.
- It is important and sometimes critical to the organisation that the right data is used to deliver services and inform decision making.
- Only data that has a clearly defined purpose should be captured and managed. The capture and retention of unnecessary or superficial data is of no value to the organisation however it can increase associated costs, resources and time in the capture, maintenance and management of this data.

**Benefits**
- Promotes focus on business requirements.
- Enables the ability to create concise data asset definitions that support the capability to deliver very effective management, sharing and governance of data assets. Promotes clarity.
- Support appropriate selection of data assets to deliver on specific business requirements.
- Assists timely identification of missing ‘data’ that is required to support business activities.
- Increases value of data asset to the organization as only data assets that relate to a specific business requirement are captured and maintained.
- Informs on the level of granularity of data required to support business activities.
- Supports confidence, efficiency and effectiveness in the use of enterprise data assets.
- Providing the right data for the task.
- Reduces unnecessary data duplication or overlap.

**Risks**
- Inaccurate matching of data assets to business requirements, inhibits business activities, sustainability, flexibility and responsiveness within a changing environment.
- Data is used for purposes beyond that of its defined purpose, creating unnecessary complexity and dependencies. Introducing artificial limitations on data set that can compromise its defined purpose.
- Problems can be misdiagnosed as ‘data’ issues when the underlying problem is the inaccurate matching of data element to deliver on a specific business requirement (i.e. data question).
- Can become a liability, if inappropriate data captured or maintained. Promotes information overload, a distraction or creates ‘noise’.
- De-values data as an enterprise asset.
- Wasted resources (time, money, staff, technology) in maintaining unnecessary data.

**Associated Data Standards**
- Data Asset
- Defined Purpose & Use
- Data Integrity
- Data Custodian
- Authoritative Source
- Single Capture & Validation
- Security Classification
- Availability Classification
**Principle 3 – Data is an Enterprise Asset**

**Definition Statement**
Data is a valuable corporate resource; it has real, measurable value. Most corporate assets are carefully selected, managed and funded, data is no exception. Data assets are to provide maximum benefit to the enterprise as a whole. However, this principle will not preclude any specific or specialist data requirements.

**Rationale**
- Data is the foundation of information sets that deliver on operational and strategic activities and decision-making, so must carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.
- Data is not ‘owned’ by an organizational unit, but viewed as an asset available to be shared across the organization (within statutory & policy constraints).
- Maximum return on investment requires data asset decisions to align to enterprise-wide drivers and priorities whilst delivering on a specific business requirement.

**Benefits**
- Consistent, reliable data gives users confidence. Improving reuse and sharing capabilities.
- Promotes efficiencies in all other data management & delivery requirements.
- Greater return (value) on investment in the capture and maintenance of data assets.
- Same data asset available for use across the organisation. Removes duplication.

**Risks**
- Inability to identify and manage data as an asset, impacts on ability to effectively respond to operational requirements, strategic or innovative opportunities. This can also significantly increase the resources (staff, time, budget) required to action a change or investigation.
- Poor quality data leads to costs in correction, rework, searching and retrieval and is viewed by decision-makers as unreliable. Every hour or dollar spent as a result of incorrect, missing, inaccessible or misleading data is an hour or dollar not spent on advancing strategic, operational or innovative activities.
- Incorrect non-authoritative data used to inform actions or decisions.
- Multiple, conflicting data sets. Authoritative data source unknown.
- Reduced ability to support an agile and dynamic business environment.

**Associated data standard**
- Data Asset
- Defined Purpose & Use
- Online Management of Data
- Data Integrity
- Authoritative Source
**Principle 4: Authoritative Source**

**Definition**
University data will have an identified authoritative source of truth. The authoritative source is generally identified through the business process that initially captures the data or with reference to a particular context within the lifecycle of the data asset or business deliverable (service or product).

**Rationale**
- One of the benefits of an architected environment is the ability to share data across the enterprise. As the degree of data sharing grows and business units rely upon common data, it becomes essential that the authoritative source for each data set is identified, published and made accessible for sharing.

**Benefits**
- Same data source used across the organisation
- Allows publication of authoritative sources of data, promoting available enterprise data.
- Removes unnecessary data duplication
- Supports efficient management and improves value of data assets

**Risks**
- Incorrect non-authoritative data used to inform actions or decisions.
- Authoritative data source unknown.
- Multiple, conflicting data sets.
- Wasted resources (i.e. time, money, staff, technology) in maintaining duplicated sets of the same data.
- Reduced ability to respond

**Associated data standard**
- Data Asset
- Defined Purpose & Use
- Authoritative Source
- Data Quality
- Single Capture & Validation
**Principle 4: Data is shared**

**Definition**
Users have access to the data necessary to perform their duties, therefore data is shared across enterprise functions and Organisational Units. Data is captured once and used many times.

Open sharing of data and the release of data must be balanced against the need to restrict the availability of classified, proprietary, and sensitive data. This principle of data sharing will continually need to reference the principle of data security. Under no circumstances will the data sharing principle cause private or confidential data to be compromised.

**Rationale**
- To support CSU's 'one university' objective, the single/one authoritative data set must be used across the organisation.
- Data is of no value unless it is shared.
- Timely access to accurate data is essential to improving the quality and efficiency of enterprise decision-making.

**Benefits**
- It is less costly to maintain timely, accurate information in a single application, and then share it, than it is to maintain duplicative data in multiple applications.
- Shared data will result in improved decisions since we will rely on fewer sources of more accurate and timely managed data sets for all of our decision-making.
- Electronically shared data will result in increased efficiency when existing data sets can be used, without re-keying, to create new data.
- Over time will benefit from the increased agility and flexibility to respond to changing data requirements. The speed of data collection, creation, transfer, and assimilation is driven by the ability of the organization to efficiently share these islands of data across the organization.

**Risks**
- Increased islands of data sets across the organization which does not guarantee ‘one view’ or ‘same view’ of the organisation at any given time.
- Increases data management costs (eg. Resources, operational costs, technology solutions & storage, accessibility).
- Reduces return (value) of investment in data capture and management.
- Information sharing may require a significant cultural change. However, sharing information strengthens a culture of working together.
- Lack of accessibility increases inefficiencies in locating and ability to use the right data at the right time.

**NOTE:** This is one of three closely-related principles regarding information: information is shared; information is an asset; information is easily accessible, open and safe. The implication is that there is an education task to ensure that all Organisational Units within the enterprise understand the relationship between the asset value of information, sharing of information, security and accessibility to information.

**Associated Data Standard**
- Data Asset
- Defined Purpose & Use
- Online Management of Data
- Data Integrity
- Single Capture & Validation
- Authoritative Source
- Security Classification
- Availability Classification
- Meta Data Captured
- Lifecycle Management
- Data Custodian
**Principle 6: Data Security**

**Definition**
The security requirements for each data asset or set is classified and implemented in accordance to the defined purpose of use and associated policies or legislative requirements.

**Rationale**
- Classifying data security level informs on the implementation and access management requirements.
- Informs about who can access the data and what they can use it for, along with physical safeguards.
- Required in order to align or implement relevant organisational policies, procedures and other legislative requirements including Privacy Act and State Records Act.
- Enterprise data must also be safeguarded against inadvertent or unauthorized alteration, misuse, sabotage, disaster, or disclosure.
- Supports assessment and decision-making around appropriateness of data being hosted and managed within an external solution.

**Benefits**
- Reduces risk for breaching security policies or laws.
- Supports establishment of an enterprise security classification that can deliver a consistent approach to managing data security across the organisation.
- Provides further clarity and understanding of data requirements that can inform decision-making on capture, use and maintenance of data, increasing the likelihood that an appropriate solution is selected for implementation.
- Promotes a proactive approach and assessment of data security.
- Informs Service Level Agreements with partners (internal & external) around the required mechanisms to enable and maintain of the data lifecycle, the appropriate level of protection.
- Allows the associated resources (including cost) used in the security of data to be used appropriately by accurately matching data to security level to required resources.
- Confidence to the Organisation, stakeholders and clients appropriate data security mechanisms have been put in place.

**Risks**
- Information must be protected to avoid unwarranted speculation, misinterpretation, and inappropriate use.
- Inadequate data security has the potential to undermine the viability or continuation of the Organisation.
- Loss of client and stakeholder confidence in the Organisation.

**Associated Data Standard**
- Data Asset
- Defined Purpose & Use
- Authoritative Source
- Data Integrity
- Data Custodian
- Security Classification
- Lifecycle Management
**Principle 7: Governance**

**Definition**
To ensure data capture, management, and use is aligned with business operational, strategic, and legislative requirements, effective clear responsibilities, accountabilities, controls and coordinating mechanisms or processes must be in place.

**Rationale**
- Ensure that all proposed changes and projects are business-driven and that they align with strategic goals, as well as the architecture principles, best practices and standards.
- Maximize the return on investments and minimize the likelihood of incompatibility.
- Ensure that individual change proposals are optimized from the enterprise perspective, rather than a narrower, possibly limiting individual perspective, i.e. project by project.
- Focus on the ongoing development of the enterprise data architecture.

**Benefits**
- A clear governance structure can avoid duplication of effort, streamline decision-making and improve communication.
- Supports data integrity, security and availability.
- Provide a ‘one university’.

**Risks**
- Increases risk of inability to resolve data issues within the organisation, particularly when it involves more than one stakeholder.
- Reduces ability to identify and manage data risks to the organisation if data governance is lacking.
- Loss of confidence in data that can promote duplication rather than sharing.
- The role of Data Custodian is critical because obsolete, incorrect, or inconsistent data could be passed to enterprise personnel and adversely affect decisions across the enterprise.
- Since data is an asset of value to the entire enterprise, Data Custodians accountable for properly managing the data must be assigned at the enterprise level.

**Associated Data Standards**
- Defined Purpose & Use
- Data Custodian
- Security Classification
- Authoritative Source
- Data Integrity
**Principle 8: Common Data Definitions & Vocabulary**

**Definition**
To provide an enterprise name and description of data assets in order to support a consistent, common understanding of the data, and aid communication across the organization and from various perspectives.

**Rationale**
- Standards and conventions for the consistent approach to the defining of data asset name, description, structure, granularity, format and classification of data should be used to maximise the efficient, manageable capture, discovery and sharing of data assets across the organisation.

**Benefits**
- Optimize for organizational benefit
- Supports a common ‘one university’ view of data assets.
- Greatly assists communication across the different Organisational Units, different levels of management, and with external parties.
- Supports change management.
- Highlights any areas that need clarification, supporting organizational growth and improvement.

**Risks**
- Increases risk of mismatching data requirements with a data asset with the potential to create data issues.
- Increases chance of data duplication.
- Incorrect data is used.

**Associated Data Standards**
- Data Asset
- Defined Purpose & Use
- Data Integrity
- Security Classification
- Lifecycle Management

**Table of amendments**

<table>
<thead>
<tr>
<th>Version number</th>
<th>Date</th>
<th>Short description of amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>