
# Network Access Control Policy

Version 2016.1

M J Church take seriously the security of its network. Access is strictly controlled to maintain security of the information it holds on behalf of customers, suppliers, employees and any other subjects it has information on. Access levels are regularly reviewed to maintain security and confidence in the information it holds.

**Scope of this Policy**
This policy applies to all M J Church site networks, IT systems and users both internal and external.

This policy sets out the requirements for all users, internal or external, to gain access to the M J Church network, IT systems and information held by M J Church on its servers and that of other hosted systems.

This policy applies to all devices capable of connecting to the M J Church network and to the information it holds. These devices include but are not limited to computers (desktop, laptop, tablet and notebook), mobile phones and other portable and removable media and devices.

**Responsibilities**
The IT department will be responsible for the issuing and monitoring of all passwords for access onto the M J Church network and for password access to internal application systems.

All users of M J Church IT equipment must strictly follow this policy.

All line managers should report any breach of this policy to the IT department. Failure to comply with this policy may result in disciplinary action being taken.

**Statement of Policy**
It is the policy of M J Church that all access rights should be restricted and controlled to maintain the security of information and systems.

M J Church reserve the right to monitor any and all aspects of the computer network including but not limited to all internet sites visited, file downloads and all communication sent and received by users.

**Policy Details**
M J Church maintain strict controls for access to its network, servers and the information that it holds. It performs this by use of the following:

Network Password Authentication:

All access to M J Church computers is achieved by the use of strong passwords. Passwords must be:

- at least eight characters in length;
- have at least one upper case character;
- have at least one number;
- have at least one special character;
- changed at least every 90 days;
- changed on first log on by a new user;
- materially different from any of the last 24 passwords used;
- kept secret from all other users;
- never written down or emailed to anyone.

Password authentication is done via Active Directory on one of M J Church domain controllers. The groups assigned to the user will dictate the level of access. Access rights are accorded following the principal of least privilege and need to know.

User accounts are immediately deactivated when an employee or contractor leaves.

Application Software:

All M J Church applications which store personal data are password protected. All users must change their initial password on first login and regularly change them thereafter on a monthly basis.

Remote Access Authentication:

M J Church gives remote access rights to a limited set of users. This is achieved using VPN connection using IP Protocol SSL. Access rights for remote users are continuously reviewed.

Guest Access:

Guest access is restricted at M J Church to selected areas only. Guests have access to the internet only. Passwords are regularly changed.

Application Software Provider Access:

Limited access is provided to external application support departments. Access is only granted when necessary, notified and authenticated.

USB lock down:

USB ports are locked down via a group policy roll out from the domain controller. Only a limited number of users have the rights granted to them to activate the USB ports on their computer.

Penetration testing:

M J Church regularly employ the services of outside contractors for penetration testing. The results of which are used to strengthen the security of the network.

Physical Security:

All server/comms rooms are restricted areas and are kept locked at all times. CCTV monitors the access to all of these areas.

User Requirements:

All users are required to:

- keep access passwords secret;
- never write down passwords;
- keep desks clear of customers, suppliers and any other clients personal information;
- if allocated a laptop it must be kept secure and not left visible inside a vehicle
- report immediately any lost or stolen laptop to the IT department and their line manager
- must report immediately to the IT department if they believe their password is no longer secret
- lock your computer when moving away from your desk

- must report immediately to the IT department if they observe any infringement of the above requirements

The lawful and correct treatment of personal information is vital to the successful operation of, and maintaining confidence within the company, and the individuals with whom it deals. Network security is a vital part of keeping information secure. M J Church has an obligation to its clients and the law to keep the data it holds secure.

For & on behalf of MJ Church

Steve Blower

Managing Director

Last reviewed: July 2017