Policy-Active Directory Domain Policy

# SCOPE

The purpose of this policy is to ensure that only properly registered and configured ICT equipment is able to join the Link3.net domain, to improve the detection of vulnerable equipment and to enhance the manageability and security of Windows desktops and other devices connected to the Link3 network.

# POLICY

1. All computers and mobility devices running a Microsoft Windows operating system or an operating system that interoperates with a Windows domain and that are connecting to Link3’s corporate networks are required to join the “link3.net” Windows domain.
2. Native Windows authentication is used to control access to the Link3’s ICT services -this authentication is transparent to domain members who would otherwise be prompted for credentials when accessing services like network drives and print queues.
3. Company policies and other actions, with regard to security settings, patch levels or operating parameters, and services only will be applied and implemented on computers and mobility devices that have joined the domain.
4. Where computers and mobility devices are being used for R&D purposes and do not require access to central resources such as file or print servers, email or internet access then an exemption to domain membership must be sought through the relevant IT Office (Infrastructure).
5. Exemptions to domain membership are conditional upon the department involved accepting responsibility for maintaining adequate patching and virus protection levels, and may also be conditional upon the limiting of network access to the non-domain computer equipment.
6. Domain Admins group access is required to deploy & verify service pack and patch levels, virus definitions, software versions and (where necessary) to purge or remove virus infections.
7. IT will create an account in the Windows domain for computer equipment and mobility devices when these are entered into the Network Administration System (NAS) database.
8. No Domain computer accounts will be created directly from client machines.
9. Through Group Policy, each computer will be enrolled into security lockout for software installation/removal and for system configuration.
10. By default, local administrator account will be disabled through Group Policy for the whole organization.
11. Staffers personal computer will not be registered into the Link3’s official Link3.net domain.

# ENFORCEMENT

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# DISTRIBUTION

This policy is to be distributed to all Staff with access to Company’s Information Resources.