

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	September 2002
Section 5.8	Information Security	Revised:	September 2004
Policy 5.8.15	Technical Support Representative (TSR) Policy	Responsibility:	Vice President and Chief Information Officer

TECHNICAL SUPPORT REPRESENTATIVE (TSR) POLICY

Overview

The TSR Program was designed to enable at least one computing technology single point of contact person in each department with the responsibility for first line problem diagnosis and to facilitate resolution of technical questions at the departmental level. The Program has evolved to become essential in the realm of information security for the Health Science Center, and: the distribution of critical information, security-related patches/updates, virus/worm vulnerability announcements, and the required reporting of security 'incidents'. In addition, a key access control responsibility for TSRs has evolved to include a password reset capability. This capability is also an essential part of the 'security architecture' for the Health Science Center and must be well controlled.

Policy

1. Every department is required to have at least one TSR. Where departments are small, or lack the necessary staff, the department may enter into a "shared relationship" with another department, and utilize the same TSR for both departments. The department heads must agree on the relationship and the individual selected to be the TSR. Larger departments may have two or more full-time or part-time TSRs, TSRs/Advanced, or TSRs/System Administrators depending on the department's environment.
2. A Dean, Chair, or Director must appoint all TSRs in writing to the Director of Information Management Client Support Services (IMCSS). The TSR cannot also be an Account Control Executive (ACE), unless compensating controls are documented in departmental procedures and are reviewed by Internal Audit.
3. A TSR, once appointed, is required to attend basic TSR training provided by IMCSS. A recommended training list for the TSR/Advanced and TSR/System Administrator will be published and provided to the Dean, Chair, or Director.

At least one TSR from each department is required to attend regularly scheduled general or special TSR meetings, which will provide new technology information, as well as policy and

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	September 2002
Section 5.8	Information Security	Revised:	September 2004
Policy 5.8.15	Technical Support Representative (TSR) Policy	Responsibility:	Vice President and Chief Information Officer

procedures updates. These meetings are the forum in which TSRs will be able to interact (share expertise and experiences) with other TSRs and the IMCSS staff.

4. As the first line of technical service for their department the designated TSR(s) are the communications link for computing technology information related to: end-user computing problems, desktop configuration upgrades, software updates, critical security update information, and other relevant technology information. This responsibility includes the distribution and/or implementation of applicable information from the TSR meetings. Additionally, the designated TSRs are the principal means by which individual users report security incidents to IMCSS, see [Section 5.8.6](#) of the *Handbook of Operating Procedures* (HOP), "Computer Incident Response Policy".
5. One or more TSRs, TSR/Advanced, or TSR/System Administrators may be designated by the Dean, Chair, or Director as the department's authority to request password resets to central computing systems on behalf of members of the department. The designated TSR(s) must follow the [Section 5.8.4](#), "Access Control and Password Management", in the HOP, and security bulletins. This responsibility is critical and has a direct impact on the security architecture of the University. For these reasons, a TSR designated with this responsibility must be a mature, responsible employee who can be relied upon to handle and maintain confidential information. To that end, a security designated TSR should meet the following guidelines:
 - Be an employee of, or assigned to the Health Science Center for at least two years and have been functioning in that department's computing environment for at least one year, or
 - Have had previous responsibility for computing support in another Health Science Center department.

Exceptions to the above requirements may be made with the approval of the Information Security Function.