**Mobile Personnel Responsibility Policy**

**Overview**

This document describes Information Security's requirements for employees that work outside of an office setting.

**Scope**

This policy applies to any mobile device, or endpoint computer issued or used for company business which contains stored data owned by the company.

**Policy**

All employees shall assist in protecting devices. Mobile devices are defined to include desktop systems in a remote environment, laptops, tablets and cell phones.

**4.1 Endpoint Security**

Computer will be issued with *<endpoint security software>* installed. Employees are to notify the security department immediately if they see error messages for these products.

**4.2 Additional Software**

Personnel may install additional software needed for the performance of work duties after notifying security of the name of software and business purpose. The software will then be added to the catalogue of software in use.

**4.3 Public Remote Working**

Personnel in public spaces such as coffee shops should be aware of the risks of performing their duties in public.

* If taking a call either on a laptop or smartphone, earbuds should be used.
* Personnel should observant of anyone staring at a device's screen, and where possible orient themselves to prevent visual eavesdropping.
* Personnel should not leave USB drives or other portable data storage unattended.

**4.4 Smartphone Security**

Personnel have a responsibility to ensure that their phone is reasonably secured so no data can be exfiltrated if it is misplaced or stolen.

* Devices should have their lock screen enabled, either via passcode, fingerprint or pattern.
* Devices should have any encryption features turned on.
* Personnel must notify security immediately if their device is misplaced or stolen.

**Policy Compliance**

**Compliance Measurement**

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

**Exceptions**

Any exception to the policy must be approved by the Infosec team in advance.

**Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**Related Standards, Policies and Processes**

**Definitions and Terms**

None.

* **Revision History**

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| **Oct 2008** | SANS Policy Team | Initial Version |
| **July 2022** | Ivy Astrix | Initial draft. |