

Policy on Privileged Access

- Reference:** CNS-P-GEN-PRIV-ACCESS **Revision:** D
- Supersedes:** System Administrator Best Practice Guideline
- Purpose:** The purpose of this policy is to prevent inappropriate use of privileged access by the Computing and Networking staff members, Application Super Users, Departmental System Administrators and any individual provide with privilege access to AUB information systems in the event of performing their normal duties.
- Source:** Computing and Networking Services (CNS).
- Approved by:** Nabil Bukhalid, Director of CNS **on:** May 12, 2005
George Tomey, VP for Administration **on:** Pending
- Applicability:** This policy is an additional policy designed to enforce, and not replace, the “*AUBnet Code of Conduct*” and other relevant policies.
- This policy and guidelines apply to CNS staff, consultants and contractors employed by CNS and to students employed by CNS for more than 20 hours per week referred to hereafter as “**CNS staff members**”.
- Contractors and consultants operating under the strict supervision of an AUB authorized personnel are exempt from completing the Privileged Access Agreement form but nonetheless are to comply with this policy and all University policies.
- University students employed solely on an hourly pay basis up to a maximum of 20 hours per week are exempt from completing the Privileged Access Agreement form but nonetheless are to comply with this policy and all University policies.
- This policy should in principal apply to all individuals, institution wide, with privileged access to computing systems, network communication, or the accounts, files, data, or processes of other users.
- Background:** 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 computing account administration, or other such employees whose job duties require special privileges over a computing system or network. Privileged access might provide such users with technical access capabilities that are beyond their functional access authority such as upgrade their functional access authority.

Individuals with privileged access must not abuse their access capability and strictly respect their functional access authority limits, 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 familiarize themselves regarding any procedures, business practices, and operational guidelines pertaining to the activities of their local department.

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

Policy: **Privileged access to AUB information systems is granted only to officially authorized individuals based on clearly defined and documented instructions.**

Computer systems that create or update mission critical university data need to be treated in specific to minimize the exposure to security, privacy and loss of mission critical data risks. The unit responsible for providing and operating such systems must conduct a systematic and detailed investigation of all the influencing factors leading to the compilation of a comprehensive **System Specific Privilege Access Policy**. System specific privilege access policies must at least fulfill the requirements of the **Privilege Access Policy**.

Privileged access shall be granted to individuals only after they have read this policy and signed a ***Privileged Access Agreement Form***.

Whenever technically possible, gaining and using privilege access should be audited.

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 only to perform assigned job duties.

Privileged access may be used to perform standard system-related duties. Examples may include:

- installing system software;
- relocating other individuals' files from a failing disk or server to a new location;
- performing repairs required to return a system to normal function, such as fixing files or file processes, or killing runaway processes;
- running security checks.

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 may include:

- disabling an account apparently responsible for serious activities such as: making attacks on root or administrator account, or using a host to send spam email, or using software to mount attacks on other hosts or engaging in activities designed to disrupt the functioning of the host itself or to load AUBnet network;
- disconnecting a host or subnet from the network when a security compromise is suspected;
- accessing files for law enforcement authorities with a valid written order.

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.

In all cases, access to other individuals' electronic information shall be limited to 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 are inadvertently exposed to information that might indicate inappropriate use, they are advised to consult with their supervisor. If the situation is an emergency, intervening actions may be appropriate.

Guidelines: **It is the sole responsibility of a CNS staff member and any AUB staff, faculty or student to identify, at his/her own discretion, the situations where he or she, is currently, or may be in violation of**

the above policies and to immediately make a full disclosure in writing and submit it to the director of CNS or his direct supervisor or director.

AUTHORIZATION: Under most circumstances, the consent of the account or data owners should be obtained, if possible, before accessing their files or interfering with their processes and/or data elements. However, if good faith efforts to obtain consent are not successful, or would unduly interfere with the performance of the assigned duties, the situation should be documented with reference to an organizational guideline or procedure justifying such actions without consent.

SUPERVISED ACCESS: Under most circumstances, the privileged access to personal or departmental systems should be performed in the presence of the system owners or his representative. However, if good faith efforts to secure the supervised access are not successful, or would unduly interfere with the performance of the assigned duties, the situation should be documented with reference to an organizational guideline or procedure justifying such actions without supervised access.

NOTIFICATION: In either case, the employee or other authority shall, at the earliest possible opportunity, attempt to notify the affected individual of the action(s) taken and the reasons for the action(s) taken.

AUB CHIEF ITC SECURITY OFFICER: The director of CNS assumes the AUB Chief ITC Security Officer responsibility and delegates the specific ITC Security Officer roles as appropriate. AUB Chief ITC Security Officer shall review the requirements and/or situation and approve the granting of the privileged access rights. The AUB Chief ITC Security Officer might seek the advice and/or the approval of the President, Provost, Vice Presidents, Deans, Director of Business Units, Internal Auditor and/or the legal council as appropriate. Decisions shall be reported in writing with justification delineating any conditions placed on the approval, rejection, etc.

ITC SECURITY OFFICERS: The AUB Chief ITC Security Officer delegates specific responsibilities to qualified ITC Security Officers as appropriate. AUB ITC Security Officers shall review the requirements and/or situation and approve the granting of the privileged access rights under their specific authority. The ITC Security Officers might seek the advice and/or the approval of the AUB Chief ITC Security Officer and Official ITC system owners as appropriate. Decisions shall be reported in writing with justification delineating any conditions placed on the approval, rejection, etc.

ACKNOWLEDGE RECEIPT OF THE POLICY: It is the responsibility of the ITC Security Officer to explain this policy before granting privilege access to the AUB ITC system under his authority in a comprehensive manner and to make sure that they acknowledge receipt of the policy statement in writing.

ACKNOWLEDGE RECEIPT OF THE AGREEMENT: It is the responsibility of the ITC Security Officer to explain the recommendations and decisions to the privilege access user in a comprehensive manner and to make sure that he/she acknowledge receipt of the decisions.

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

Consequence of

Non-Compliance: Non-compliance with this policy could expose the individual to University disciplinary actions and/or legal actions.

Additional

Information: - AUBnet Code of Conduct