Computer and Network Accounts Administration

IT-18

About This Policy

Effective Dates:
09-14-2000

Last Updated:
09-14-2000

Responsible University Administrator:
Office of the Vice President for Information Technology & Chief Information Officer

Policy Contact:
University Information Policy Office, uipo@iu.edu

Scope

This policy applies to all users of Indiana University information technology resources regardless of affiliation, and irrespective of whether those resources are accessed from on-campus or off-campus locations.

Policy Statement

Identity and eligibility to use Indiana University technology resources will be authenticated for all users. Level of identification and authentication will be commensurate with the capabilities and sensitivity of the specific resources they are using.

Each eligible individual obtaining an account will have a University-wide unique username assigned, built from a standard format agreed to by all naming parties. All necessary steps will be taken to coordinate the assignment of usernames among ALL technical operations within the University where naming takes place.

All usernames will be three to eight characters in length. The required naming pattern/sequence is as follows:

1. The first initial of the first name followed by up to seven characters of the last name (e.g., csmith).
2. The first initial of the first name followed by the middle initial followed by up to six characters of the last name (e.g., casmith).
3. The first initial of the first name followed by up to six characters of the last name, followed by a numeric tiebreaker (e.g., csmith6).

Usernames will not be changed unless the individual's name changes in the official University databases and the individual personally requests such a change, or in cases where there might be personal danger to the individual if they have a commonly derived username. Changes will also be allowed where the combinations of characters result in an objectionable name or term. Vanity username changes will not be permitted.

To ensure optimal use of resources and to address security concerns, accounts databases will be kept clean. That is, published eligibility criteria will be consistently applied, testing procedures will be applied at required intervals, and appropriate account removal and archiving tasks will be performed as required.

All accounts will be directly assigned to single individuals based on eligibility rules, and those individuals will be the sole contact and have sole responsibility for all actions taken with and in that account.

Account holders who leave their accounts active and unattended will be charged with a violation of University policy. They may also be charged with more serious violations if others use their unattended account for more serious infractions.

Passwords are assigned to individuals, and never will Accounts or System Administrators, supervisors, or any other agent of Indiana University ask for or require a user to give them their password for any reason. Only the account owner will know the password for computer accounts assigned to them. Circumstances under which Accounts or System Administrators or other any other person can learn or obtain the user's assigned password must be minimal in the extreme, and where possible initially assigned passwords must expire causing the user to choose a new one that only they know.

All account holders will read and agree to a set of responsibilities BEFORE they gain control of their account.

Individuals may have multiple accounts assigned to them. Requests for such accounts must be reviewed and the reason for them must be consistent with activities related to Indiana University functions. The individual to which the accounts are assigned will be responsible for all actions taken with and in these accounts.

"Group" accounts (that is, those assigned to and used by members of an organization) will be created only in support of activities directly associated with Indiana University functions. A current full-time faculty or appointed staff member must identify himself or herself as the person responsible for management of and use of the account. When requesting or renewing the account, this "sponsor" will provide information stating their relationship to the group, outlining the group's membership and affiliation/benefit to Indiana University, and an indication that they understand their responsibilities related to the use of the group account. To be eligible for a group account, the membership of the group must be comprised of 50% or more members otherwise eligible for Indiana University personal computer accounts.

Accounts may be assigned to individuals not affiliated with Indiana University only in support of activities directly associated with Indiana University functions. A current full-time faculty or appointed staff member must identify himself or herself as the sponsor or contact related to the individual's activities while they are at the University. When requesting or renewing the account, this "sponsor" will provide information stating their relationship to the individual, outlining the individual's affiliation/benefit to Indiana University, and an indication that they understand their responsibilities related to the use of the individual account.

Account Administrators will make the initial determination regarding eligibility of an individual to receive an IU account. Cases where eligibility is unclear will be passed to the campus Chief Information Officer or to the University Information Technology Policy Officer for review and approval.

Accounts Administrators will retain all documentation related to computer accounts while the account is active, and for 1 year following the point at which the individual is no longer associated with Indiana University, or from the point where the organization having a group account has been dissolved.

The standard Indiana University identification number maintained in the official University employee or faculty or student information databases ("Student ID", "Employee ID", or "Faculty ID") will be used to track account assignments. ID numbers assigned to accounts will be that of the account holder or account sponsor.

Extracts of student, staff, or faculty information in support of computer account administration activities or user directories will be taken from the official University sources.

Extracts of faculty/staff or student information in support of accounts administration activities or user directories will be used ONLY for this purpose. Secondary release of this information is not permitted without review and approval by the University IT Policy Officer and the Data Steward associated with the data involved.

Reason For Policy

In order to ensure that University information systems and processes have a consistent view and that the outside world has a consistent view of the Indiana University population, accounts administration and management processes and procedures must be consistent.

Procedure

In partnership with campus Chief Information Officers and other naming functions and stakeholders, the University Information Technology Policy Office will coordinate accounts administration procedures, and will develop and publish central account procedures and processes to be used on all campuses.

Individual campuses Chief Information Officers will be responsible for local adherence to this policy, and for additional local processes, procedures, and additions to this and other accounts policies on their campuses as required.

Definitions

Indiana University Information Technology Resources includes all University-owned computers, peripherals, and related equipment and software; voice communications infrastructure, peripherals, and related equipment and software; data communications infrastructure, peripherals, and related equipment and software, and all other associated tools, instruments, and facilities. Included in this definition are classroom technologies, computing and electronic communication devices and services, modems, electronic mail, phone access, voice mail, Fax transmissions, video, multimedia and hyper media information, instructional materials, and related supporting devices or technologies. The components may be individually controlled (e.g., assigned to an employee) or shared single-user or multi-user, and they may be stand-alone or networked.

History

- Posted as draft: September 14, 2000