neuways
IT Strategy, Security & Support

Remote Worker Security Guidelines

Awareness

Corporate Devices

- Do not share your corporate devices with family or friends.
- All work-related activities must be performed on the device provided by your organisation.

Social Media Guidance

- Do not reveal business itineraries, corporate info, daily routines, etc.
- Be careful if sharing photos of your WFH setup online – your screen might contain sensitive information.

IT Checklist

- ☐ Enable local encryption.
- ☐ Secure local admin accounts with strong passwords.
- ☐ Limit external sharing of Cloud applications (OneDrive, Dropbox, etc).
- ☐ Maintain a robust data backup plan for all remote workers.
- ☐ Enable Mobile Device Management (MDM) for remote wipe capabilities.
- ☐ Enable remote Endpoint Security tools that can be centrally reviewed and monitored.
- ☐ Implement the Principle of Least Privilege (PoLP) so that remote workers only have access to the necessary services they need to fulfil their role effectively.
- ☐ Provide the means to securely exchange files and information, both internally and externally (eg. Office 365 encryption option enabled).
- ☐ Enable multi-factor authentication (MFA) for remote connectivity that expires after 4-8 hours of use.
- ☐ Review your incident response procedure with all relevant parties.

neuways
IT Strategy, Security & Support

Employee Checklist

- [ ] **Secure your workspace**
  - Lock your laptops and other business devices when not in use.
  - Conduct confidential business communications in private, free from eavesdropping.
- [ ] **Secure your WiFi**
  - Change your default router passwords.
  - Enable WPA-2 or stronger encryption.
  - Ensure your local router firmware is updated.
- [ ] **Review and comply with corporate policies and procedures.**
- [ ] **Secure personal devices**
  - Update Internet of Things device firmware (Smart thermostats, doorbells, surveillance cameras etc.)
  - Change default settings of all personal devices.
  - Keep software updated on all devices within your home network (including corporate devices, IoT devices, and home laptops & tablets).
- [ ] **Be wary of potential phishing attempts**
  - If a communication looks potentially harmful, call the sender to verify its legitimacy.