creativeOne
WEALTH

Lost or Stolen Laptop Procedures

Losing or having your work laptop stolen can be stressful, but acting quickly minimizes risks to company data, your personal information, and business operations. Follow these steps immediately—time is critical to prevent unauthorized access.

1. **Assess the Situation**: Double-check common spots where you might have left it (e.g., under a seat, in a bag, or at a desk). If you're in a public place like an airport, hotel, or office, contact lost-and-found immediately.

2. **Notifications**: Notify Supervisor (if applicable), C1W IT Department and C1W Compliance: Report the incident right away via phone or email. Provide details like the location, time, and any suspicious activity.

3**. Log Out of Cloud Services and Accounts**: From another device, sign into company apps (e.g., Google Workspace, Microsoft 365, email) and revoke access for the lost laptop. Look for "active sessions" or "devices" in account settings to log it out remotely. This prevents thieves from accessing cloud-stored files.

4. **Change All Relevant Passwords**: Update your company login, email, and any work-related accounts immediately, especially financial accounts. If multi-factor authentication (MFA) is enabled, verify it's still secure. Do the same for personal accounts if the laptop has autofill data.

5. **Enable Remote Features** (If Not Already Done):

- For Windows laptops: Use Find My Device to locate, lock, or erase the laptop once it connects to the internet.
- For MacBooks: Use Find My to mark it as lost, play a sound, or remotely wipe it.

6. **Monitor for Unauthorized Activity**: Check your work email and accounts for unusual logins. If personal financial info was on the device, contact your bank/credit card issuers to freeze accounts and monitor for fraud. Consider placing a fraud alert on your credit report.

7. **Document**: Note the exact time, location, circumstances, and steps you've taken. Share this with C1W IT Department and C1W Compliance.

Best Practice

- Always use a strong password and enable full-disk encryption (e.g., BitLocker for Windows, FileVault for Mac).