OAKLAND UNIVERSITY

ADMINISTRATIVE POLICIES AND PROCEDURES

880 SYSTEM ADMINISTRATION RESPONSIBILITIES

SUBJECT: SYSTEM ADMINISTRATION RESPONSIBILITIES

NUMBER: 880

AUTHORIZING BODY: STRATEGY COUNCIL

RESPONSIBLE OFFICE: UNIVERSITY TECHNOLOGY SERVICES

DATE ISSUED: MAY 2003

LAST UPDATE: MARCH 2013

RATIONALE:

The policy is intended to protect the wide array of information technology resources that are supported by departmental System Administrators and faculty, as well as by University Technology Services (UTS) staff.

POLICY:

System Administration must be accomplished in a professional and timely way with a goal of protection of University assets and the broad array of information technology resources in use at the University. System Administrators have responsibilities to the University and should use reasonable efforts:

- To comply with all technology policies, the technical direction and standards established by University Technology Services, Technical Currency best practices, and other guidelines or standards defined by the unit.
- To disseminate information about specific policies and procedures governing access to, and use of, systems and technical services.
- To know the information technology resources and assets in the assigned realm of responsibility and to appropriately inventory and track those assets.

- To take precautions against theft of or damage to the system components and data, and to report such events to appropriate areas when such events occur.

- To treat information about, and information stored by, the system's users in an appropriate manner respecting privacy and confidentiality. The System Administrator's ability to access must not be confused with authority to access data.

- To know the data elements stored in a system, to understand the data classifications as defined in Policy #860 Information Security, and to take precautions to protect the security of a system or network and the privacy, confidentiality and quality of information contained therein.

- To cooperate with the System Administrators of other information technology resources, whether within or outside the University, to find and correct problems caused on another system by or through the use of the system under his/her control.

SCOPE AND APPLICABILITY:

This policy is applicable to all University students, faculty and staff and to others responsible for the maintenance, support and operation of University information technology resources as defined in OU AP&P #890 Acceptable Use. This policy refers to all University information technology resources whether individually controlled or shared, stand-alone or networked. It applies to all information technology resources, including systems and servers, owned, leased, operated, or controlled by the University.

Locally Defined and External Conditions of Use: Individual units within the University may define "conditions of use" for information technology resources under their control as long as those conditions do not conflict with appropriate University use guidelines found in the OU AP&P #890 Acceptable Use or this policy. Individual units are responsible for publicizing both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible.

DEFINITIONS:

- **Access Accounts**: Access Accounts are part of an access identity management scheme and typically provide an individual system user with an identity commonly called a username and a password to login and gain access to a system, network or application. An Access Account will be assigned specific privileges appropriate to the individual's job responsibilities and the purpose of the access.

- **Identity Management Systems**: Identity Management Systems are systems designed for the purpose of managing login credentials, such as login identities, passwords, and personal identification numbers.

- **Responsible Administrator**: While the University is the legal "owner" or "operator" of all information technology resources purchased or leased with University funds, oversight of any particular system may be delegated to the head of a specific subdivision of the University governance structure, such as Vice President, Dean, Department Chair, or Administrative Department head where the system information technology resource is not under the control of University Technology Services. For University-owned or leased equipment, that person is the Responsible Administrator referred to in this policy.

- **System Administrator**: The Responsible Administrator is the System Administrator by default, but the Responsible Administrator may designate another person to manage the system. This designate is the System Administrator, who is responsible for the maintenance, support and operation of a system or systems. System Administrators have additional responsibilities to the University as a whole for the system(s) under their oversight, regardless of the policies of their department or group. The Responsible Administrator has the ultimate responsibility for the actions of the System Administrator. System Administrators are accountable to their constituencies.

- **System Administration**: System Administration refers to specific responsibilities and assigned tasks of the System Administrator. Such tasks include, but are not limited to: installing, supporting, and maintaining operating systems, database management systems, application software, and hardware; planning for, trouble-shooting, resolving, responding to system problems or outages; and providing knowledgeable facts about the use of the system in the organization.

- **Technical Currency**: The status, age, and state of non-obsolescence of hardware and software. The University strives to maintain adequate and up to date hardware by adhering to reasonable replacement cycles, and maintains secure and functional software by monitoring and installing required releases, security updates and patches.

PROCEDURES:

a. Access Account integrity

Whenever possible, Access Accounts are integrated with UTS managed Identity Management Systems such as the NetID system (LDAP) or Active Directory (ADMNET). Centralized authentication adheres to University policy allowing the Systems Administrator to focus on systems and applications management, user

rights assignment, and user roles within the system. Security is enhanced by reducing the proliferation of login identities and passwords.

In the event that System Administrators manage Access Accounts, Access Account activities must be performed on a timely basis, including providing new accounts and removing old accounts promptly. All Access Accounts are authenticated using individually assigned unique usernames and passwords. Accounts will be assigned and enabled with least needed privileges.

All Access Accounts are disabled immediately upon employment termination unless approved in advance by University policy or University Technology Services. All Access Accounts are reviewed periodically for the existence of malicious, out-of-date, or unknown accounts. Access Accounts will be disabled and deleted based on the access rules for the environment and in compliance with all licenses. System Administrators will ensure that Access Accounts can be traced to an individual person, that the Access Accounts system access that matches the authorization of the user, that initial or vendor-supplied default accounts or passwords are disabled, and that Access Account implementation matches this policy.

System Administrators will verify that access to Confidential Data (defined in Policy #860 Information Security) is logged by Access Account and system time, including root and administrative access.

System Administrators will assure that strong passwords are used and those passwords are changed frequently, within the limits of the system environment. System Administrators must verify that all passwords on all systems and network devices are encrypted in transit and at rest with strong encryption. Stored Access Account authentication data (e.g., password files, encryption keys, certificates, personal identification numbers, access codes) must be appropriately protected with access controls, strong encryption, shadowing, etc. – e.g., password files must not be world-readable.

b. Licenses, copyrights and contracts

System Administrators must respect and enforce copyrights, software licenses and contracts. All software protected by copyright must not be copied or accessed except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any University facility or system, except pursuant to a valid license or as otherwise permitted by copyright law. The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract. System Administrators are responsible for enforcing systems compliance with related contract, software, and purchasing policies.

c. Data protection

System Administrators will implement adequate protections of Confidential Data (defined in Policy #860 Information Security), including identification of appropriate storage locations, encryption processes, and removal of confidential data that are not maintained under retention guidelines.

d. Data and system backup services

System Administrators must perform regular and complete backup services for the systems they administer, or they must work with UTS administrators to add their systems to a larger University backup structure. System Administrators will describe the data restore services, if any, offered to the system users. A written document given to system users or messages posted on the computer system itself shall be considered an adequate backup description.

UTS maintains system schematics describing systems in its administration and maintains daily backups of those systems, approved by the Chief Information Officer, for disaster recovery purposes only. UTS backups are created on a rotation schedule and stored in locations approved by the Chief Information Officer. The Chief Information Officer authorizes special UTS backups.

e. Enforcement

UTS will audit the security of systems that have a presence on the University network. UTS may scan or examine systems for compliance and may either disconnect or quarantine any non-compliant system from the University network until the system is brought into compliance. In accordance with this policy, violators may be denied access to University computing resources and may be subject to other penalties and disciplinary action including University disciplinary procedures appropriate to their University status per Policy #890 Acceptable Use.

f. Investigation of possible misuses and system logs

A System Administrator must report any possible misuse of data and security breaches immediately upon discovery to University Technology Services and the Oakland University Police Department. The System Administrator may be the first witness to possible misuse. Systems Administrators will immediately investigate any possible breach reported to them by University Technology Services.

System Administrators are assigned to periodically and regularly monitor system logs for possible abuse and misuse. System Administrators must report any log anomaly, abuse indication or misuse indication to UTS within two regular workdays or 48 hours, of discovery. When a security breach or unauthorized data exposure

occurs, UTS may disable access to the system while a forensic copy of the system is made or while working with law enforcement on criminal investigations.

System Administrators should maintain appropriate system logs for a minimum of 48 hours and not more than 30 days if such logs enable the identification of a person, unless there are specific legal or regulatory requirements requiring longer retention as reviewed with UTS and the Office of Legal Affairs. Logs that do not identify a user or person may be kept as needed by a System Administrator.

Subpoenas and all other information requests for electronic data or system records must be immediately referred to the Office of Legal Affairs. A System Administrator may be charged with providing information about what electronically stored information is available (including system schematics, backups and logs), preserving electronically stored information and producing that information for the Office of Legal Affairs. Litigation notices override standard policies and practices for backup cycles and retention.

g. Modification or removal of equipment

Information technology resources that are retired, disposed, or transferred to another location must have all data and licenses removed, erased and made unreadable prior to release of the equipment. Software and information technology resources licensed to the University may not be transferred to a third party. Removal must meet standards for security established by University Technology Services. Equipment must be disposed using methods approved by Property Management. System Administrators must not attempt to modify or remove computer equipment, software, or peripherals that are controlled or administered by others without proper authorization.

h. Network consistency

System Administrators will implement systems in compliance with the overall University structure for Internet Protocol (IP) addressing, domain services, wireless connectivity strategies, firewall rules, and directory services, as established by University Technology Services.

i. Special areas of compliance

The University must comply with certain special regulations. In particular, Payment Card Industry (PCI) and Health Insurance Portability and Accountability Act (HIPAA and the related HiTech Act) have specific requirements. Other legal and regulatory areas may emerge from time to time requiring specific systems administration protocols. Systems that process, store or transmit credit card or other payment methods must meet Payment Card Industry compliance standards. Systems that process, store or transmit electronic protected health information (EPHI) must meet

HIPAA and related HITECH compliance standards. UTS must be informed of all systems that process, store or transmit PCI or HIPAA data.

Systems Administrators responsible for PCI or HIPAA compliant systems must attend annual training on compliance.

All systems and applications used to process, transmit or store Cardholder Information or EPHI must have access controlled and permitted by uniquely assigned login identities and passwords. Whenever possible, administrative access will be LDAP-enabled. Access Accounts are only given access to the minimum resources needed to perform a function. Administrator accounts are required to change passwords every 90 days. Password policy must enforce use of strong passwords at least 8 characters in length. Passwords must contain both numeric and alphabetic values. A new password for an individual account cannot be the same as the prior four (4) passwords.

Accounts are locked when multiple attempts to access fail. Repeated unsuccessful login attempts must lock an account after six (6) attempts. Lockout durations must be set to 30 minutes; administrative override after verification is permissible.

Systems must have the latest security patches installed on a timely basis unless overruled by the System Administrator and then only with compensating controls in place. Server hardening implementations must be based on industry-recognized best practices. Systems are physically secure and access is restricted to authorized administrators. Software that maintains the integrity of files is used to detect improper alteration of either system files or log data. Access control logs contain successful and unsuccessful login attempts and access to logs. Centralized logs recording data access, successful login attempts, and unsuccessful login attempts are retained for three months online and one year offline.

j. Remote access

Remote access used for System Administration must be handled through secured, encrypted communications verified in advance by University Technology Services.

k. Removal from the network

For the purpose of assuring all University system users a sound environment, and to meet the University expectations for network services, a system found to be in non-compliance with University policies may be removed from the University network. When immediate disconnection is not necessary, System Administrators will still be expected to take prompt action, to diagnose the problem, to stop any ongoing abuse, and to make whatever changes are needed to prevent reoccurrence. This will involve adopting best practices for security. This process should preserve any evidence that might be needed to locate the source of the problem and take any legal or disciplinary action that might be appropriate. System Administrators may be

asked to demonstrate compliance to this document and to University policies before network services are restored after a documented instance of non-compliance.

l. System integrity

System Administrators are responsible for installing and maintaining all aspects of system integrity, including obtaining releases and fixes to assure the currency of operating system upgrades, installing patches, managing releases, installing anti-virus software, updating virus definitions, changing all vendor default passwords, synchronizing system clocks, and closing services and ports that are not needed for the effective operation of the system. Prompt renewal of vendor hardware and software agreements is required. Absence of a vendor support contract does not mean that University Technology Services is able to repair and restore systems without prior agreement or notice. System Administrators must make every effort to remain familiar with the changing security technology that relates to their system and continually analyze technical vulnerabilities and their resulting security implications.

m. Third party access

Third parties with access to University information technology resources must be contractually obligated to comply with University security policies and practices.

n. Vendor accounts and passwords

System Administrators must verify that vendor default passwords are disabled or changed immediately upon installation and for the duration of the implementation. All vendor passwords must be encrypted. Accounts needed by vendors are enabled only for the time needed, and disabled upon completion of work.

RELATED POLICIES AND FORMS:

- OU AP&P #212 Payment Card Information Security Requirements
- OU AP&P #360 Property Management
- OU AP&P # 830 Information Technology
- OU AP&P # 850 Network Policy
- OU AP&P # 860 Information Security
- OU AP&P # 870 Software Regulations
- OU AP&P # 890 Acceptable Use

APPENDIX: