DRAFT Security Resolution Document

The following resolutions result from the necessity of reducing the vulnerability of the computing environment – the campus networks and the devices connected to them – used to conduct University business. This necessity arises from a sharply different landscape in both IT security and regulatory complexity, and, consequently, spiraling remediation costs and legal, fiscal and media liability for the institution.

These resolutions address the need for broad community awareness, acceptance and accountability for security at all levels of network and device services. The community represents individuals that use computers and networks as part of their university responsibilities (network users), organizations that provide local computer and network services and campus-wide network services (service providers) and extends to groups that implement and monitor network and security policies (service monitors).

It is broadly acknowledged that the primary role of service providers and monitors is to maintain the integrity of the network and related services to enable campus business to be conducted in a timely, efficient and secure manner. In doing so, it is the responsibility of the service providers and monitors to work in a coordinated manner to take protective measures to forestall disruption and to take responsive action to stop disruptive or malicious attacks in progress. The institution’s obligations will sometimes require executive decision-making coordination that can potentially affect service providers. Within this context the following resolutions are meant to delineate and clarify levels of responsibility:

Original wording: OIT, working in conjunction with CTS and local administrators will proactively work to minimize threats to the campus network.

1. The Office of Information Technology, in coordination with Communication Technology Services, and local network providers will work proactively to minimize threats to the campus network. This includes educational awareness activities, timely security alerts, traffic monitoring and shaping, and agreed upon levels of network scanning and reporting.

Original wording: All devices connecting to the campus network must meet minimum security standards as must the network to which they attach.

2. Each device that connects to a network must meet minimum security standards. Standards must be reasonable and flexible to balance the requirements of people who use the network to conduct their duties with the responsibilities of those who protect the network and the devices connected to it. Standards must be broadly communicated, easily adaptable and widely accepted as reasonable.

Original wording: Each campus unit is responsible for its own impact institutionally, on the campus backbone network and beyond.

3. Each unit (individual user, business unit or academic department) that connects to a network service is responsible for its impact on the entire community of networks.
which includes local, backbone, and Internet services. There must be clear communication of risks and consequences for non-compliance and avenues for recourse when disputes arise. Any delineation of consequences must be jointly formulated by individuals representing a broad spectrum of the university community.

**Original wording:** During a security event, CTS will first protect the campus backbone network and isolate the problem traffic, network or hosts.

**Revision one wording:** During a security event, each network service provider will first protect the network for which it is responsible to isolate the problem traffic, network or hosts. After the immediate threat has been contained, both central and local providers will coordinate to determine the cause and resolution of the problem and promptly communicate any actions taken to all relevant individuals and units.

4. During an event which adversely impacts the UCLA campus backbone network, or significantly affects an external network, CTS will isolate and block the problematic traffic [inbound/outbound], networks or hosts. Concurrently, each network service provider will protect the network(s) for which it is responsible to isolate and block the problem traffic, networks or hosts. After the immediate threat has been contained, both central and local providers will coordinate to determine the cause, identify short-term/long-term resolutions of the problem, and promptly communicate actions taken to all relevant individuals and units.

**Original wording:** There need to be consequences for non-compliance and an avenue for recourse when disputes arise.

This is addressed in the first three paragraphs of the document.