Company Travel Cybersecurity Policy

Company Travel Cybersecurity Policy

Objective:

This policy outlines the cybersecurity measures and best practices that employees must adhere to when travelling overseas with their work laptops. The purpose is to safeguard company information, minimise cybersecurity risks, and ensure the secure use of technology during international travel.

1. Full Disk Encryption:

All work laptops must have full disk encryption enabled to protect data in the event of loss or theft. Employees are responsible for ensuring that encryption is active on their devices.

2. Strong Passwords:

Employees must use strong, unique passwords or passphrases for laptop logins. Two-factor authentication is encouraged for an added layer of security.

3. Software and Antivirus Updates:

Ensure that all software, including operating systems and antivirus programs, is kept up-to-date. Regular updates are crucial to patch vulnerabilities and protect against cyber threats.

4. VPN Usage:

When connecting to public Wi-Fi networks, employees must use a Virtual Private Network (VPN) to encrypt internet traffic and protect sensitive data from potential interception. Corporate VPN or 3rd party VPN's such as NordVPN, ExpressVPN.

5. Backup Data:

Before travel, employees must back up all critical data. Regular backups ensure that important information is not permanently lost in the event of theft or loss.

6. Laptops Should be Shut Down When Not in Use:

Laptops should be fully shut down when not in use. Shutting down the laptop will protect any company data stored in the laptop's memory (RAM).

7. Physical Security:

Employees should keep laptops physically secure. Cable locks are recommended, and laptops should not be left unattended in public spaces. Laptops should be secured into hotel safes when not in use.

8. Remote Wipe and Tracking:

Laptops must have remote wipe and tracking capabilities enabled. In case of loss or theft, IT can remotely erase sensitive data and track the device's location.

9. Separate Work and Personal Devices:

Employees are advised to use separate devices for work and personal use to minimise the risk of cross-contamination.

10. Disable Bluetooth and Unused Ports:

Employees should disable Bluetooth when not in use and turn off unused ports to prevent unauthorised access or malware infections.

11. Regular Check-ins:

Employees should check in regularly with the IT department while travelling to report any issues promptly.

12. Review and Follow Company Policies:

Employees must review and adhere to the company's cybersecurity policies, including data handling procedures, acceptable device use, and incident reporting.

Compliance:

Failure to comply with this policy may result in disciplinary action, including but not limited to suspension of travel privileges, loss of access to company systems, or termination of employment.

Acknowledgment:

I acknowledge that I have read, understood, and agree to comply with the company's travel cybersecurity policy.

Employee Name: _____

Date: _____

LAST PAGE