

Data Access Governance

Short Data Access Governance Best Practice Guide


Access governance is best defined as "governing who has access to what within an organization."

Best Practices for Data Access Management

- Create a complete inventory of your users and resources and keep it up to date.
- Work with department managers and other business owners to determine where your sensitive data is and who owns it.
- Determine who has access to what and who owns what data in your organization. For example, you can export access lists of your file servers using PowerShell scripts or third-party software.
- Establish a security structure by creating security groups and making users members of the appropriate groups.
- Assign each group appropriate access to shared data.
- Empower data owners to control access rights to the data they own.
- Audit the actions of data owners to be sure that all operations are authorized.
- Establish an access request workflow (such as a request portal) so users can easily request access to data they need to do their jobs.
- Audit and report on access to sensitive data as well as changes to it.
- Make all sensitive shares hidden by adding a dollar sign (\$) to the end of each share name.
- Run an access certification program to align access with business needs.

Best Practices for File Server Permissions

- Have users log on using domain user accounts rather than local accounts. This approach centralizes the administration of share permissions.
- Create a file server permission policy that clearly defines your permission management process.
- Remove the Everyone permission from every resource except the global folder designated for file exchanges.
- Assign permissions to groups, not user accounts. This approach enables you to add users to or remove them from groups without having to reassign permissions, simplifying management and improving accuracy.
- Give each group a succinct yet descriptive name to avoid errors.
- Define sets of permissions that reflect the access needs of a particular department or a specific role in the organization.
- Assign the most restrictive permissions that still allow users to perform their jobs. For example, if users need only to read information in a folder and not to change, delete or create files, assign the Read permission only.
- Organize your resources so that objects with the same security requirements are located in the same folder. For example, if users require the Read permission for several application folders, store those folders in the same parent folder. Then give Read permissions to the parent folder, rather than sharing each individual application folder separately.
- Avoid denying permissions to a shared resource explicitly. It is usually necessary to explicitly deny permissions only when you want to override specific permissions that are already assigned; this can indicate that either permissions were assigned directly rather than via group membership, or that a user is a member of the wrong group.
- Assign the Full Control permission only to the Administrators group and strictly limit membership in this group. This permission enables a user to manage application software and control user rights.
- Create a "global deny" group so that when employees leave the company, you can quickly remove all their file server access by making them members of the group.
- Audit every change to permissions on your file servers and always check whether those changes were authorized.

 Gain **#completevisibility** into who has access to what across your file servers with Netwrix Auditor for Windows File Servers: netwrix.com/go/trial-fs