IT POLICY

PHYSICAL SECURITY

Physical Security

Physical security is at the heart of any organisation's successful security strategy. Operating Companies wherever they are located in the world should have in place reasonable and appropriate controls to prevent unauthorised access to Operating Company systems and to prevent loss of data.

Whilst Instalcom recognises that the physical and environmental security challenges will vary between Operating Companies, the controls outlined below are recognised as good security protocols to have in place and Operating Companies should develop and document physical and environmental security processes and procedures that incorporate controls such as those identified in this Policy.

Physical Security Access Controls

Instalcom must operate an access control system to its site(s) e.g. swipe cards, combination door locks, lock & key, to ensure that only authorised persons are able to access Company premises. Office management or equivalent must maintain records (including electronic logs where possible) of persons entering Company sites and securely retain this information for at least three months. The purpose of retaining access information is to record who enters and leaves Company sites and may have gained access to confidential, proprietary, sensitive or critical information.

Particular emphasis and planning should be given to areas within the Operating Company where confidential, proprietary, sensitive or critical information is stored e.g. an IT server room or segregated work area and if appropriate, additional access controls should be implemented. Restrictions on IT server room access are set out in more detail in Server Room Access Policy.

Outgoing Staff and Physical Security

Whenever an Instalcom member of staff or freelancer leaves, all physical security access must be removed and deactivated. In cases where a member of Instalcom staff is serving their notice, the physical security access rights for that individual must be reviewed by appropriate senior management to ensure that any access permitted during the notice period adequately protects Company and client information.

Visitors to Operating Company Sites

Visitors to any Company site must be escorted at all times when in areas where there is confidential data. In the event that any visitor is granted access for more than one visit to any company site such access should be provided for a fixed time period and on a limited basis.

Security Alarm Systems

All Companies sites must be equipped with fire systems as required by law and physical intrusion alarm systems.

Physical Security of Operating Company Assets and Media

It is the responsibility of Instalcom staff to take care of Company computers and associated equipment when using them both inside and outside Company premises. Instalcom staff should take reasonable precautions to ensure that their laptops and other equipment (including mobile devices and memory sticks) are not left unsecured in unoccupied vehicles, hotel rooms, restaurants etc. Care should be taken to prevent physical damage, loss or theft.





IT POLICY

PHYSICAL SECURITY

Restrictions on Operating Company Server Room

Access Restrictions on IT server room access are set out in more detail in the Server Room Access policy.

Clear Desk Policy

Operating Companies should adopt and implement a clear desk policy which will apply to all staff. Where appropriate, staff should be provided with lockable storage for documentation and equipment in order to comply with the clear desk policy.

Physical segregation

Physical segregation of teams may be required by client contracts, discuss your client's requirements with senior management.

Signed.....Date: 15/01/21
Brian Lynch – Head of IT

Signed.....Date: 15/01/21
Vince Bowler - Managing Director