Kiteworks

How to Share Files Securely: A Best Practices Checklist

Secure file sharing safeguards sensitive information from unauthorized access and potential cyber threats. By following secure file sharing methods and best practices, you can mitigate data leaks, financial losses, and regulatory compliance violations and instead ensure the confidentiality, integrity, and availability of your data. These best practices highlight some of the strategies and practices for securely sharing files.

☑ Use a Secure File Sharing Solution

Key features to look for include end-to-end encryption, secure file transfer protocols, access controls, and audit logs. A secure file sharing solution should also be easy to use and integrate seamlessly with your existing workflows.

☑ Ensure Every File is Encrypted

Encryption protects your data from unauthorized access even if the file is intercepted during transfer. Symmetric encryption uses a single key for both encryption and decryption, while asymmetric encryption uses a pair of public and private encryption keys for these processes.

☑ Use Secure File Transfer Protocols

Protocols like secure file transfer protocol (SFTP), hypertext transfer protocol secure (HTTPS), and transport layer security (TLS) ensure that data is encrypted and protected from eavesdropping and tampering during transfer. These protocols also provide authentication mechanisms to verify the identity of the sender and receiver.

☑ Adopt a Secure File Sharing Mindset

Ensure that all employees and trusted third-parties prioritize data protection and consistently follow secure file sharing practices. Reinforce with policies, security awareness training programs, and continuous improvement.

☑ Use Strong Passwords and Multi-Factor Authentication

Passwords should be at least 12 characters long and include a mix of uppercase and lowercase letters, numbers, and special characters. Bolster with multi-factor authentication (MFA) to help protect accounts even if the password is compromised.

☑ **Regularly Update and Patch Software**
Regularly install updates and patches for file sharing applications and other software to ensure that security vulnerabilities are addressed promptly. Automating this process helps streamline this process and ensures that all software is consistently updated.

☑ **Implement Access Controls**
Implement role-based access controls (RBAC) to assign permissions based on the user›s role within the organization. Also, regularly review and update access controls, ensuring that permissions remain appropriate over time.

☑ **Securely Manage Endpoints**
Implement endpoint security measures like antivirus software, firewalls, and intrusion detection systems to protect devices from malware and other threats. Ensure all endpoints are encrypted and require strong authentication methods. Finally, enable remote wipe capabilities to protect data if a device is lost or stolen.

☑ **Educate and Train Employees**
Conduct periodic training sessions on secure file sharing methods. Provide employees with guidelines on how to share files securely, including the use of secure file sharing solutions, strong passwords, and multi-factor authentication.

☑ **Monitor and Audit File Sharing Activities**
Implement logging and monitoring tools to track file sharing activities, including who accessed files, what actions were taken, and when they occurred. Regularly review audit logs to identify any unusual or unauthorized activities.