Reason for the Guidelines

1. Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

2. Official Guideline
   1.1 HSC departments must submit to the Office of Information Technology (OIT) a list of administrative contacts for their systems that are connected to the HSC network.

   1.2 All users must sign the HSC Acceptable Use Agreement before access is given to an account.

   1.3 All users of administrative/special access accounts must have account management instructions, documentation, training, and authorization.

   1.4 Each individual that uses administrative/special access accounts must refrain from abuse of privilege and must only initiate investigations under the direction of the ISO.

   1.5 Each individual that uses administrative/special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).

   1.6 Each account used for administrative/special access must meet the HSC Password SAP.

   1.7 The password for a shared administrator/special access account must change when an individual with the password leaves the department or HSC, or upon a change in the vendor personnel assigned to the HSC contract.

   1.8 In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
1.9 When special access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:

- must be authorized,
- must be created with a specific expiration date, and must be removed when work is complete.

2. VIOLATIONS

Violations of this policy may result in disciplinary action which may include termination for employees and temporary workers; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY:

Vice President for Finance and Administration