# Remote or Teleworking Policy

## Objective and Scope

The objective of this policy is to define the security measures to be put in place and adopted to manage risks in relation to remote and teleworking. This includes accessing, processing or storing information at teleworking sites.

The scope of this policy covers:

- all employees and other interested parties with access to secure organisational data or IS systems or personal private information as prescribed in the Privacy Policy
- working outside a formal workplace including working from home, commuting, or using flexible workplaces such as public transport or public places
- work using telecommunications devices including making use of the internet (internal or public), accessing the web, email accounts, or telephonic systems (mobile phones, public phones) regardless of whether devices used are company or privately owned.

## Roles, Responsibilities and Authorities

The Operations Director or competent IT Team delegate takes ownership of the data security protocols in place for remote and teleworking activities.

Responsibility of technology equipment for individual devices is assigned to users/owners for general use and compliance to this policy.

The Operations Director and the IT Team takes ownership of asset management in relation to assigning, tracking and return or redundancy of remote assets. Equipment and portable devices (regardless of ownership) are listed on the Asset Register against the assigned user.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

## Legal and Regulatory

| Title | Reference |
|---|---|
| The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000 | www.hmso.gov.uk/si/si2000/20002699.htm |
| Computer Misuse Act1990 | www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm |
| The Privacy and Electronic Communications (EC Directive) Regulations 2003 | www.hmso.gov.uk/si/si2003/20032426.htm |
| The Freedom of Information Act 2000 | https://www.legislation.gov.uk/ukpga/2018/12/contents |
| Online Safety Act 2023 | https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted |
| National Assistance Act 1948 | https://www.legislation.gov.uk/ukpga/Geo6/11-12/29/enacted |
| Criminal Law Act 1967 | https://www.legislation.gov.uk/ukpga/1967/58/introduction |
| The Copyright, Designs and Patents Act 1988 | https://copyrightservice.co.uk/ |

# Remote or Teleworking Policy

| **ISO 27001/2 REFERENCES** | ISO 27001: 2013 Clause ID | ISO 27002: 2013 Annex A ID | **ISO 27001: 2022 Clause ID** | **ISO 27002: 2022 Control ID** |
|---|---|---|---|---|
| Remote working | | 6.2 | | 6.7 |
| Mobile devices | | 6.2.1 | | 8.1 |
| Teleworking | | 6.2.2 | | 6.7 |

## Related Information

- Mobile Devices Policy - User endpoint devices
- Working from Home: WHS Checklist
- Physical (Equipment) Asset Management Policy (including maintenance and acceptable use of physical assets)
- Asset Register
- Information Classification Policy
- Clear Desk / Clear Screen Policy

## Policy

To ensure the security of information when personnel are working remotely *Prevision Research* requires a set of protocols to be followed regardless of ownership of devices used.
*Prevision Research* considers remote and teleworking to be any form of work outside a designated office location. Working from home, in all modes of transport or hotels is considered remote working.

*Prevision Research* accepts that privately owned mobile devices may be used remotely or for general company purposes only on approval by the Operations Director with agreed user standards in place. All roles with high risk IS access shall be provided with company owned equipment and cannot use these devices for any other purpose.

### Minimum company standards

Technologies including desktop computers, laptops and mobile phones shall be password protected with further access to company intranet or secure folders using an additional MFA process.

Data shall never be held on any remote device under any circumstance, all company data shall be stored via the cloud or designated approved destination.

### Work permitted to be undertaken via teleworking

# Remote or Teleworking Policy

1. No highly classified information shall be accessed via any public transit locations such as an airport, shopping centre or hotel.
2. Confidential information related to clients or projects may only be accessed through the company cloud functions with data transferred via secure means as agreed with the client.

## Physical security of remote locations (including home offices)

Any semi-permanent remote site, such as a home office or project office, is subject to a secure building arrangement with key access to office location and equipment.

Home offices shall have a dedicated location for working from home either as a shared office related room or separate office. The home must be locked and devices holding data turned off when premises are not attended. Where practical, segregate laptops and other devices from other household members.

All staff working from home are required to complete the Working from Home: WHS Checklist.

## Equipment used when working remotely

The use and management of laptops, desktops or mobile phones as applicable to the business remains applicable to remote offices and teleworking in transit.

Mobile phones used for business purposes whether company or privately owned require secure login passwords. Company supplied phones shall not be shared with other persons due to risk of access to company related emails.

Note that the company clear desk / clear screen policy applies to remote working.

## Device security

Computers, whether desktop or laptop, shall be virus and malware protected. Secure mechanisms for authentication and enabling of access privileges shall be established according to the Operations Director security and information classification level.

The owner or user of the device shall take responsibility to ensure all virus or malware software applications are maintained with current versions and patches. When a version change or patch update is notified on the device, this shall be enabled immediately.

Devices shall not be shared with other persons in the environment due to risk of access to company related data.

Note that the company Mobile Devices Policy (user endpoint devices) applies to devices used in remote working environments.

When working from hotels or when in transit between destinations, logging into hotel or other WiFi networks in cafes, airline lounges should be avoided. If this must occur, only use accepted protected networks. When in doubt use personal hotspots.

Portable devices are not to be left unattended in public places and are subject to a timeout screen saver requiring a login access.

# Remote or Teleworking Policy

## Suspected unauthorised access of devices

Report any lost, damaged property, unauthorised access, use or suspected malware activity immediately to the Operations Director. Provide details regarding likely impact on data security and effects on company or client information.

## Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change or a policy breach is known to have occurred. Refer below for the most recent review.

# History table

| Date | Rev No | Changes | Reviewed By | Approved By | Training Y/N |
|---|---|---|---|---|---|
| | | | | | |