Technical Support Representative Designation

(UTHSCSA Handbook of Operating Procedures Policy 5.8.15)

Department Name:			**Select TSR Type (Check One)**			**Authorized to Reset Passwords?**
Employee			**TSR**	**Advanced TSR**	**System Administrator**	**Yes / No**
Last Name	**First Name**	**MI**				

Instructions: Designate employee then indicate TSR Type and indicate Yes or No to Authorized to reset passwords. Add new designees starting in the first blank position. Line through the name of anyone to be removed from the Program. Sign, Date, and forward to IMS Client Support Services, attention Helpdesk Services.

The reverse side of this page contains an explanation of the TSR Program and Definitions that may be useful.

Designating Authority (Dean, Chair, or Director):

_____

(Printed Name)

_____

(Signature)

_____

(Date)

TSR Program Description and Definitions

(Extracted from HOP Section 5.8.15)

Program Overview:

The TSR Program is a time-tested, functional Program providing an open information technology forum and a distribution channel of computing technology information, including critical security-related information across the Health Science Center campuses.

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 UTHSCSA: 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.

The TSR Program makes use of informational meetings, training programs, and cooperative, mutual assistance among TSR members.

At least one designated TSR is required in each department in order to assure that a responsible person in that department has the knowledge and training to receive and distribute time-critical computing and security-related information and to report general computing and security incidents to Information Management and Services (IMS).

The Dean, Director, or Chair is responsible for appointing the TSR(s) in their departmental entity.

Definitions:

TSR (Basic): Technical Support Representative (TSR). The departmental representative assigned the responsibility of receiving computer technology- and security-related information from IMS and distributing that information as appropriate within their department. All TSRs should have a working knowledge of basic computer concepts.

Advanced TSR: Technical Support Representative (TSR)/Advanced is a TSR who has received significant training, more technical proficiency in the department's environment, and information technology support duties as a primary job responsibility. Advanced TSRs may, at the discretion of the Dean, Director, or Chair, be designated to receive additional security and related information from IMS and distribute that information as appropriate within their department.

System Administrator: A TSR/System Administrator may be a more technically proficient member in the department's environment and has been designated as having information technology support and/or server system administrator duties as part of their job responsibility. TSR/System Administrators may, at the discretion of the Dean, Director, or Chair, be designated to receive security and related information from IMS and distribute that information as appropriate within their department. Refer to Handbook of Operating Procedures Policy (Section 5.8.14) for Administration of Security on Decentralized Server Computers for additional information.

Password Reset: One or more TSRs, TSR/Advanced, or TSR/System Administrators may be designated by the Dean, Director, or Chair 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 Access Control and Password Management Policy, in the HOP, Section 5.8.4, and IMS 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 UTHSCSA 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 HSC department.

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