Network Security Incident Handling

“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.” (Excerpted from the UCLA Security Resolutions document adopted by the ITPB March 2004.)

Roles and Responsibilities

Note: Expected final destination: New campus security

Network Operations Center (NOC)

1) The NOC fields incoming reports of network problems for UCLA (24x7 for telephone calls). When so notified, the NOC in turn notifies the appropriate Network Coordinator (NC) and follows the incident through to closure.

2) In the event of a security incident of the campus backbone network or its shared infrastructure (whether disrupting UCLA or UCLA disrupting others), the NOC will act, starting with the least disruptive means and escalating as appropriate (documented in UCLA Procedure 350.6).

3) Recourse: A pattern of failures in responding to NOC incident notifications by an organization will be referred to the IT department head and without reasonable response then escalated to the Dean or Vice Chancellor.

Campus backbone aggregation points

4) Each area directly connected to the campus backbone network must designate a limited number of Network Coordinators who will work with the NOC to resolve network problems associated with the range of IP addresses under their control. The department head must maintain up-to-date contact information on file with the NOC for incidents occurring outside of business hours (e.g., pager, cell phone, home phone).

5) A Network Coordinator must be an employee of the university. If an organization does not have the resources to have a permanent NC, the organization’s M.S.O. may serve as the organizational NC.

6) A Network Coordinator is expected to be available on a 24x7 best-effort basis.

7) A Network Coordinator must protect network resources and remove from the network any system that is causing wider disruption if the problem cannot be resolved in a timely manner.
Procedures when a system or network is causing disruption

Note: Expected final destination: UCLA Procedure 350.6 (Data Services)

8) Current text: “Network activity that seriously disrupts, degrades, or threatens the performance or function of the CBN will be considered an emergency circumstance as defined in the UC Electronic Communications Policy. Under such conditions, CTS may elect to protect the CBN by implementing a temporary block to contain the disruptive traffic. When such an action is taken, CTS Network Operations will notify, as soon as possible, the Network Coordinator(s) (NC) responsible for, or affected by, the block, as well as the UCLA IT Security Coordinator. The scope of the block will be the minimum feasible and necessary to overcome the disruption. The block will be removed when the NC warrants that the disruptive traffic has ceased.”

General procedures by the NOC

9) When the NOC is notified of a system or network causing disruption (to UCLA or to others), the NOC will first attempt to contact the organizational NC for problem resolution using the contact information on file provided by the organization.

10) If the NOC is unable to immediately get in contact with an NC, it will leave a message but may take other steps in order to isolate traffic and protect the campus backbone. The NOC will begin with the least disruptive means available to deal with a network security incident (rerouting traffic, isolating the offending machine or throttling traffic to/from that computer).

11) If the NOC needs to apply an ACL rule, the NOC shall notify the NC so that the department is aware of the measure taken and can implement a similar ACL locally. The NOC will maintain a list of current ACL rules in a form accessible by the NC.

12) The NC assumes responsibility for an incident after notification by the NOC. The NOC can expect a reply, as quickly as is reasonably possible, with a suggested course of problem resolution and a suggested time frame for problem resolution.

13) When so notified by the NC that the incident has been resolved, the NOC will close the incident.

Suggested general procedures for a Network Coordinator

Note: These procedures are not expected to be included in UCLA Procedure 350.6.)

14) The NC assumes responsibility for an incident after notification by the NOC and replies, as quickly as is reasonably possible, based upon the urgency which may be specified by the NOC, with a suggested course of problem resolution and a suggested time frame for problem resolution.

15) The NC will begin with the least disruptive means available to isolate the problem (rerouting traffic, isolating the offending machine or throttling traffic to/from that
computer), but in severe cases may shut off the system, the subnet or backbone network access to the problem system until there is resolution by the organization or owner of the offending system. In all cases, notification of the steps taken will be sent to the owner of the system, by whatever means are available, (help desk, local web site, telephone messages, etc.) as soon as is reasonably possible.

16) When the problem has been resolved, the NC will affirmatively close the incident with the NOC. By sending an email which includes an identification of the system, a brief reference to the problem and the resolution.

**Emergency circumstances for the NOC**

Note: Definitions from the UC Electronic Communications Policy:

17) Emergency circumstances: Circumstances in which time is of the essence and there is a high probability that delaying action would almost certainly result in compelling circumstances.

18) Compelling Circumstances: Circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policies listed in Appendix C, Policies Relating to Non-Consensual Access, or significant liability to the University or to members of the University community.

19) Time-dependent, Critical Operational Circumstances: Circumstances in which failure to act could seriously hamper the ability of the University to function administratively or to meet its teaching obligations, but excluding circumstances pertaining to personal or professional activities, or to faculty research or matters of shared governance. Examples: A rapidly spreading “zero day” event such as Slammer.

20) Emergency and time-dependent, critical operational circumstances will require the NOC to take immediate steps and then notify the appropriate NC (or all NCs, as appropriate), by whatever means are available, as soon as is reasonably possible.

21) Network access to a problem system can be blocked until there is resolution by the organization.

22) The NOC will maintain a list of any ACLs being currently applied in a form accessible by NCs.

23) If a network is behind a NAT device and the NOC cannot isolate the specific device causing disruption, the NOC will throttle bandwidth and/or shut off connectivity in order to contain the damage. This will impact all systems behind the NAT device. For this reason it is not recommended that departments use NAT at the aggregate backbone connection.