**TUGAS KULIAH**



**NAMA : ARBAI**

**NIM : 223220066**

**UNIVERSITAS AKI**

**FAKULTAS TEKNIK DAN INFORMATIKA**

**2023**

1. Membuat kebijakan penggunaan file: Tetapkan kebijakan yang jelas mengenai penggunaan file dalam sistem. Termasuk di dalamnya aturan tentang lokasi penyimpanan, jenis file yang diizinkan, ukuran maksimum file, dan hak akses pengguna terhadap file tersebut.
2. Mengatur struktur penyimpanan: Rancang struktur direktori dan penyimpanan file yang terorganisir agar memudahkan pencarian, pemeliharaan, dan manajemen file. Pertimbangkan untuk menggunakan hierarki direktori yang logis dan deskriptif.
3. Mengimplementasikan kontrol akses: Terapkan kontrol akses berbasis peran atau pengguna pada file agar hanya pengguna yang berwenang yang dapat mengakses, memodifikasi, atau menghapus file. Hal ini membantu mencegah akses tidak sah atau modifikasi yang tidak diinginkan.
4. Memantau penggunaan file: Lakukan pemantauan terhadap penggunaan file untuk mendeteksi aktivitas yang mencurigakan, seperti akses tidak sah, percobaan pembobolan, atau penggunaan yang berlebihan. Gunakan alat pemantauan dan log aktivitas untuk melacak dan menganalisis perilaku pengguna terkait file.
5. Melakukan backup dan pemulihan data: Lakukan secara berkala proses backup file untuk menghindari kehilangan data yang disebabkan oleh kesalahan manusia, kegagalan perangkat keras, atau serangan malware. Pastikan untuk menguji dan memverifikasi keberhasilan pemulihan data dari backup secara berkala.
6. Memperbarui keamanan: Pastikan sistem yang digunakan dalam pemrosesan file diperbarui secara teratur dengan pembaruan keamanan terbaru. Ini termasuk menjaga perangkat lunak antivirus dan firewall terkini, serta menerapkan patch keamanan untuk sistem operasi dan perangkat lunak terkait.
7. Menghapus file yang tidak diperlukan: Tetapkan kebijakan penghapusan file yang tidak diperlukan secara berkala untuk menghindari akumulasi data yang tidak relevan atau sensitif. Pastikan untuk menghapus file dengan cara yang aman, termasuk penghapusan permanen dari media penyimpanan.
8. Menerapkan kebijakan retensi data: Jika ada persyaratan hukum atau kebijakan internal terkait retensi data, pastikan untuk mengimplementasikan kebijakan retensi yang sesuai. Hal ini melibatkan menyimpan file dalam jangka waktu yang ditentukan sebelum menghapusnya sesuai dengan kebijakan yang berlaku.
9. Memeriksa integritas file: Secara berkala, lakukan pemeriksaan integritas file untuk memastikan tidak ada kerusakan atau perubahan yang tidak sah pada file. Hal ini dapat dilakukan dengan menggunakan metode checksum atau hash yang membandingkan nilai checksum atau hash saat ini dengan nilai checksum atau hash yang disimpan sebelumnya.
10. Memonitor dan mengoptimalkan penggunaan ruang penyimpanan: