INFORMATION SECURITY POLICY

1. Purpose of this Document

The purpose of this document is to establish guidelines and procedures for securing, protecting, and managing the information necessary for Monitor Group's business operations and to outline the acceptable use of computer-based systems, software applications, and data processing by employees.

In addition it defines the tools and methods used to secure information held by Monitor Group, including the use of the electronic system for time and attendance tracking and ensures employees handle company data in a secure and confidential manner, in compliance with UK GDPR regulations.

2. Scope of this Document
This policy applies to all employees of Monitor Group, whether working on-site or remotely. It applies to all information held by Monitor Group and all IT systems, including the electronic time and attendance system for workforce management tracking.

3. Data Storage & Security
Monitor Group uses Datto Backup for cloud-based file storage, accessible only by external IT consultants with two-step authentication. Personal and confidential company data must only be stored on secure cloud storage or authorised systems such as Microsoft Office 365. Data held within the electronic time and attendance system, including time and attendance records, biometric data (if used), and PIN-based authentication records, is securely stored and protected in compliance with UK GDPR.

4. Transfer of Data
Employees may transfer data via Microsoft Office 365 email, which is secured by individual authentication and stored on dedicated UK/EU/US servers compliant with UK GDPR. Personal data must not be shared or transferred outside of company-approved platforms, including the electronic time and attendance system without management authorisation.

5. Removable Media
The use of removable media (USB sticks, external hard drives) for company data is strictly limited and requires senior management approval. Any data transferred must be immediately deleted after its required use.

6. Bring Your Own Device (BYOD)
Employees are discouraged from using personal devices to access company data. The electronic time and attendance system mobile app may be used for clocking in/out, provided security settings, including location tracking (if enabled), are properly configured. Any data stored on personal devices must be deleted once it is no longer required for work purposes.

7. Physical Security
Offices are secured with lockable doors and access control measures, including key codes. All paper-based records, including printed reports from electronic time and attendance system, must be stored securely and disposed of through confidential waste procedures.

8. Electronic Security

Data transmission is protected by a firewall system maintained by external IT support. Anti-virus and malware protection are installed on all company devices.
Wireless access is password-protected and restricted to business hours.

9. Password & Authentication Policy

All system passwords must:

- Be private and unique
- Be at least 8 characters long, with a combination of letters and numbers
- Never be written down or shared (except under managerial oversight in exceptional circumstances)

Electronic time and attendance system authentication methods include:

- Biometric fingerprint scanning (where enabled)
- RFID cards for authorised employees
- PIN-based access
- Facial recognition (where available)
- Mobile app login with secure user credentials

10. Acceptable Personal Use
Company systems are for business purposes. Limited personal use is permitted during break times but may be revoked if abused. Employees should not use company IT resources for personal financial gain, political activities, or inappropriate content.

11. Social Media
Company social media accounts must be used professionally and never for sharing confidential information.

12. Software Downloads
Employees must seek managerial approval before installing software on company devices. Unauthorised downloads may be removed without notice.

13. Clear Desk – Clear Screen Policy
Employees must lock their screens when away from their desks. Paper-based confidential information must be stored securely when not in use.

14. Support Functions
Data Breaches: Report immediately to a line manager or senior staff.
Network & IT Support: Managed by Verbo Computers.
Electronic time and attendance system issues: Any problems related to time tracking, biometric authentication, or access should be reported to your Manager or the Head Office Admin Team.

15. Data Retention & Deletion
Time and attendance records, including electronic time and attendance system data, will be stored in compliance with legal retention periods. Departing employees' biometric data (if applicable) will be removed from the electronic time and attendance system to ensure compliance with data protection laws. IT hardware will be disposed of securely, following CESG-approved data destruction methods.

16. Action resulting from a breach in this policy

Employees are expected to adhere to this policy at all times and Managers are expected to enforce it. Failure to adhere to this policy may result in disciplinary action.

17. Alteration to this policy

This policy will be subject to regular review and will be updated to reflect changing legislation and the changing needs of the business itself. Any revisions will be re-issued to all employees at that point.