8020.S000 Information Security Risk Management – Exception Standard

Implements:	CSU Policy #8020.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8020.0.shtml

Introduction

A campus may decide to allow exceptions to CSU or campus policies, standards or practices. Campuses must develop criteria for determining the organization with authority to approve an exception (i.e. manager, ISO, CIO, data owner, or combination of personsas appropriate). Exceptions may be granted when the campus decides, after a risk assessment, that there are adequate compensating controls. When adequate compensating controls do not exist, the campus must follow it's risk management process to ensure that the exception is approvied by an appropriate Vice-President or other campus administratior with fiscal responsibility for addressing the result of risk acceptance.When a campus grants an exception or accepts a risk, it must comply with the following minimum standards to identify, monitor and periodically review the exception.

1.0 Exception Process

Each campus must develop a process for documenting, reviewing and approving exceptions.

1.1 The campus exception process must include the following:

a) Required management approval from the requesting organization's appropriate administrator.

b) A description of the nature and types of exceptions which must be reviewed by the campus ISO.

c) A process and timeline for periodic review of granted exceptions in which periodic reviews must be performed at least every three years.

d) A record documenting the exception process including:

   a. Contact information for individual and/or organization requesting the exception.

   b. The policy, standard or other requirement to which exception is being requested..

   c. Justification for the proposed exception.

   d. Description of any proposed compensating control or mitigating circumstance.

   e. Information security risk analysis using the campus risk assessment methodology.

   f. Designation (i.e. "high", "medium") of risk under the campus' risk assessment methodology.

   g. Appropriate approvals.

e) Retention of exception review and approval records for at least 3 years after the exception is withdrawn or expired, or as required by applicable records retention schedule.

2.0 Periodic Review of Granted Exceptions

Exceptions must undergo periodic review and approval by appropriate administrators.

2.1 The exception review process must include:

a) Periodic review as per the schedule established in §1.1(c).

b) Confirmation from the requestor of whether or not the exception remains necessary.

c) Review sufficient to determine if controls remain adequate to mitigate risk.

d) Update of the exception record to reflect changes and record completion of the review including:

   a. Updated approval from changed management or organization.

   b. Any changes in hardware, software, policy or standard relevant to this exception.

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.0	6/10/2014	Macklin	First draft – ISAC development team	All
1.1	2/24/15	Macklin	CISO comments/ISAC development team	1.1, Intro
1.2	3/1/15	Macklin	CISO comments	1.1, Intro
1.3	3/1/15	Macklin	CISO comments	1.1(c)

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
3/2/15	P&S Committee with CISO	CISO comments reviewed and discussed (3/2/15 – 10am). This version includes those comments. Next steps collaborative review.
3/2/15	Leslie DeCato	Added Draft Watermark. Submitting to ISAC/ITAC for Review.
3/3/15	Perry	Reviewed and accepted all (track changes). Submitted to DeCato for ISAC/ITAC Review. Review period will be 3/6/15 to 4/10/15.
6/4/15	Perry (CISO)	Approved for Posting