

## ITS Program Charter

**Program Title:** *Campus Security Program*

### *Section I: Program Summary*

<p><b>Background and Problem Statement:</b></p>	<p>A secure IT infrastructure is important for every aspect of campus business. It is important to protect the security and integrity of university assets and information, both from the perspective of legal compliance and in order to maintain confidentiality, integrity, and availability of information.</p> <p>Historically, UCSC has had a bottom-up approach to IT security, addressing specific identified security needs, threats and vulnerabilities as they are encountered. While this approach is both useful and necessary for addressing immediate or general security needs, UCSC also needs a way to protect campus assets, information and reputation in a strategic manner that is responsive to common security needs across campus, consistent with campus values and priorities, and balanced against campus resources.</p> <p>Information technology enables campus processes, including teaching, research and business, making IT security a campus issue, not just an IT issue. Security programs must, therefore, approach security from both the bottom-up, need-based side mentioned above, as well as from a top-down, overall campus perspective, and must be consistent from both directions.</p> <p>A top-down, executive-supported campus-level approach to IT security establishes security policy and practices that apply to the entire campus population. It creates a climate of security awareness that acknowledges each campus member’s responsibility for the security and protection of university assets and information. A top-down security program would necessitate campuswide risk assessment to establish an overall picture of the current state of campus risk and compliance, and develop appropriate, coordinated security responses.</p> <p>This program provides the framework for a top-down campus security program and an overall context for a series of projects supporting this program.</p>
<p><b>Values/Principles:</b></p>	<p>It is important to protect the security and integrity of university assets and information, both from the perspective of legal compliance and in order to maintain confidentiality, integrity, and availability of information. An effective security program creates a climate of security awareness and support. It also reveals and mitigates areas of risk and non-compliance. A coherent campuswide security program must be responsive to common needs, consistent with campus values and priorities, and balanced against campus resources.</p>
<p><b>Benefits and Return on Investment:</b></p>	<p>Adding a top-down campus security program will result in a more comprehensive, complete approach to campus IT security that ties into overall campus and IT strategic planning and better represents campus business needs and priorities. On a more fundamental level, effective implementation of this program will result in a comprehensive set of campus IT security policies and practices, a more complete picture of campus IT assets, risk, and state of compliance, a standard incident response plan, and a campus community that is educated about their personal roles and responsibilities with respect to IT security.</p>
<p><b>Approach and Deliverables:</b></p>	<p>The Campus Security Program provides the framework for a top-down campus security program and an overall context for a series of projects supporting this program. The goals of this Program are to:</p> <ul style="list-style-type: none"> <li>➤ Uphold an IT environment that is aligned with campus priorities by maintaining confidentiality, integrity, and availability of information</li> <li>➤ Enhance the status of the University by ensuring technical compliance with legal and policy constraints</li> <li>➤ Develop procedures and training to ensure that IT customers are aware of their</li> </ul>

# ITS Program Charter

**Program Title:** *Campus Security Program*

	<p>roles, responsibilities and campuswide security practices with respect to IT resources</p> <ul style="list-style-type: none"><li>➤ Develop an assessment toolkit and central security solutions</li><li>➤ Support campus business continuity</li></ul> <p>Acceptance of this Charter will indicate campus approval for the overall program.</p> <p>The following projects are currently identified as separate, but related components of this program. Each will be chartered separately and will have separate budgets and governance structures: These projects will span a 2-3 year timeline. Project #1 is fundamental for this Program and should be completed first. The other projects will incorporate a blend of concurrent and staggered implementation. Please see the general timeline at the end of this document for initial staging and timing estimates.</p> <ol style="list-style-type: none"><li>1. Develop roles and responsibilities for all UCSC IT users.<ul style="list-style-type: none"><li>• Project currently under development</li><li>• This project lays the groundwork for this Program, establishing that all individuals who use campus information resources have a role and responsibilities in ensuring the security of these resources.</li><li>• This project has a 6-month timeframe.</li></ul></li><li>2. Identify and document existing, generally-accepted UCSC IT security practices, and assess appropriateness/desirability; Compile recommended set of IT security practices for UCSC based on this assessment.<ul style="list-style-type: none"><li>• The first part of this project is a prerequisite for project #3, below.</li><li>• This project has a 1-year timeframe.</li></ul></li><li>3. Map existing IT security practices to IS-3 and identify gaps; Identify projects to address gaps.<ul style="list-style-type: none"><li>• The first part of project #2, above, is a prerequisite for this project.</li><li>• This project has a 6-month timeframe.</li></ul></li><li>4. Develop a standard campus incident response plan<ul style="list-style-type: none"><li>• This project will, for suspected and confirmed breaches of campus IT assets, develop standard mechanisms for reporting and documenting incidents, determining notification requirements, implementing remediation strategies, and reporting to management.</li><li>• The scope of this project does not extend to incident management</li><li>• This project has a 10-month timeframe.</li></ul></li><li>5. Develop and implement campus IT risk assessment<ul style="list-style-type: none"><li>• Project currently under development</li><li>• This is a multi-phase project that will develop a toolkit and resources for risk assessment and will likely result in recommendations for additional projects based on the information obtained from the risk assessments.</li><li>• This project has a 2-3 year timeframe.</li></ul></li><li>6. Develop security training and education program for all campus users<ul style="list-style-type: none"><li>• This project creates a mandate for IT security training and education for the campus community and develops training and education requirements for different populations of IT users.</li><li>• All projects under this Program incorporate a training and education component. Their outputs will inform this project and determine some of its content.</li><li>• This project has a 6-month timeframe for establishing a mandate and framework. Training content and delivery mechanisms will be developed over a 2-year timeframe in conjunction with the other projects under this Program.</li></ul></li></ol>
--	--

## ITS Program Charter

**Program Title:** *Campus Security Program*

<b>Scope, Customers, System Users:</b>	<p>This program applies to all users of campus IT resources. If adopted, an implied goal is to change campus culture regarding security. Both this cultural change and the projects associated with this program have a campuswide scope.</p> <p>Within ITS, outputs of the projects under this program will inform the Security Architecture project, interact with OPM for coordination and development of training and education as well as for communication, result in recommendations for additional ITS projects, and both support and heavily involve Security.</p>
<b>Sponsor: Program Leader: Program Manager:</b>	<p>Sponsor: Vice Provost of Information Technology, Larry Merkley          Leader: Director IT Services, Janine Roeth          Manager: Community and Compliance Service Manager, Julie Goldstein</p>
<b>Technical Features</b>	<p>The outputs of this program will typically be policy, procedures, practices, education and communication. This program may lead to technical solutions in partnership with Security Architecture. There may also be a computer-based component to the education and outreach portions of this program.</p>
<b>Cost/Budget for initial phase:</b>	<p>The budget for the Campus Security Program will be the total of the budgets of all of the projects under the program. Each Campus Security Program Project will be chartered separately, and the budgets will be determined separately. There is no cost associated with the charter of the Campus Security Program beyond the staff time associated with its development and review.</p> <p>The projects under this program will affect the entire campus community and need to be highly collaborative both within and outside of ITS. The types of resources that will be needed include short- and long-term representation on project teams and workgroups from ITS (including departmental representation), client constituencies across campus, and internal audit. There is also the possibility of bringing in outside consultants to help with the development or implementation of the Risk Assessment project, and perhaps with other projects, if there is an identified need for specific outside expertise.</p>
<b>Completion Date for initial phase:</b>	<p>Start Program Charter by July 5<sup>st</sup>, 2005; Adoption by ???</p>

**Approval:**

*This approval is an authorization to proceed with the program and concurrence with the terms of the program.*

\_\_\_\_\_  
Program Leader

\_\_\_\_\_  
Date

\_\_\_\_\_  
Program Sponsor

\_\_\_\_\_  
Date

# ITS Program Charter

**Program Title:** *Campus Security Program*

## General Timeline for Campus Security Program Projects

2005					2006												2007												2008											
Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun					
Roles and Responsibilities																																								
											Identify & Document Existing Practices; Compile Recommended Set of Practices																													
											Map Practices to IS-3; Identify Projects																													
					Campus Incident Response Plan																																			
Risk Assessment																																								
											Develop Security Training and Education Program Complete Mandate & Framework																													