IT POLICY

NETWORK ACCESS SECURITY

Network access security is critical to safeguarding Instalcom data. Reasonable measures must be in place to protect all networks from unauthorised access.

Access to Company Networks

Where systems are supplied with default vendor username and passwords, default passwords must be changed, and usernames changed after first successful login.

Access should be provided to company staff based on their need and their role in the company and the department/team in which they work; staff should not have unrestricted access to all Company data except in the case of certain IT administrators where it is required as part of their role. Administration access must be limited, documented and controlled.

When access is given to freelancers and other temporary staff, particular care should be given to the level of access that they are given and named accounts should be created with a termination date matching their agreed engagement period.

When someone (whether employee or temp) re-joins the business after leaving their old account can be used but their new rights and access rules should reflect their new role only.

Generic accounts for use by multiple people must not be used.

End-user password configuration. Password configurations should be in accordance with current official guidance issued by the UK National Cyber Security Centre (NCSC).

Password configurations should be in accordance with current official guidance issued by the UK National Cyber Security Centre (NCSC). For legacy or existing contracts password configurations should be in accordance with Instalcom mandated length and expiration cycles set out below:

- Password Expiration: 90 days.
- Minimum Password Length: 7 characters.
- Account Lockout Trigger: 5 attempts.
- Account Lockout Duration: 30 minutes (or earlier if unlocked by IT).
- Minimum # Passwords Before Reuse: 24 cycles.
- Certain applications may not support this particular list of criteria; in that case this list is to be used as good practice and complied with so far as is possible.

Accounts with privileged access rights to operating systems should be given only to individuals suitably qualified and based upon validation of their understanding of the appropriate policies and procedures associated with those rights.

Regular, documented reviews of privileged access rights to operating systems should be undertaken. Passwords and other login criteria should not be given to other staff.

Mandated Security Measures to Prevent Unauthorised Access by External Parties Firewalls and other protective security technologies must be operated at the boundary between Operating Company systems and the outside world. This should be achieved through measures such as:





IT POLICY

NETWORK ACCESS SECURITY

- Implementing firewall policies.
- Checking firewall status regularly.
- Periodic review of logs.
- Maintenance of full configuration documentation
- Ensuring that the protective security technology software and firmware is patched in accordance with manufacturers' recommendations.

Malware Prevention and Monitoring

Malware includes viruses, Trojans and other malware including spam emails containing rogue attachments and/or internet links to spoofed websites. The following measures are required to be

The following measures are required to be implemented to limit the risk of malware:

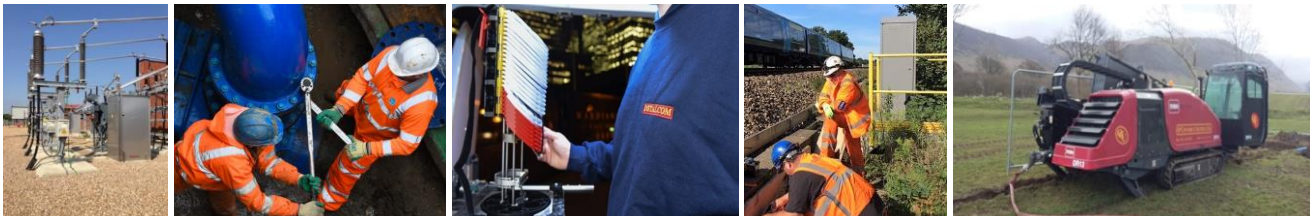
- Any system with an infection of any sort is to be removed from the network immediately to prevent further infection and negative impact to the business.
- All files must be scanned for vulnerabilities.
- All systems should be automated to scan for vulnerabilities regularly.
- All data should be scanned for vulnerabilities prior to being received in the business.
- E-mail attachments and files from external sources must be scanned by anti-virus software before they are loaded onto Instalcom systems.
- The latest security-update program must always be applied.
- Users must be provided with appropriate anti-virus support, including relevant information and preventive and remedial measures.
- Anti-virus software must be updated in accordance with manufacturer recommendations.

External Connectivity

External connection to clients and third parties should be restricted and limited to minimise risk of exposing Company systems to computer vulnerabilities.

Any permanent network connectivity to third party site (e.g. Site to Site VPN), whether client or otherwise, as well a direct access to our networks by third parties, must be configured and operated securely, utilise multi factor authentication, and must have the express permission of the Company Head of Group IT

Controls must be in place to ensure that any permanent network connectivity to our networks by third parties can be disabled, if required. Regular reviews should take place of such external connections and redundant connections removed or disabled.



IT POLICY

NETWORK ACCESS SECURITY

Signed.....Date: 03/01/22
Brian Lynch – Head of IT

Signed.....Date: 03/01/22
Vince Bowler - Managing Director