IT Policy & Security 2025

Supported by
Intuitive Computer Management

Table of Contents

Toolkit Level 2 Security

MOHS have been keen to follow and implement the guidelines and recommendations for the Gov Toolkit V2 IT policies and Framework.

Projects have been completed and continued future work has been scheduled to keep the protection of IT Security, Data Protection and best practices in accordance with the Toolkit V2 and General IT Security recommendations up to date.

MOHS currently outsource all their IT Support and Consultancy to a local company who have helped re-develop in house systems & security.

IT Policy

MOHS strict in-house IT policy is a collection of policies that have been implemented to secure and streamline in-house IT systems:

- Active Directory Users and groups
- Data Permissions via NTFS
- Device Encryption
- Strong Password policies
- GPO based policies
- GPO unified logon control
- Logging & Auditing of sensitive Data
- Internet Policies that are controlled & Blocked by Security Appliances
- 2 Factor Authentication applied to email accounts. (2FA)

Security Policy

MOHS takes IT Security very seriously. Every Computer & Device connected to the Network is protected with Antivirus & Internet security, which is all centrally managed on in-house servers and monitored by the out-sourced IT Support Company.

Emails are now hosted within Microsoft 365 Platform and all users have been configured with (2FA) which includes enhanced logging, alerting and reporting capabilities with additional security measures using (DLP).

Data loss prevention (DLP) in Office 365 helps you identify, monitor, and protect sensitive information in your organization through deep content analysis. DLP is increasingly important for enterprise message systems, because business-critical emails often include sensitive data that needs to be protected.

USB and Data Pens are controlled via Network Policies and Antivirus Policies to make sure Exploits are blocked from transferring onto the MOHS IT infrastructure.

Data is locked down to prevent unauthorised access which is controlled via group policy access using Active Directory and NTFS Technologies.

Internet Failover

In the event of a Internet network failure. The new DrayTek router is equipped with a secondary 4G connection that will be utilised until the primary (main) broadband connection to the business is restored, at which point the router will switch back to using that connection. This is essential for cloud services to maintain a continuous connection with SharePoint, Email, Cloud and Phone services. In addition to the failover mode, the router can utilise both connections simultaneously to improve the total Internet bandwidth available to your network while both connections are available.

Data Protection for Remote Users

MOHS have enforced that all remote workers must have Antivirus protection on all devices that connect to the MOHS network for remote working. Laptops, Tablets & USB devices that carry MOHS Data are in the planning of centrally managed Encryption to help prevent Data loss and Data Protection.

Data Protection and GDPR

MOHS are continuing and planning further to facilitate the need to keep Data safe. Guidelines have been followed and implemented that helps reduce Data being exposed, lost or stolen. MOHS and ICM is committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Bill.

MOHS and ICM are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

Disaster Recovery

The important aspect of keeping Data safe has always been a high priority for MOHS. A recent investment has allowed the business to have a full Disaster Recovery solution implemented in accordance to further develop the IT infrastructure of the Business.

Continuous backups and Virtualisation technology will allow systems to be up at all times. In the event of complete devastation, all data is replicated outside of the Business to Cloud servers in virtualised formats allowing the business to be up and running very quickly in the event of disaster. ICM manage the Cloud backups and recovery using a graphical interface which alerts for failures during the backup process. Cloud Backup protects business data

and prevents downtime from natural disaster, hardware failures, accidental deletions, ransomware, or just user error—with fast restores from the cloud.

Cloud backup data centres are located in Slough and are designed to offer the security, availability and reliability you need to help safeguard vital business data.

DATA PROTECTION

All backup data is encrypted locally using AES 256-bit encryption prior to transfer to the data centre. Data is further protected in transit using TLS 1.2 over a secure connection.

PHYSICAL SECURITY

Data centres provide 24/7 security, including biometric hand geometry readers for every door and server cage. CCTV digital cameras cover the entire data centre, including cages with detailed surveillance and audit logs. Shipping and receiving areas are walled off from colocation areas, equipment is checked upon arrival, and critical areas have windowless exteriors.

RELIABILITY

Power: All data centres are equipped with full uninterruptable power supplies, backup systems, and N+1 (or greater) redundancy, including diesel electrical generators.

Physical Environment: Data centres are built above sea level, away from rivers and lakes, and have no basements, which protects against flooding. Moisture sensors and barriers, dedicated pumps, and more protect against water damage. Fire protection systems are multizone, dry-piped, double-interlocked, and pre-actioned. Very Early Smoke Detection and Alarm (VESDA) systems are also used.

Data centres meet or exceed local building codes for seismic design for earthquake protection.

Operating Environment: Data centres use robust HVAC for stable airflow and N+1 on all major equipment and up to N+2 on chillers and thermal energy storage.

Data centres use geo-diverse internet feeds for redundancy. Servers use best available hardware coupled with mission-critical support. All servers are protected through redundancy in hardware, and all storage is RAID6 (with mission-critical support).

Pen Testing

Mohs have recently invested in a Consultancy Administration Day which allows one of our IT Technical Consultants to continuously improve IT systems and Network security on a monthly basis. One of the important aspects of this is the continuous auditing and testing of the system, making sure that Windows Updates are applied to all relevant systems, Antivirus is protecting all that it should, Firewalled Routers & Gateways are carefully monitored, policies are regularly checked & applied and software is fully patched and kept up to date. Security improvements are continuously being applied and monitored for weakness.

Declaration

This report was created by the IT Support & Consultancy Company who are currently supporting MOHS Workplace Health.

Phil Gwinnell

Managing Director

Intuitive Computer Management

Tel : 01384 913914
Email : phil@intuitivecm.co.uk
Web : www.intuitivecm.co.uk

Last reviewed: December 2024