**Mempersiapkan Data untuk Eksplorasi**

**Pedoman organisasi/pengaturan**

Bacaan ini merangkum praktik terbaik untuk penamaan, organisasi, dan penyimpanan file.

**Praktik terbaik untuk konvensi penamaan file**

Tinjau rekomendasi penamaan file berikut:

* Tentukan dan setujui konvensi penamaan file di awal proyek untuk menghindari penggantian nama file berulang kali.
* Selaraskan penamaan file Anda dengan konvensi penamaan file yang ada di tim atau perusahaan Anda.
* Pastikan nama file Anda bermakna; pertimbangkan untuk menyertakan informasi seperti nama proyek dan hal lain yang akan membantu Anda mengidentifikasi (dan menggunakan) file dengan cepat untuk tujuan yang tepat.
* Sertakan tanggal dan nomor versi dalam nama file; format umum adalah YYYYMMDD untuk tanggal dan v## untuk versi (atau revisi).
* Buat sebuah file teks sebagai file sampel dengan konten yang menjelaskan (menguraikan) konvensi penamaan file dan nama file yang menerapkannya.
* Hindari spasi dan karakter khusus dalam nama file. Sebagai gantinya, gunakan tanda strip, tanda hubung bawah, atau huruf besar. Spasi dan karakter khusus dapat menyebabkan kesalahan pada beberapa aplikasi.

**Praktik terbaik untuk menjaga agar file tetap teratur**

Ingat tips berikut untuk tetap teratur saat Anda bekerja dengan file:

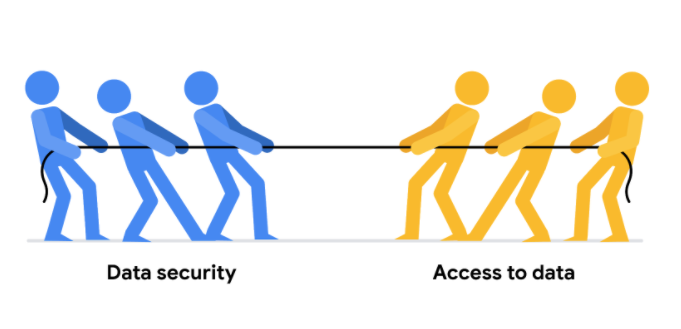
* Buat folder dan subfolder dalam hierarki logis sehingga file terkait tersimpan di tempat yang sama.
* Pisahkan pekerjaan yang sedang berlangsung dari pekerjaan yang sudah selesai sehingga file proyek Anda saat ini lebih mudah ditemukan. Arsipkan file lama di folder terpisah, atau di lokasi penyimpanan eksternal.
* Jika file Anda tidak dicadangkan secara otomatis, sering-seringlah mencadangkan secara manual untuk menghindari kehilangan pekerjaan penting.

**Menyeimbangkan keamanan dan analitik**

**Pertempuran antara keamanan dan analitik data**

Keamanan data berarti melindungi data dari akses tidak sah atau kerusakan dengan menerapkan langkah-langkah keamanan. Biasanya tujuan dari keamanan data adalah untuk mencegah pengguna yang tidak berwenang untuk mengakses atau melihat data sensitif. Para analis data harus menemukan cara untuk menyeimbangkan keamanan data dengan kebutuhan analisis mereka. Ini bisa menjadi langkah yang rumit. Kita ingin menjaga data kita tetap aman dan terlindungi, tetapi juga ingin menggunakannya sesegera mungkin sehingga kita dapat melakukan pengamatan yang bermakna dengan tepat waktu.

Untuk melakukan ini, perusahaan perlu menemukan cara untuk menyeimbangkan langkah-langkah keamanan data dengan kebutuhan akses data.



Untungnya, ada beberapa langkah keamanan yang dapat membantu perusahaan untuk melakukan hal tersebut. Dua yang akan kita bicarakan di sini adalah enkripsi dan tokenisasi.

**Enkripsi** menggunakan algoritma unik untuk mengubah data dan membuatnya tidak dapat digunakan oleh pengguna dan aplikasi yang tidak mengetahui algoritma tersebut. Algoritma ini disimpan sebagai "kunci" yang dapat digunakan untuk membalikkan enkripsi; jadi jika Anda memiliki kuncinya, Anda masih dapat menggunakan data tersebut dalam bentuk aslinya.

**Tokenisasi** menggantikan elemen data yang ingin Anda lindungi dengan data yang dihasilkan secara acak yang disebut sebagai "token". Data aslinya disimpan di lokasi terpisah dan dipetakan ke token tersebut. Untuk mengakses data asli yang lengkap, pengguna atau aplikasi harus memiliki izin untuk menggunakan data yang telah tertokenisasi dan pemetaan token tersebut. Ini berarti bahwa meskipun data yang telah tertokenisasi tersebut diretas, data aslinya tetap aman dan terlindungi di lokasi yang terpisah.

Enkripsi dan tokenisasi hanyalah beberapa opsi keamanan data yang ada. Ada banyak lainnya, seperti menggunakan perangkat otentikasi untuk teknologi AI.