The College's Policy on Access & Authorization

Executive Summary

The Columbia College Computing Community's policies on access and authorization extend from the recognition that information security is of paramount importance to achievement of The College's mission and operations.

To protect our organization -- its resources, our colleagues, and our constituencies -- we must exercise due care in bestowing privileges to persons, processes, and devices and performing privileged actions.

This document sets guidelines for authorizing the granting, revocation, and use of privileges.

Definitions

A **subject** is an active entity, generally in the form of a person, process, or device, that causes information to flow among objects or that changes the state of a system.

People are most often familiar with system **users** as subjects. Users are a person or process that can access and use a computer system. Users are uniquely identified by a user id (i.e. account name).

An **object** is a passive entity that contains or receives information. Access to an object potentially implies access to the information that it contains. Examples of objects include data records, files, directories, network shares, servers, and user accounts.

Access refers to a subject's ability to view, modify, or communicate with a target object. Access enables the flow of information between the subject and the object.

Accountability is a security principle indicating that individuals must be able to be identified and to be held responsible for their actions. Accountability enables explanation of how a system moved from one state to another.

Identification is the process that enables one subject to recognize another subject or object. Identification is the first step in an authentication process. For example, an account's username identifies a subject to a system.

Authentication is the verification of a subject requesting the use of a system and/or access to a network resource. For example, the correct submission of an account's password for its corresponding username authenticates a user.

Authorization is the granting of access to a subject to an object after the object has been properly identified and authenticated. The granting of access is performed by an authorization mechanism acting in accordance with rules set forth by the object's owner or information owner.

The steps to giving a subject access should be identifying, authenticating, and authorizing.

An **information owner** is a person or group of persons who has final responsibility for protection of a defined information asset and would be the one held liable for any negligence when it comes to protecting this information asset.

The person who holds this role is responsible for (i.e. has authority for) determining what levels of security should be applied to an information asset, what subjects may access the information asset, what privileges subjects may hold on an information asset, and how it is to be protected.

Privileges are how subjects can interact with the information asset.

Often information owners define **role-based access** for their information assets. Role-based access provides access and privileges to resources based on the role a subject has or the tasks that the subject has been assigned.

Least privilege (sometimes referred to as Just Enough Privilege) is the security principle that requires each subject to be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or un-authorized use and is considered a best practice.

Support

Columbia College Information Technology (CCIT) is available to assist, advise, and consult in the structuring of access and privileges for computing resources.

CCIT and its team members are charged with ensuring the availability and security of The College's computing resources and The College Computing Community supported by these resources. Thus, CCIT is responsible for ensuring compliance with this policy.

Determination of Least Privileges Necessary to Accomplish a Function

CCIT will work with information owners to establish the minimum set of privileges necessary for accomplishment of a given function or set of duties.

Given its role and responsibility for managing and ensuring the availability & security of the College Computing Community as a whole, CCIT is the information owner of CCIT deployed computing systems (servers, workstations, application software, etc.)

Thus, CCIT will have final determination of what privileges may be provided given the understood needs and practices of an information owner and the needs and practices of the larger computing environment.

User Accounts within the College Domain

To ensure accountability, except under exceptional circumstances, CCIT will solely issue uniquely identifiable accounts to members of the Columbia College Computing Community.

In keeping with the least privilege policy of The College, user accounts are provided the minimum set of privileges necessary for accomplishment of their job roles within the organization.

Service Accounts

Service accounts are issued for applications, daemons, and services to accomplish their purpose under the auspices of an established account's credentials.

In keeping with the least privilege policy of The College, service accounts will be provided the minimum set of privileges necessary for the accomplishment of a desired function.

The authentication credentials of service accounts will be closely guarded and periodically changed by CCIT.

Shared Accounts

Shared accounts are well known to be subject to misuse and thwart access, authorization, integrity, and confidentiality controls for information assets and business processes. CCIT will not issue shared accounts to users.

Shared accounts are permitted when used as service accounts permitting use of a shared computing resource that does not process, transmit, permit access to, or store information assets of the organization that would otherwise be subject to access, authorization, integrity, and confidentiality controls requiring accountability.

Thus, shared accounts may be used for such purposes as public kiosks, but not for such purposes as convenience in reducing account management overhead (i.e. facilitating intern access to a workstation through one shared account is not permitted).

In keeping with the least privilege policy of The College, such accounts will be provided the minimum set of privileges necessary for the accomplishment of a desired function.

The authentication credentials of service accounts will be closely guarded and periodically changed by CCIT.

Information Owners

Information owners and their delegates are to be identified and mapped to business processes, information assets, and other objects for which CCIT is responsible for 1) the granting & revocation of access & privileges or 2) the execution of requests on behalf of the information owners.

Information owners are subject to The College's least privilege policy and may not authorize privileges in excess of that which is determined necessary by CCIT and themselves for the successful accomplishment of a function.

One's Identity & Information Assets

On occasion, an individual seeks others to be able to do things on behalf of themself (e.g. have another person send an email that appears to be from him or herself).

One's information assets include one's emails, one's account/profile space, and other such assets to which one has the expectation of a reasonable degree of privacy and person control.

Individuals is the information owner for their identity and their information assets. Only they or someone to which they directly report in the organization may authorize the delegation of the use of their identity or their information assets to another person.

Delegates

An information owner may delegate their authority to authorize the granting, revocation, or use of privileges to others by submitting a written request to CCIT identifying the following:

- The individual to whom they are delegating authority,
- The degree of authority being delegated, and
- The period of time for which the delegation is valid (e.g. until explicitly revoked).

Authorization of Requests Granting or Revoking Privileges or Directing a Privileged Action

Only information owners or their authorized delegates may submit requests to CCIT for the authorization of 1) requests granting or revoking privileges and 2) requests directing a privileged action to be performed on a business process or information asset for which they are responsible.

All such requests must be made in writing by the information owner or their delegate and be authenticated by CCIT.

It is not permissible for an information owner to simply be copied on a request.

Absence or Unavailability of Information Owners

Should an information owner or their delegate be absent or unavailable to authorize a request, a member of senior management to which the information owner (and not their delegate) directly reports may authorize a request.

As with all authorization requests, the request must be made in writing to CCIT.

CCIT will notify the information owner of the authorization decision made in their absence.

Use of Privileges

Privileges granted to a subject may only be used for the purpose for which they were authorized and will be revoked when no longer necessary.

Escalated Privileges

On rare occasion, escalated privileges may temporarily be required to effect a given action.

Escalated privileges must be authorized by an information owner and justified prior to their temporary provision to a subject by CCIT.

At the discretion of CCIT, one or the other of the following options may be employed:

1. CCIT will perform the requested action on behalf of the subject with authorization of the information owner, or

2. CCIT will extend such privileges on a temporary basis and within a monitored context.

Protocol for Access & Authorization to Objects Managed By CCIT

1. A written request will be sent to CCIT by the information owner of a business process or information asset for which they are responsible identifying:

    a. the subject
    b. the objects of the action
    c. what action is authorized
    d. the purpose for which the action is authorized

2. If the request is not made by appropriate information owners, CCIT will:

    a. decline the request & request the written approval of all necessary information owners, or
    b. forward the request to identified information owners

3. The request will be authenticated as coming from the information owner.

4. CCIT will authenticate whether the information owner is the established information owner for all the business process(es) or information asset(s) affected by the action requested.

    If other business processes or information assets are affected, CCIT will:

    a. decline the request & request the written approval of all necessary information owners, or
    b. forward the request to identified information owners for their authorization.

5. If there is 1) any confusion as to what action is to be taken or 2) a structural or policy reason why an action cannot be executed as requested, CCIT will obtain necessary clarifications and work with information owners to achieve the desired effect of the requested action.

6. When all necessary approvals have been received in writing from all affected information owners, CCIT will execute the requested action.

7. All communications (including the initiating request) and all actions taken will be logged in a Bugzilla ticket.