Duy trì bảo mật dữ liệu sau khi nhân viên nghỉ việc

Quản lý người dùng · https://gcs.vn/kho-tai-nguyen/google-workspace-admin-center/duy-tri-bao-mat-du-lieu-sau-khi-nhan-vien-nghi-viec/

Với tư cách là quản trị viên của tổ chức bạn, hãy giữ cho dữ liệu của tổ chức bạn an toàn và bảo mật khi người dùng rời đi bằng cách hoàn thành các phương pháp hay nhất sau:

1. **Xóa mọi thiết bị di động**
   Sử dụng Bảng điều khiển dành cho quản trị viên để xóa dữ liệu từ xa khỏi thiết bị của người dùng. Bạn có thể xóa từ xa toàn bộ thiết bị hoặc chỉ xóa dữ liệu của tổ chức.
2. **Thu hồi quyền truy cập khôi phục mật khẩu**
   Xóa địa chỉ email và số điện thoại khôi phục của người dùng để họ không thể sử dụng tính năng khôi phục mật khẩu để truy cập vào tài khoản cũ của họ.
3. **Thay đổi mật khẩu của người dùng**
   Điều này có thể làm giảm đáng kể nguy cơ truy cập trái phép vào tài khoản cũ của họ.
4. **Thu hồi tất cả mã thông báo ứng dụng OAuth 2.0**
   Việc thay đổi mật khẩu của người dùng cũng thu hồi mã thông báo OAuth 2.0 được cấp để truy cập một số sản phẩm. Xem lại tất cả quyền truy cập được phép và thu hồi bất kỳ ứng dụng được phép nào khác.
5. **Đặt lại cookie đăng nhập của người dùng**
   Điều này cũng làm giảm nguy cơ truy cập trái phép.
6. **Thu hồi khóa bảo mật và quyền truy cập mật khẩu ứng dụng**
   Thu hồi mọi khóa bảo mật hoặc mật khẩu dành riêng cho ứng dụng đã được cấp quyền truy cập vào tài khoản của người dùng.
7. **Xóa tài khoản của người dùng**
   Di chuyển bất kỳ dữ liệu nào của người dùng mà bạn muốn lưu sang tài khoản khác. Sau đó xóa hoàn toàn tài khoản ban đầu của họ. Đây là cách tốt nhất để đảm bảo họ không thể truy cập vào dữ liệu của tổ chức bạn.