IT Privileged Access Agreement

INTRODUCTION

Privileged access enables an individual to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, staff performing computing account administration or other such employees whose job duties require special privileges over a computing system or network.

Individuals with privileged access must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant laws or regulations. Individuals also have an obligation to keep themselves informed regarding any procedures, business practices, and operational guidelines pertaining to the activities of their local department.

In particular, the principles of academic freedom, freedom of speech, and privacy of information hold important implications for computer system administration at UACCM. Individuals with privileged access must comply with applicable policies, laws, regulations, precedents, and procedures while pursuing appropriate actions required to provide high-quality, timely, reliable, computing services.

GENERAL PROVISIONS

- Privileged access is granted only to authorized individuals. Privileged access shall be granted to individuals only after they have read and signed this Agreement.
- Privileged access may be used only to perform assigned job duties.
- If methods other than using privileged access will accomplish an action, those other methods must be used unless the burden of time or other resources required clearly justifies using privileged access.
- Privileged access may be used to perform standard system-related duties only on machines and networks whose responsibility is part of assigned job duties. Examples include:
    - resetting passwords;
    - installing system software;
    - relocating individuals' files from critically overloaded locations;
    - performing repairs required to return a system to normal function, such as fixing files or file processes, or killing runaway processes;
    - running security checking programs;
    - monitoring the system to ensure reliability and security.
- Privileged access may be used to grant, change, or deny resources, access, or privilege to another individual only for authorized account management activities or under exceptional circumstances. Such actions must follow any existing organizational guidelines and procedures. Examples include:
    - disabling an account apparently responsible for serious misuse such as: attempting to compromise root (UNIX) or the administrator account (Windows), using a host to send harassing or threatening email, using software to mount attacks on other hosts, or engaging in activities designed to disrupt the functioning of the host itself;
    - disconnecting a host or subnet from the network when a security compromise is suspected;

- accessing files for law enforcement authorities with a valid subpoena.

In all cases, access to other individuals' electronic information shall be limited to the least perusal of contents and the least action necessary to resolve a situation.

Individuals with privileged access shall take necessary precautions to protect the confidentiality of information encountered in the performance of their duties.

If, during the performance of their duties, individuals with privileged access inadvertently see information indicating serious misuse, they are advised to consult with their supervisor. If the situation is an emergency, intervening action may be appropriate.

AGREEMENT

I have read this *Privileged Access Agreement*, the UACCM *Acceptable Use Policy*, and the UACCM *Information Systems Access Policy*.

I agree to comply with the provisions of this *Privileged Access Agreement*, the UACCM *Acceptable Use Policy*, and the UACCM *Information Systems Access Policy*.

Applicant Signature _____

Supervisor Signature _____

Systems or Resource Access Requested:

Please be specific when listing access to resources. If there is an existing account that has the desired level of access, please list that account as the source for the new account.