ALL SAINTS WOODFORD WELLS

Title	ICT Technical Guidelines
Owner	Operations Manager
Issue Date	November 2024
Reviewed By	Bob Darby
Approved By	PCC
Approved Date	February 2019 November 2024 March 2026
Next Review Due	March 2027

1 Purpose

The ICT Technical guidelines details and explain how the technical aspects of information security is to be implemented.

2 ICT Guidelines

1. Selection and deployment of networks, systems and servers shall address all security requirements and issues.
2. Physical and environmental security shall be designed in advance: e.g. putting critical assets such as network communication lines, servers, switches, firewalls and file servers in secured area(s). Entry to that environment shall be restricted to those whose job requires it.
3. Private IP addressing scheme shall be used for internal networks, to prevent internal network from access by external network.
4. The network security model shall adopt zoning i.e. segregation of network according to security requirements, e.g. the office network is totally isolated from the internet or servers and computers are located behind the firewall. Unsecured or unmanaged systems are not allowed to make connection to internal network.
5. Firewalls and network routers shall be hardened by limiting the administrative access to specified locations, closing unnecessary network services for incoming and outgoing traffic or using encrypted communication channel for administration.
6. Servers shall be configured to secure the operating system by uninstalling unnecessary services and software, patching the system timely and disabling unused accounts.
7. Applications shall be secured by means of installing security patches, hardening the configuration of the applications and running the application with a least privilege account.
8. Any third-party access or connections to the network will be based on a formal contract that satisfies all necessary security conditions.
9. The risk from viruses and malicious code shall be mitigated by ensuring anti-virus software is kept current with up-to-date signatures installed in desktop and network servers to prevent the spread of virus / worm.
10. Access rights and privileges shall be granted on an as-needed basis and shall be reviewed regularly. Access rights shall always be granted according to the principle of least privilege.
11. A standard secure pc/workstation configuration standard build shall be adopted
12. Backups shall be performed regularly, and recovery tested. Backups shall be stored off-site.
13. Regular patch management shall be undertaken.
14. Good documentation of configuration and procedure shall be maintained.
15. All IT equipment shall be disposed of securely, to prevent information from being ‘leaked’.