Data Security Best Practices During Travel

It is important to protect the data on your devices, especially in heightened situations where device loss, theft, or confiscation may be more likely.

Please follow the best practices outlined below to keep your data secure during travel. These practices significantly reduce the risk of data exposure, which protects you and the company.

Protect Yourself Before, During, & After Travel

Use these guidelines to reduce cyber risk while traveling or working remotely.

Report Cybersecurity issues immediately:

- **Urgent issues:** Contact the Global Technology Operations Center (24/7)
- **Non urgent support:** Reach out to the Service Desk
- **Lost mobile device:** If you lose your mobile device, or it is stolen, contact cybersecurity@wbd.com

Before You Leave

- Save important files to WBD-approved cloud storage, such as OneDrive or SharePoint; delete sensitive information from your devices
- Leave any non-essential devices at home
- Ensure all company managed laptops and mobile devices have the latest operating systems and apps installed
- Disable Wi-Fi and Bluetooth auto-connect features

During Travel

- Keep devices with you at all times or secured in a locked location
- Always use the company VPN when accessing the internet or company resources
- Use only trusted networks, personal hotspots, or mobile data; if in doubt, don't connect
- Avoid using public Wi-Fi unless absolutely necessary (VPN required)
- Be cautious in public spaces, use privacy screens when possible
- Stay alert to phishing and scams; do not click links in unexpected emails or messages
- Avoid public USB charging stations; use wall outlets, personal chargers, or a USB data blocker
- Limit browsing only access trusted, known websites
- Do not store passwords on devices; disable "remember passwords"
- Use only company-issued USB devices

When You Arrive/Return to a Safe Location

- Monitor accounts for unusual activity, like unexpected MFA requests or unusual device behavior
- Change all passwords for accounts accessed during travel
- Delete any travel apps or information you used on your trip but no longer need
- If you used a travel loaner device, return it so it can be securely wiped
- If your device was out of your control, contact the Service Desk or visit your local tech bar to scan it. Provide details about when it was out of your control, (e.g. Customs, airport security, etc.)

These guidelines should be followed in conjunction with the WBD Acceptable Use Policy (AUP). For questions related to this policy, contact cybersecurity@wbd.com.