Secure Access and Information Sharing Landing Page

Secure Access and Information Sharing Landing Page

For more information on securing your data, see Information Protection @ MIT.

On this page:

- Overview
- How to
  - Grant Access to users and groups based on roles and privileges
  - Limit access to authorized individuals and for authorized purposes
  - Revoke access when a user no longer needs access to information at this level (i.e. upon project completion or job change).
  - Review which user accounts have access to information, applications, or servers at this level (at least) annually.
- See Also
- Have Questions or Still Need Help?

Overview

Information owners should work with system administrators to ensure information is accessible only for authorized purposes and shared only with those authorized to receive it. This includes revoking permissions when a user no longer needs access to information (e.g., upon project completion or job change), and performing regular reviews of which user accounts have access to data, applications, or servers with Medium or High Risk level information - at least annually.

Not all users require access to nor have a need to know for medium or high risk information. Regularly auditing accounts/credentials for who has access to what, when, and for what purpose are critical for reducing the exposure, unauthorized use or loss.

To achieve this, an Information Owner will need to know the level of the information they have, where it is stored, and what types of access control the platform or application provides.

How to

Grant Access to users and groups based on roles and privileges

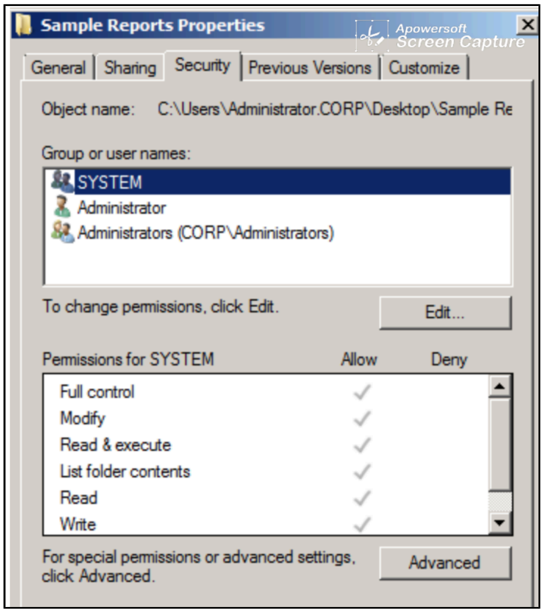
Authorized users should initially be granted access information based on their roles, responsibilities. This is often accomplished by placing users into predefined groups with privileges appropriate to the group. For instance, personnel in Accounts Payable, or Finance would need access to financial records which may be kept in some electronic system or application. Then, depending on their specific role, they may have a variety of privileges or ability to view and act on the financial information they have access to. For instance:

- Basic User Role: Read only access - can only generate reports
- Analyst Role: Can enter and read financial data and generate reports
- Senior Analyst Role: Can enter and modify financial data up to $10k and generate reports
- Supervisory Role: Can enter and modify financial data over $10k and generate reports, has access to logs
- Administrator Role: Access level four - Full access to all data within the system or application
- System Administrator Role: Full access to the underlying system (Operating System upgrades, patching, hardware migration)
- Database Administrator Role: Full access to the database structure (SQL server, Oracle)

Limit access to authorized individuals and for authorized purposes

Closely manage electronic information permissions to ensure all individuals with access have only the minimum privileges required to complete their tasks.

- Permissions include typically allowing or denying access for Everyone while allowing a subset of your organization and/or data owner Full Control, Modify, Read & Execute, List folder contents, Read, Write. These can be configured on individual files, file-shares, cloud-based applications such as Dropbox, and other programs with options similar to the following:



Object name: C:\Users\Administrator.CORP\Desktop\Sample Re

Group or user names:

- SYSTEM
- Administrator
- Administrators (CORP\Administrators)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

- Dropbox team folder settings - Membership (including adding/removing members) can only be modified by Admins and Group managers. Ensure the lists of Admins/Group managers reflect current roles and membership is limited to those with a need to know.
- It is a common practice to implement role-based access controls to manage authorized access. This is done by assigning/dividing users into role groups then assigning the appropriate permissions based on each role.
- Another consideration is the duration of access required. For instance, if a third party requires access to information or systems for the duration of a contract or engagement that has an end date, accounts should be configured to automatically expire on that date. Requests for extensions should be formalized.

Revoke access when a user no longer needs access to information at this level (i.e. upon project completion or job change).

Keeping access control lists up-to-date across all areas of an organization can be a challenge. Users often have multiple groups into which they fall and have access to various information systems. Additionally, there's not always a centralized way to track internal access or as a users leaves current roles/positions.

Here at MIT, there are various procedures that happen when students, faculty, or staff leave the institute. If access to information is tied to a Kerberos account some access may be revoked automatically. Otherwise, review the methods to create and revoke accounts in your applicable platform.

It may also help to establish an out-processing checklist to track project completions, departures, and changes to ensure access is updated/revoked as appropriate and documented as a part of a formal procedure.

Out-processing Task	Information Owner	Signature/Date
Visit x office to have account deleted		

Review which user accounts have access to information, applications, or servers at this level (at least) annually.

Once you have an inventory of your information and have documented who should have access to it (Information Inventory Landing Page here), review to ensure that no accounts have been left active unintentionally.

Conduct regularly scheduled audits to identify privileged user accounts and accounts with access to sensitive information.

For example:

- Check user account information in moira
- If account has been deleted, they should not still have access to any information

See Also

- United States Computer Emergency Readiness Team (US-CERT) Article about Limiting Access
- BeyondTrust Article on Least Privilege
- Center for Internet Security on Controlled Use of Administrative Privileges
- Leaving MIT KB
- Varonis on Permissions (Screenshot source)

Have Questions or Still Need Help?

- MIT KB Regarding History of Authorizations Granted and Revoked for a User
- Microsoft Least Privilege Models
- Role based access control (RBAC)
- Contact the IS&T Security Team