University of Portland

ADMINISTRATOR ACCEPTABLE USE POLICY

1. **PURPOSE**: The purpose of this policy is to provide guidance regarding the ethical and acceptable use of University of Portland (UP) information services (IS) resources by network/system/database administrators, also known as "Administrators." The directive also details that auditing and monitoring will be employed to ensure that Administrators do not misuse their authority. This directive establishes a policy for reporting information technology security incidents involving Administrators that may compromise the availability, integrity, and confidentiality of the University's infrastructure and information systems.

2. **SCOPE:** This directive applies to all individuals working within Information Services. Departments not reporting to the Chief Information Officer (CIO) are strongly encouraged to follow the policy and procedures stated in this directive.

3. **DEFINITIONS:** These are collectively referred to as central administrators.

   a. **Database Administrator:** A person responsible for the design and management of one or more databases and for the evaluation, selection and implementation of database management systems.

   b. **Network Administrator:** A person who manages a communications network within an organization. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program and providing for routine backups.

   c. **System Administrator:** A person who manages the computer systems in an organization. The responsibilities of a system administrator and network administrator often overlap. A system administrator is involved with operating system and hardware installations and configurations and may be involved with application installations and upgrades. A system administrator may also perform systems programmer activities.

   d. **Application Administrator:** A person who manages enterprise applications in an organization. The responsibilities of an application administrator and system administrator often overlap. An application administrator is involved with application configurations and may be involved with application installations and upgrades. An application administrator may also perform systems programmer activities.

4. **POLICY:** Administrators are required to manage, configure and monitor UP IS resources. Administrators also have the ability to create, access, modify and/or delete electronic resources, data and systems configurations within a given technology discipline as well as granting permissions to other individuals commensurate with their own privileges in a given technology discipline. Because administrators are trusted with rights and privileges beyond those granted to normal UP system users (users) they must adhere to the highest standards of ethical conduct in the use of and administration of UP IS resources.

   In addition, Administrators will be subject to stringent auditing and monitoring of their activities to maintain the highest level of internal security. The auditing and monitoring may be performed by external vendors. Adherence to best practices and guiding principles will be enforced by internal security team. The separation of duties shall be utilized as a measure of avoidance for a potential conflict of interest. This process shall provide validation and confidence of the health and security of the University's infrastructure and information systems within the perimeter of the University. If an incident is detected the incident must be reported to the CIO.

5. **GUIDELINES:** Acceptable uses of University of Portland Information Services resources by administrators include but are not limited to:

   a. Adherence to the standards set forth in the Information Security Policy and Other Authorized User Internet Use and Electronic Mail Communications.

   b. Performance of activities deemed necessary to support the overall health, availability, integrity and security of:

   - Servers, desktops, and laptops owned or controlled by UP.
   - Network and infrastructure systems owned or controlled by UP.
   - Physical and electronic security systems owned or controlled by UP.

   c. Database and application systems owned or controlled by UP.

   d. Guarding against corruption, compromise, or destruction of UP computer and network resources and information assets.

   e. Maintaining and applying all system patches and system updates considering the expense of applying the patch, the expense of recovering from a failed patch and the likelihood that not applying a given patch will result in a security breach.

   f. Taking reasonable and appropriate steps to ensure that all hardware and software license agreements are faithfully executed on all systems, networks, and servers.

   g. Ensuring agency network addresses are assigned only to those entities departments or schools that are part of the University. Administrators shall not assign network addresses to non-university entities or organizations without the specific written approval of the Chief Information Officer (CIO).

   h. Limiting access to root, administrative, service or privileged supervisory accounts (privileged accounts) on UP computer and network resources to administrators only. Privileged accounts are accounts that have virtually unlimited access to all programs, files, and resources on a computer system. Users shall not be given access to privileged accounts without the specific approval of the university CIO. Privileged accounts must be used only for the purposes for which they were authorized and only for conducting UP business.

   i. Ensuring that default passwords shipped with servers, operating systems, databases, network equipment, or software applications are changed using strong password methodologies when the resource is installed or implemented.

   j. Never sharing personal or privileged account logins or passwords with anyone including other administrators without the approval of the university CIO.

   k. Never allowing users to log into computer resources with anonymous privileged accounts.

   l. Performing all regular UP activity under a personal account and not through an anonymous privileged account.

   m. Never knowingly creating pathways that allow for violations of network security.

   n. Never gaining unauthorized access to a system (or area of a system) using knowledge of access abilities gained during a previous position at another department or school.

   o. Never giving access on a system you do not administer to another user.

p. Always logging off or appropriately securing sessions with privileged account access to a point that requires a new log-on whenever leaving your work area.

q. Treating the files of system users as private unless there is reason for suspicion such as hacking, sending illegal material, etc. Administrators routinely monitor and log general usage data. When problems become apparent, they may review this data for evidence of violation of law or policy as directed by the Vice President for University Operations, Vice President of Human Resources or Vice President and General Counsel. When necessary, they may monitor all the activities and inspect the files of specific users on their computers and networks. If there is reason for suspicion departmental head, and the CIO must be contacted before any action is initiated.

r. Respecting the privacy of electronic communication. Administrators shall not obtain/intercept or attempt to obtain/intercept any electronic communication or information not intended for them unless such activities are performed as part of their authorized job duties. Administrators have the duty to the owners of the information to protect the confidentiality of all such information. This includes making changes to, ensuring unauthorized users do not have access to, or not divulging to a third party that information.

s. Ensuring that all network activities tracked are complete for all users. Administrators may not single out individual users for tracking or logging, unless directed to do so by the Human Resource office and/or University legal counsel. All users must be tracked or logged equally. To ensure the integrity of procedures and policies of network administration or to ensure network security, additional or extra activities of the administrators may be tracked.

t. Never engaging in any illegal or inappropriate use of UP IS resources or engaging in activities that interfere with or disrupt network users, services, or equipment. Illegal use shall be defined as use which violates local, state, or federal law as well as UP or IS policy. Inappropriate use shall be defined as a violation of the goals, purpose and intended use of the network. This includes, but is not limited to, the following: stalking others, supporting partisan political activities, transmitting or originating any unlawful, fraudulent, defamatory, or obscene communications, or any communications where the message or its transmission or distribution, would constitute or would encourage conduct that is a criminal offense or would give rise to civil liability. Interference or disruption includes, but is not limited to, distribution of unsolicited advertising or mass mailings; "spamming," propagation of computer worms or viruses.

6. EXCEPTIONS: There are no exceptions to this policy.

7. SANCTIONS: Accounts and network access may be administratively suspended by the University with or without notice when, in the University's judgment, continued use of the University's resources may interfere with the work of others, place the University or others at risk, or violate University policy. Any violation of this policy by a student may lead to disciplinary charges under the appropriate student disciplinary policy, which may include expulsion or suspension of student status. Faculty and staff violations will be addressed by their respective disciplinary policies and procedures. All known and/or suspected violations will be reported to the Vice President for University Operations. Users of University of Portland computing facilities are subject not only to University Policies, but also to applicable local, state and federal laws.