DRAFT ITAC SECURITY CRITICAL ISSUES

	CRITICAL ISSUE	DESCRIPTION/PROBLEM STATEMENT	EXAMPLES OF THIS ISSUE	GOAL(S) FOR THIS ISSUE	CURRENT ACTIONS TAKING PLACE TO MEET GOAL	FUTURE ACTIONS NEEDED TO MEET GOAL
1	Large number of unmanaged or mismanaged computers on our network.	UCB has more than 45,000 systems on our network and a majority of these systems are either unmanaged or inadequately managed. These include student computers, faculty and staff systems in off-campus locations, and computers in departments that lack professional support. Even in departments with adequate resources available, many computers are administered by non-professionals out of convenience or tradition. There is no way to track or ensure the integrity of these systems, or to monitor activities. This is a great threat to our ability to fulfill our missions.	▪ Res Hall has over 6000 student systems, all of them are self-managed. ▪ SNS has blocked network accesses for over X systems in the past 12 months. ▪ In EECS, 2 out of 5 registered Windows systems were compromised by “blaster”, with over 65% of the graduate student laptops were compromised.	▪ An automated certification-on-entry setup for devices to gain access to our network. ▪ Inventory (database) of all campus networked devices. ▪ Adequate authority to enforce IT policies and standards.		

DRAFT ITAC SECURITY CRITICAL ISSUES

	CRITICAL ISSUE	DESCRIPTION/PROBLEM STATEMENT	EXAMPLES OF THIS ISSUE	GOAL(S) FOR THIS ISSUE	CURRENT ACTIONS TAKING PLACE TO MEET GOAL	FUTURE ACTIONS NEEDED TO MEET GOAL
2	Lack of adequate resources to bring campus systems into compliance with minimum standard.	Campus recently adopted the “minimum security standard” policy, effective May 2004, with a grace period of 12 months. Many of our existing networked computers do not comply, either due to lack of expertise, staffing, or availability of software, or outdated hardware configurations. Systems not in compliance with this policy can be denied networked access. Campus also has provisionally passed “DMUP” which requires data classifications and ownership identification, as well as proper protection for certain data. Failure to comply could put the University at risk for violation of state or federal laws. UCB currently does not have any IT organization to provide comprehensive services to assist individual departments to meet these requirements. User level consultations, evaluations, training, etc. are not readily available. Existing system/desktop management support is not viable for many departments. Funds for technology refresh do not exist.	▪ Technology refresh has not been high priority during budget planning. ▪ There is no campus organization funded to provide the tracking, monitoring, and consulting for individual departments or organizations to be in compliance with the IT policies (such as DMUP). ▪ Staff resources in most departments have already been stretched due to the recent budget cuts. ▪ One of the major concerns from Academic Senate and Deans/Chairs with respect to DMUP is the mandates it imposes but are unfunded. ▪ DMUP calls for an “office of records” to be established and act as a record keeping for data classifications, however, funding for this, as well as staffing to review and ensure compliancy, is not addressed in the policy.	▪ Create a cost-effective service infrastructure to bring systems into compliance. ▪ Create an IT audit/consulting organization that is responsible for the auditing of compliancy to policies, reviewing security plans submitted, and providing advises and assistance to the individual groups. ▪ Emphasize the mandates for SNS, especially the educational/training component, by allocating adequate permanent budget to SNS. ▪ Create a convenient budget process to help departments or organizations obtain new hardware. ▪ Provides cost-effective IT services that meets campus needs.		

DRAFT ITAC SECURITY CRITICAL ISSUES

	CRITICAL ISSUE	DESCRIPTION/PROBLEM STATEMENT	EXAMPLES OF THIS ISSUE	GOAL(S) FOR THIS ISSUE	CURRENT ACTIONS TAKING PLACE TO MEET GOAL	FUTURE ACTIONS NEEDED TO MEET GOAL
3	Need of IT security related education and cultural change.	The cultural climate in UCB has long tolerated or even celebrated a mixed model in which centralized, distributed, and highly autonomous support schemas coexisted. The culture on campus has been largely value neutral regarding these models and there is a lack of awareness concerning the security implications to this “anything goes” environment. Increasing awareness of security issues is limited by the difficulty of educating all relevant decision-makers in our environment. Effectively educating the campus on computer security issues is also impeded by the lack of resources for SNS to fulfill the educational component of their mandate.	▪ No funding for user awareness and training for SNS even when it is part of group’s mandate. ▪ Current IS&T outreach to other campus IT constituents is limited to self-initiated mailing lists and user groups. ▪ IT awareness is not built into student orientation. ▪ No outreach to faculty; only limited trainings (mostly are application based) are available to staff.	▪ IT orientations for incoming students. ▪ Mandatory IT professional certification. ▪ Periodic campus wide trainings for different focused groups, including faculty.		