CCS Administrative Procedure
8.10.02-B Data Governance

Implementing Board Policy 8.10.02
Contact: Chief Information Officer, 279-6062

1.0 Purpose

Data are valuable resources for CCS and must be carefully managed. This data governance procedure is intended to ensure that all CCS data are managed as institutional assets, assure consistent and reliable data, and manage such data with a district perspective for fulfilling CCS's mission of instruction, research, and public service.

Data, and ready access to data in its many forms, are vital to the successful operation of CCS. Faculty, staff, and others need appropriate access to CCS data through online inquiry and/or downloads in support of CCS functions. In turn, faculty, staff, and others with access are obliged to appropriately use and effectively protect CCS data. This procedure is intended to supplement, not override, the definition of access to data under the Washington Public Records Act, RCW 42.56, and the Preservation and Destruction of Public Records law, RCW 40.14.

2.0 Scope and Requirements

CCS data are the items of information that are collected, maintained, and used for the continued operations of CCS, specifically administrative data such as fiscal, student, and employee data and other data maintained and safeguarded for CCS operational purposes. This includes data held by central offices as well as data held by departments or individuals.

Other research data, scholarly work of faculty or students, and intellectual property are not covered by this procedure.

For security and retention rules for such data, contact the Office of Records Retention, Institutional Research, and/or the Office of Information Technology.

2.1 Where referenced in this procedure, data encryption shall be accomplished according to current commercially reasonable business practices and CCS IT procedures.

2.2 Data are valuable institutional assets of Community Colleges of Spokane (CCS). Data procedures are needed to ensure that these resources are securely managed and wisely used. Six areas have been identified which define data administration:

Data Access --Inquiry and download access to CCS data

Data Classification--Management responsibility for CCS data

Data Usage --Appropriate use and release of CCS data

Data Maintenance --Upkeep of CCS data

Data Security --Protection of CCS data

Data Retention and Disposition -- Preserving CCS data as required per retention and disposition laws of Washington State (RCW 40.14), and WACTC's General Retention laws

3.0 Data Administration

3.1 Access

3.1.1 **Data Stewards** - CCS data shall be administered by executive officers of CCS, referred to as Data Stewards, who comprise the membership of the Data Governance Council (DGC). The DGC will convene periodically to review policies, procedures, and issues regarding data.

3.1.2 **Data Stewards** - have charge over CCS data and are responsible for its safekeeping. Each Data Steward is responsible, within the bounds of CCS policy, for operational policies and procedures governing inquiry and download access, dissemination, usage, collection, maintenance, and protection of the data in a designated data area. The Data Steward is responsible for the definition and classification of data in that area as well as verifying its authenticity as needed. Documentation characterizing CCS data will be maintained and made available for CCS use.

3.1.3 **Data Custodians** - A Data Steward may delegate any or all of his/her data administration duties to one or more functional area administrators known as a Data Custodian(s); however, the Data Steward retains ultimate responsibility. Data Stewards and recommended Data Custodian(s) for each CCS data set are listed below.

Data Roles at CCS

Data Set	Data Steward	Data Custodian(s) (Example)
Associate Address*	Chief Information Officer CIO	Information Security Officer
Donor	Chief Institutional Advancement and External Affairs Officer	Executive Director CCS Foundation
Facilities	Chief Administration Officer	Director of Facilities
Personnel	Chief Administration Officer	Director of Human Resources
Financial	Chief Financial Officer	Director of Fiscal Services/Controller
Library	VP of Instruction VP of Learning	Deans overseeing Library Services
Institutional Research	Provost/Chief Academic Officer	Managing Directors of Institutional Research

Data Set	Data Steward	Data Custodian(s) (Example)
Program/Class - SCC	Vice President of Instruction	Director of Admissions & Registration Associate Registrar
Program/Class - SFCC	Vice President of Learning	Associate Dean of Enrollment Services Associate Registrar
Student - SCC	Vice President of Student Services	Director of Admissions & Registration Associate Registrar
Student - SFCC	Vice President of Learning	Associate Dean of Enrollment Services Associate Registrar
Public Information	Chief Institutional Advancement and External Affairs Officer	Communications Director

* Includes identity and access to information such as authentication, authorization, individual usage data and email

3.2 Classification

Data stewards will classify the data for which they are responsible in accord with RCW 40.14 according to the following four inquiry access categories.

3.2.1 Public -- Public information that can be or currently is released to the public. It does not need protection from unauthorized disclosure but does need integrity and availability protection controls.

3.2.2 Sensitive -- Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

3.2.3 Confidential -- Confidential information is specifically protected from disclosure by law. It may include but is not limited to:

- personal information about individuals, regardless of how that information is obtained.
- information concerning employee personnel records.
- information regarding IT infrastructure and security of computer and telecommunications systems.

3.2.4 *Confidential with Special Handling* – Confidential information requiring special handling is specifically protected from disclosure by law and for which especially strict handling requirements are dictated, such as by statutes, regulations or agreements. Serious

consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

3.3 **Usage and Responsibility**

CCS data shall be used only in the performance of assigned roles/duties within CCS and in accordance with CCS Procedure 8.10.01-A Acceptable Use of IT Resources unless an approved agreement allows release to an external entity in accordance with CCS Procedure 1.50.02-A Public Records Request.

3.3.1 Each individual with access to CCS data has the responsibility to use those data and any information derived from them appropriately. Individuals will be held responsible for any use made of CCS data under their user IDs and passwords.

3.3.2 CCS data must not be used to promote or condone discrimination on the basis of race/ethnicity, color, creed, religion, national origin, gender, sexual orientation, age, marital status, the presence of any sensory, mental, or physical disability, or whether a disabled veteran.

3.3.3 CCS data must not be used to promote or condone any type of harassment, copyright infringement, political activity, personal business interests, or any activity that is unlawful and/or precluded by CCS policies.

3.3.4 Willful misuse of CCS data, violation of state ethics laws and rules with regard to CCS data, or other breaches of this policy, may result in termination of access privileges, CCS disciplinary action which may include termination of employment, and/or civil and criminal penalties. (See Ethics in Public Service, RCW 42.52, CCS Procedure 8.10.01-A Acceptable Use of IT Resources, and CCS Procedure 1.50.02A Public Records Requests.

3.4 **Maintenance**

CCS data are managed as institutional assets for use by the CCS community. The usefulness and effectiveness of CCS data depend on these data being accurate and complete. The integrity of CCS data shall be maintained by authorized individuals on behalf of CCS.

3.4.1 Data Integrity - Every effort must be made to ensure the accuracy, timeliness, and completeness of CCS data. Data collection and maintenance shall be performed as close to the original source of the data as feasible.

3.4.2 All collection and maintenance of centrally managed CCS data must be processed through centrally managed edit routines. This includes uploaded data or other electronically supplied data values.

3.4.3 Access to data for maintenance purposes shall be authorized by the appropriate Data Steward.

3.4.4 It is the responsibility of each unit that generates and manages institutional data to ensure the application of uniformly high standards in data management to ensure that the integrity is never compromised.

3.4.5 An Administrative Data Rapid Response Team reporting to and acting as advisory council to the Data Governance Council shall be tasked to coordinate with a district-wide perspective the creation, use and maintenance of administrative data to assure appropriate data integration, alignment, definitions, coding processes, practices and standards.

3.5 Security

CCS data shall be safeguarded to ensure its confidentiality, integrity, utility, and availability.

3.5.1 Sensitive or confidential data connected with an individual's name shall be stored securely on physically secured storage devices or media and displayed in an encrypted or otherwise obscured manner. Sensitive or confidential data will be disclosed in full only to specifically authorized individuals as needed to conduct business functions of CCS.

3.5.2 Sensitive and confidential data shall be stored or transported on portable devices/media (laptops/tablets, USB drives, CD-ROM, DVD, etc.) only as required to conduct CCS business functions. Where necessary to store or transport such data on a portable device/medium, they should be protected from disclosure in the event of device/media loss using commercially reasonable business practices such as device locks or data encryption.

3.5.3 Sensitive and confidential data must be protected during network transmission according to commercially reasonable business practices such as secure transport mechanisms or data encryption.

3.5.4 Individual CCS employees and agents are responsible for accessing and implementing security software and tools CCS makes available. A department or individual employee may substitute software or tools that provide a level of security equal to or greater than those provided by CCS, so long as the department or individual employee has obtained all necessary licenses for such use.

3.5.5 All security incidents or suspected incidents involving CCS sensitive or confidential data or personally identifiable information must be reported immediately to the Information Technology Help Desk at 509-533-4357.

3.6 Retention and Disposition

All data and copies of data created or received in the conduct of CCS business are considered public records for the purposes of retention and disposition, and its retention and disposition will be managed in accordance with CCS Procedure 1.50.2-B Records Management.

4.0 Related Information

4.1 RCW 40.14 – Preservation and Destruction of Public Records

4.2 RCW 42.56 – Public Records Act

4.3 CCS Administrative Procedure 1.50.02-A – Public Records Requests

4.4 CCS Administrative Procedure 1.50.02-B – Records Management

4.5 CCS Administrative Procedure 8.10.01-A Acceptable Use of Information Technology Resources

4.6 Contact information for CCS IT Support Information Technology Help Desk: 509-533-4357

Originated: November 2015 Formerly 7.30.10-C
Cabinet approval: May 23, 2016