**Title Page**

DATA SECURITY – RESTRICTED SHARED FOLDERS.  
How to Protect Shared Folders with Proper Metadata, Disclaimer, and Validation.

**Introduction**

Data security ensures that sensitive information is protected from unauthorized access.

One of the most crucial aspects of data security is controlling access to shared folders.

This eBook explains how to restrict shared folders and includes proper formatting, metadata, disclaimer, and validation guidelines.  
  
  
 **Key Points / Instructions**1. DATA SECURITY: THE SHARED FOLDERS SHOULD BE SET TO RESTRICTED.

2. Need to add Metadata-Keywords (already done).

3. Need to make it in proper format like adding DISCLAIMER, DISCLOSURE, etc.

4. Need 100% clarity. More validation on preview tools.

5. Need to improve the GITHUB ACTIONS pipeline (like there should be less blank space) — less important.  
  
 **How to Restrict Shared Folders**1. Open the folder in your drive (Google Drive, OneDrive, or GitHub).

2. Click on Share.

3. Change General Access to Restricted.

4. Add only authorized users with required permissions (Viewer, Editor).   
  
 **Disclaimer**This eBook is intended for educational and informational purposes only.

The author and publisher are not responsible for any errors or omissions,

or for any outcomes related to the use of this content.

All trademarks and registered trademarks are the property of their respective owners.

The reader assumes all responsibility for the use of this information.

The author shall not be held liable for any damages or losses.

This eBook is sold "as is" and all sales are final - no refunds or returns will be issued.

**Disclosure**

All information provided in this document is for learning and educational purposes only.

Users must implement security practices responsibly based on their organization’s policies.