

## Policy on Departmental Security Contact Person

- Reference:** CNS-P-DEPARTMENT-CONTACT      **Revision:** B
- Supersedes:** None
- Purpose:** The purpose of this policy is to ensure that all departments, divisions and centers can be contacted in the event of a computer or network security incident. The ability to quickly contact responsible departmental personnel and have them take appropriate action can mitigate the negative effects of an incident both locally in the department and more globally throughout AUBnet and the Internet.
- Source:** Computing and Networking Services (CNS).
- Approved by:** Nabil Bukhalid, Director of CNS      **on:** October 3, 2003  
Peter Heath, Provost      **on:** Pending
- Applicability:** This policy should in principal apply to all organizational entities within AUB, for example: academic department, administrative department, or research centers. Although larger organizational units, such as schools, may choose to consolidate their security contact function under a single address, an essential requirement is that the designated contact be able to identify responsible administrators for every networked computer within their department(s).
- Background:** Like many universities, AUB is experiencing an increase in unauthorized attempts to access its network and computer systems. Attempts to break into campus computers are a regular event.
- Risks to our academic mission are very serious. The loss or corruption of information or access to information on research or instructional workstations and servers, student records, and financial systems could greatly hinder the university work. AUB has a responsibility to secure its computers and networks and to respond quickly to cyber threats. A compromised computer in one department can easily be used as a Trojan to launch attacks on computers in other departments or the Internet.
- Because of these risks, CNS security personnel must take action when they become aware of a security incident specifically

involving an AUBnet computer. In cases where the incident poses a potentially serious threat to AUBnet information system resources or the Internet, the computer will be immediately blocked from network access.

When a compromised computer is identified, whether or not it is blocked from network access, CNS security personnel must be able to quickly contact someone in the appropriate department who can take action and/or pass the information on to the appropriate departmental support personnel. Quickly reaching a departmental contact is also important so that any affected user(s) may be informed of the situation. In addition, CNS security personnel will inform this contact person of possible irregularities such as computers with configuration problems that could negatively impact the network or that appear to be infected with a virus.

**Policy:** Each department needs to appoint a security contact and one or more backup contacts. Groups of departments may agree to share contacts for efficiency.

**Guidelines:** All security contacts for a given department should be reachable through email address, work phone number and mobile phone or pager. CNS and departmental security contacts will all use authenticated email exchange (ASMTP).

CNS security personnel should clearly identify in the security incident report the “Severity” of the security incident and accordingly the “Actions” and the “Expected Completion Date-time”. The departmental security contacts must promptly respond to security incident reports and pass them on to the responsible departmental or third party support personnel as appropriate.

Departmental security contacts need to have some familiarity with the computers in their department and be able to determine and locate a responsible technical person; it is not necessary for the contact to have extensive security expertise.

Departmental security contacts are responsible for ensuring that appropriate personnel take action in response to each security incident (including escalating the incident to an appropriate departmental authority if action is not taken) and that resolution of each incident or any variance or update is reported to CNS security officer [security@aub.edu.lb](mailto:security@aub.edu.lb).

**Additional Information:** “Security Incident Report”