**University of Colorado Process for Data Classification and System Security Categorization**

Date of Initial Draft: 6/7/13

Date of Last Review: 12/15/13

**Information can be defined as data endowed with meaning and purpose. Information is a significant institutional asset; thereby it is imperative to develop a comprehensive approach to protecting and governing data.** This document addresses the task of enabling availability and accessibility of institutional data for academic, research, functional and administrative needs, while effectively protecting its confidentiality and integrity. Since it is not possible to protect against every possible threat, the main emphasis needs to be placed on protecting mission critical data elements. If mission critical information is protected, the impact of security incidents is significantly reduced. Effective classification of data is a vital step in applying suitable controls for enhancing its confidentiality, integrity and availability.

Ultimately, it will be the responsibility of the Data Governance groups, data and business process owners to identify data management roles, legal requirements, and ensure accountability for both appropriate access and protection of institutional data.

Data Protection strategies:

There will be a two-pronged approach to data protection and management:

Classification strategy: This strategy entails classifying data elements into three categories (Highly Confidential, Confidential, and Public) to undertake appropriate protection measures. This strategy will be more relevant to the data and business process owners who would have responsibility for classifying data as well as individuals (data users) who use or access data on a regular basis.

System Security Categorization and Control strategy: This strategy entails mapping appropriate controls for information type based on the level of risk to the confidentiality, integrity, or availability of information. The strategy will be more relevant to the technical and executive audience (Data owners, stewards and custodians) who are directly responsible for securing the data. This strategy applies primarily to information systems rather than data elements.

The control strategy as defined above may incorporate some elements of the classification strategy in order to fine-tune the controls for the information types.

Classification Strategy explained:

Initial baseline classification of data elements is shown below. The exact data elements in each category will be based upon the decision made by the data and business process owners.

Highly Confidential information:

This category includes data elements that require protection under laws, regulations, contracts, relevant legal agreements and/or require the institution to provide notification of unauthorized disclosure/security incidents to affected individuals, government agencies or media.

This information is only for the “eyes of the authorized individuals” in any form including paper or electronic. This information is prohibited from being (1) transmitted or stored without encryption. (2) Handled on networks or systems without appropriate firewall, monitoring, logging, patching, anti-malware and related security controls.

Documented Data Retention policy is required for handling Highly Confidential information.

The users should contact their IT Security office to ensure protection of data if compensating controls are used to secure the data in place of the above mentioned controls.

The following are the examples of common data types under the “Highly Confidential” information category:

* Protected Health Information
* Social Security Numbers
* Payment Card Numbers
* Financial Account Numbers; including University account numbers, student account numbers, and Faculty and Staff Direct Deposit account numbers
* Driver’s License numbers
* Health Insurance Policy ID Numbers
* Level 4 and 5 of Student data (SSN, NID, Financial Aid (except work study), Loan and Bank Account Numbers, Health Information, Disability, Race, Ethnicity, Citizenship, Legal Presence, Visas, Religion)

Confidential information:

This category includes data elements not usually disclosed to the public but are less sensitive than Highly Confidential data. If a legally required and applicable, Colorado Open Records Act (CORA) request is submitted, these records may be released. This information is protected by (1) Ensuring authenticated access on a need to know basis (2) Not using any electronic mediums and services (Emails, file shares, etc.) other than those provided or approved by the institution to transmit/store data (3) Storage on machines with latest anti-virus, security updates installed and residing on networks that have appropriate security controls in-place (Firewalls, monitoring, logging).

The following are the examples of common data elements under the Confidential information category:

* Faculty & Staff personnel records, benefits, salaries and employment applications
* Admission applications
* University Insurance records
* Donor contact information and non-public gift amounts
* Fundraising information
* Non-public policies
* Internal memos and email, and non-public reports
* Purchase requisitions, cash records, budgetary plans
* Non-public contracts
* University and employee ID numbers
* Level 2 and 3 of Student data (Military Status, Veteran’s Status, GPA, Probation, Suspension, COF, Service Indicators, All non-directory data not listed and Work Study Information, Gender, Birthdate, Dorm, Emergency Info, Student ID, UUID, Residency)

Public information:

* Any information on University websites to which the data owner allows access without authentication
* Information made freely available through the institution print material
* Directory information

System Security Categorization and Control Strategy explained:

FIPS 199 defines Information type as “A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.”

FIPS 199 & NIST 800-60 provides a framework for mapping types of information and information system resources to security risk categories. Ultimately a security category can be represented **as Security Category information type = {(confidentiality, impact), (integrity, impact), (availability, impact)};** where the acceptable values for potential impact are low, moderate, or high. Processes defined by FIPS 199 results in a wide variety of information types that are associated with a business processes, operations and sub-functions. Examples of information types include student information, administrative information, or collections information

At CU, all business groups and departments handle at least one information type. For example, the Registrar’s office at CU handles with student information while the Office of the Treasurer handles financial information**.** To map effective controls, it is critical for every department to identify all the information types it handles. There could also be a sub-type definition within an information type. For example, financial information under the CU System Office of the Treasurer could include the subtypes - Payment card data and University account numbers.

The next step would be to map impact levels for each of the information type and sub types. For any information type, a level of impact is assigned to each of three security categories. Following definitions are defined for security categories:

**Confidentiality**— “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…” [44 U.S.C., Sec. 3542]. A loss of confidentiality is the unauthorized disclosure of information.

**Integrity** — “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…” [44 U.S.C., Sec. 3542]. A loss of integrity is the unauthorized modification or destruction of information.

**Availability**— “Ensuring timely and reliable access to and use of information…” [44 U.S.C., SEC. 3542]. A loss of availability is the disruption of access to or use of information or an information system.

The impact levels are defined as high, moderate and low.

The potential impact is **high** if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (1) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (2) result in major damage to organizational assets; (3) result in major financial loss; or (4) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

CU uses the following as guides for defining impact:

* Financial – direct or indirect monetary costs to the institution where liability must be transferred to an organization which is external to the campus, as the institution is unable to incur the assessed high end of the cost for the risk; this would include for e.g. Use of an insurance carrier
* Reputation – when the impact results in negative press coverage and/or major political pressure on institutional reputation on a national or international scale
* Safety – when the impact places campus community members at imminent risk for injury
* Legal – when the impact results in significant legal and/or regulatory compliance action against the institution or business.

The potential impact is **moderate** if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (1) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (2) result in significant remediation cost to the university

CU uses the following as guides for defining impact:

* Financial – direct or indirect monetary costs where liability is transferred to the campus as the business unit/school is unable pay the assessed high end cost for the risk
* Reputation – when the impact results in negative press coverage and/or minor political pressure on institutional reputation on a local scale
* Safety – when the impact noticeably increases likelihood of injury to community member(s)
* Legal – when the impact results in comparatively lower but not insignificant legal and/or regulatory compliance action against the institution or business.

The potential impact is **low** if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (1) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (2) result in minor damage to organizational assets; (3) result in minor financial loss; or (4) result in minor harm to individuals.

CU uses the following as guides for defining impact:

* Financial – impact results in direct or indirect monetary costs to the institution where business unit/school can solely pay the assessed high end of the cost for the risk
* Reputation – when the impact has a nominal impact and/or negligible political pressure on institutional reputation on a local scale
* Safety – where the impact has nominal impact on safety of campus community members
* Legal – when the impact results in none or insignificant legal and/or regulatory compliance action against the institution or business.

 The definitions are provided only as guides and should not be considered without the context of the broader environment. While making the impact determinations, it is important to realize that the value of an information type may change during its life cycle. So, information subtypes may include the relevant statements. For example, consider the case of contracts as an information type. The sub types could be Contracts-initial discussion, Contracts-finalized, Contracts-terminated and all these subtypes may have different impact levels for the security categories.

For better understanding of information type categorization, please refer to Appendix A.

Process steps:

* Each department needs to identify its information types and sub-types.
* For every information type and sub-type, determine the impact levels for each of the security categories. Office of Information Security or Campus IT Security Office can assist in this effort.
* Baseline security standards will be mapped to the systems that handle the above information types. High water mark (explained on page 8 in Appendix A) will be used in cases where systems are handling multiple information types.
* The baseline controls will then be implemented after an approval from the data and business process owners.
* These controls will be assessed and monitored for their effectiveness and changes will be made, if necessary

Definitions:

Encryption standards:

All the encryption requirements mentioned in this document should meet at least Triple DES or AES standards. Further guidance on the implementation can be found here:

<http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf>

**Appendix A**

Example of information type categorization from NIST 800-60 publication regarding Financial Management information:

|  |  |  |  |
| --- | --- | --- | --- |
| *Financial Management* | Confidentiality | Integrity | Availability |
| Asset and Liability Management | Low | Low | Low |
| Reporting and Information | Low | Moderate | Low |
| Funds control | Moderate | Moderate | Low |
| Accounting | Low | Moderate | Low |
| Payments | Low | Moderate | Low |
| Collections and Receivables | Low | Moderate | Low |

For the Funds control information type in the above table,

Security Category funds control = {(confidentiality, moderate), (integrity, moderate), (availability, low)}

To enable a better understanding of how the above impact levels were assigned to the security categories for Funds control, here is the related information from the NIST 800-60 publication:

*Funds Control includes the management of the Federal budget process including the*

*development of plans and programs, budgets, and performance outputs as well as financing. Federal programs and operations through appropriation and apportionment of direct and reimbursable spending authority, fund transfers, investments and other financing mechanisms. Funds control management includes the establishment of a system for ensuring an organization does not obligate or disburse funds in excess of those appropriated or authorized. The recommended security categorization for the funds control information type is as follows:*

*Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}*

*Confidentiality*

*The confidentiality impact level is the effect of unauthorized disclosure of funds control information on the ability of responsible agencies to develop plans and programs, budgets, and performance outputs and outcomes; and to finance Federal programs and operations through appropriation and apportionment of direct and reimbursable spending authority, fund transfers, investments and other financing mechanisms. In general, unauthorized disclosure of funds control information, particularly of budget allocations for specific programs or program elements, can be seriously detrimental to government interests in procurement processes. In many instances, such unauthorized disclosure is prohibited by executive order or by law (e.g., Federal Acquisition Regulation). Premature release of draft funds control information can yield advantages to competing interests and seriously endanger agency operations – or even agency mission.*

*Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of funds control information for programs that process classified or high-impact information can give adversaries damaging insights into details of agency plans, priorities, and operations. (Classified programs and systems are outside the scope of this guideline.) In rare cases, actions taken based on unauthorized disclosure of funds control details can pose a threat to human life or a loss of major assets, so the confidentiality impact would be high.*

*Recommended Confidentiality Impact Level: While, in many cases, unauthorized disclosure of funds control information will have only a limited adverse effect on agency operations, assets, or individuals, the potential for serious harm is such that the provisional confidentiality impact level recommended for funds control information is moderate.*

*Integrity*

*The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Funds control activities are not generally time-critical. An accumulation of small changes to data or deletion of small entries can result in budget shortfalls or cases of excessive obligations or disbursements.*

*Recommended Integrity Impact Level: In most cases, the adverse effects of consequent negative publicity on mission functions, image or public confidence in the agency can be serious. Therefore, the provisional integrity impact level recommended for funds control information is moderate.*

*Availability*

*The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the funds control information. Funds control processes are generally tolerant of delay. Typically, disruption of access to funds control information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.*

*Recommended Availability Impact Level: The provisional availability impact level recommended for funds control information is low.*

As discussed in the classification structure document, the departments can decide to map controls to information sub-types. To provide more flexibility, there could also be an aggregation for every department. Thus, in the above sample table, the whole Financial Management information category could just have one set of impact levels using a **“High water mark”** where, the highest impact in each of the security categories could be chosen for the information category. Using the high water mark concept, the entire above table could simply be represented as:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Confidentiality | Integrity | Availability  |
| Financial Management  | Moderate  | Moderate  | Low |

It is important to note that the above consolidation does not substitute the need to define the information types and sub-types clearly.