Technical Writing Permissions Cheatsheet

A quick reference guide to understanding and managing permissions within technical writing workflows, focusing on templates and documentation control.

Fundamentals of Permissions

Permission Types

Read	Allows users to view the document or template but not modify it.
Write/Edit	Allows users to modify the document or template. Includes adding, deleting, and changing content.
Comment	Allows users to add comments and annotations without directly altering the original content.
Admin/Owner	Full control over the document or template, including permissions management, deletion, and major modifications.
Execute	Specifically for Templates, allows to instantiate a new document from template.

Levels of Access

User-Specific	Permissions granted to individual users. Highly granular but can be difficult to manage at scale.
Group-Based	Permissions assigned to groups of users. Simplifies management for teams with common roles.
Role-Based	Permissions tied to predefined roles within the organization. Ensures consistent access based on job function.
Public Access	Accessible to anyone, typically for published documentation or templates meant for wide distribution. Requires careful consideration of content.

Importance of Permission Control

- **Data Security:** Prevents unauthorized access to sensitive information.
- **Version Control:** Maintains document integrity by limiting modification rights.
- **Compliance:** Ensures adherence to regulatory requirements regarding data access.
- **Workflow Efficiency:** Streamlines processes by defining clear roles and responsibilities.
- **Intellectual Property Protection:** Safeguards proprietary information within templates and documentation.

Template Permissions

Template Access Control

Restricted Access	Only authorized personnel can modify the base template. Prevents accidental or malicious alterations that could impact all future documents created from it.
Copy Permissions	Control who can create new documents from the template. This is separate from editing the template itself.
Version Control Integration	Link template permissions to version control systems to track changes and revert to previous versions if needed.

Scenarios

- *Technical Writer*: Read/Write access to templates they manage; Read access to reference templates.
- *Subject Matter Expert*: Comment access for providing feedback on template content.
- *New User*: Read access to approved templates; no modification rights.
- *Manager*: Full control over templates owned by their team.

Best Practices

- Regularly review and update template permissions.
- Use group-based or role-based permissions to simplify management.
- Document the rationale behind specific permission settings.
- Implement a change control process for template modifications.
- Audit template usage and access to identify potential security risks.

Documentation Permissions

Controlling Document Access

Draft Stage	Restrict access to only the writing team and subject matter experts during the initial development phase.
Review Stage	Grant comment access to stakeholders for feedback and approval.
Published Stage	Provide read-only access to the intended audience, while maintaining write access for updates and revisions.
Archived Stage	Limit access to administrators or compliance officers for record-keeping purposes.

External Sharing

Watermarking	Add watermarks to documents shared externally to discourage unauthorized copying or distribution.
Password Protection	Require passwords to access sensitive documents shared with external parties.
Limited-Time Access	Grant temporary access to documents with automatic expiration to prevent long-term unauthorized access.
Disable Download/Printing	Restrict the ability to download or print documents to prevent offline distribution.

Permissions Tools

- **Document Management Systems (DMS):** Centralized platforms for managing and controlling access to documents.
- **Collaboration Platforms:** Tools like Google Docs, Microsoft SharePoint, and Confluence offer built-in permission features.
- **Identity and Access Management (IAM) Systems:** Solutions for managing user identities and controlling access to resources across the organization.

Troubleshooting Permissions

Common Issues

- **Overly Permissive Access:** Granting more access than necessary, increasing the risk of data breaches.
- **Orphaned Permissions:** Permissions assigned to users who no longer require them.
- **Conflicting Permissions:** Conflicting rules that result in unexpected access behavior.
- **Lack of Documentation:** Absence of clear documentation on permission settings and rationale.

Resolution Steps

- **Regular Audits:** Conduct periodic reviews of permissions to identify and resolve issues.
- **Principle of Least Privilege:** Grant only the minimum level of access required to perform a task.
- **Centralized Management:** Use a DMS or IAM system to streamline permission management.
- **User Training:** Educate users on the importance of permissions and responsible data handling.

Auditing Permissions

Logs analysis	Checking logs for suspicious activity.
Access review	Periodically review user access rights and permissions.
Automated tools	Use automated tools for access review.