Google for Education

Google Workspace for Education

Checklist Pengelolaan Data Sensitif dan Pencegahan Kebocoran Data

Google Workspace for Education edisi berbayar (Education Standard, Teaching and Learning Upgrade, dan Education Plus) membantu Anda menciptakan lingkungan pembelajaran inovatif dengan alat tingkat perusahaan yang disesuaikan untuk pendidikan. Berikut ini panduan tentang tindakan yang dapat Anda lakukan untuk membantu mengelola data sensitif dan mencegah kebocoran data.

> Baru pertama kali menggunakan Google Workspace for Education?
>
> Hubungi pakar dan pelajari lebih lanjut di sini.

Sebaiknya Administrator Google Workspace melakukan beberapa langkah dasar untuk membantu mengelola data sensitif, termasuk:

- Mengaktifkan Pencegahan Kebocoran Data (DLP) untuk Gmail dan Drive. Dengan DLP, Anda dapat mengontrol konten yang dapat dibagikan pengguna dan mencegah eksposur informasi sensitif yang tidak diinginkan, seperti nomor kartu kredit atau nomor identitas.
- Meninjau praktik terbaik berikut untuk meningkatkan keamanan akun administrator Anda, dan mengikuti checklist keamanan ini saat menerapkan setelan di seluruh aplikasi Workspace. Anda juga dapat menggunakan Kondisi Keamanan untuk memantau konfigurasi setelan keamanan dan mendapatkan rekomendasi berdasarkan praktik terbaik.
- Menetapkan hak istimewa admin untuk melindungi privasi pengguna
- Menjaga keamanan data setelah pengguna keluar dari institusi Anda
- Menyiapkan aturan agar mendapatkan notifikasi saat ada aktivitas tertentu dalam domain Anda

Google for Education