Essential Technology Practices for Employees Working Remotely

CHECKLIST

Tourism businesses that require people to work remotely (such as from home or when travelling) should follow guidelines when using technology to lessen the chance of disruptions or down time, help prevent security breaches, and protect records and information.

- ☐ **Ensure employees have proper technology and set-up**, for example:
  - Computer
  - Email
  - Phone conferencing
  - High-quality internet connection
  - Access to internal networks
  - Appropriate workstation: desk for computer, comfortable chair
- ☐ **Require workers to have a secured Wi-Fi network** with a trusted virtual private network (VPN)
- ☐ **Provide simple, accessible communications tools** (e.g., Teams, Slack, Zoom)
- ☐ **Provide orientation training to help employees set up remote workstation**:
  - Assist with getting the technology set up and connected
  - Review the tools and services available to staff to get started
  - Describe how to access company communications channels
  - Review cyber security and data management protocols
  - Let them know where they can access help, when needed
- ☐ **Implement guidelines for cyber security standards and procedures**, including:
  - Log-in procedures
  - Remote access
  - Use of personal devices
  - Information and data backup procedures
- ☐ **Apply cybersecurity policy** by establishing procedures, for example:
  - Follow password rules: create secure passwords, change passwords as required, do not share passwords
  - Use secure internet connections (e.g., do not use public networks)
  - Update software as required
  - Use secure software
  - Use secure web browsers and search engines
  - Follow protocols for allowing/removing cookies
  - Verify authenticity of emails or attachments
  - Report suspected breach of security immediately
- ☐ **Provide guidance on how to troubleshoot or resolve computer or applications issues**, for example:
  - Check power supply and internet connection (e.g., surge protection, battery status)
  - Check online for solutions
  - Have a dedicated staff person or third-party technology provider on call to assist, where needed

- ☐ **Implement policies on the management of data**:
  - Restrict access to authorized persons
  - Back up electronic files periodically
  - Verify antivirus and anti-malware software is working and updated frequently
  - Check system for infections on a regular basis
  - Report breach of confidentiality
- ☐ **Require employees to protect confidential records and documentation**:
  - Leave no private documents unattended
  - Label documents as confidential, where appropriate
  - Restrict access to authorized persons only
  - Keep computer screens from the sight of others

N O T E S