



Privileged Access Agreement

Version: 7.1

Revision: June 18, 2007

Abstract

This agreement is required of individuals seeking privileged access to restricted systems or resource on the University of Cincinnati systems.



INTRODUCTION

Privileged access enables an individual to take actions which 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 system or computer 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 all relevant laws, policies and 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 UC. 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. You, as a privileged user, must comply with provisions of the University of Cincinnati (UC) policies concerning:

- [General Policy on the Use of Information Technology](#)
- [Information Technology Management](#)
- [Information Security](#)

KEY POINTS FROM THE POLICIES ABOVE

*Reading this section is **not** a replacement for reading the full details of the policies linked above*

1. Privileged access is granted only to authorized individuals. Privileged access shall be granted to individuals only after they have read and signed this Agreement.
2. Privileged access may be used **only** to perform assigned job duties.
3. 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.
4. Privileged access may be used to perform standard system-related duties only on machines and networks whose responsibility is part of assigned job duties.
5. 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 all applicable existing organizational guidelines and procedures.

In the absence of compelling circumstances, the investigation of information in, or suspension of, an account suspected to be compromised should be delayed until normal business hours to allow appropriate authorization and/or notification activities.
6. 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.
7. 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 or contact the UC Information Security department at 558-ISec or send an email to abuse@uc.edu. If the case appears to involve any



illegal activity, they must contact the UC Police Department at 556-1111 immediately. If the situation is an emergency, intervening action may be appropriate.

University policy governs all activities involving university electronic communication resources. University policy provisions must be followed when electronic communication records are involved in any situation.

Authorization

Under most circumstances, the consent of the owner of an electronic communications record must be obtained before accessing their files or interfering with their processes. If consent cannot be obtained, then provisions in university or governmental policy granting access without consent must be met.

Notification

In either case, the employee or other authority shall, at the earliest opportunity consistent with law and university policy, attempt to notify the affected individual(s) of the action(s) taken and the reasons for those action(s).

RECOURSE

If conflicts or disputes arise regarding activities related to this Agreement, individuals may pursue their rights to resolve the situation through existing procedures. Such procedures would include informal supervisory or departmental conflict resolution procedures, relevant provisions of employment policies or contracts, student or faculty conduct procedures, or other such provisions which pertain to the particular individual's affiliation with the university.

AGREEMENT

1. I have read this **Privileged Access Agreement** and all referenced policies.
2. I agree to comply with the provisions of this **Privileged Access Agreement** and all referenced policies.
3. I understand that, after agreeing to comply with the provisions of this Privileged Access Agreement and all referenced policies, failure to follow the provisions may result in administrative penalties up to and including termination of employment.

Print Name _____

Signature _____

Date _____

Authorized by:

Print Name _____

Dept _____

Signature _____

Date _____