Data Retention Policy			
Owner:	**Managing Director**	**Ref:**	**POL014**
		Revision:	**1**

1.0 SCOPE

This policy applies to all ITM Monitoring Limited (The Company) employees. This policy applies irrespective of grade, role or hours worked unless otherwise specified.

2.0 AIMS

To provide a procedure and set of principles regarding the processing and protection of personal data contained within manual records and on computer databases.

3.0 POLICY STATEMENT

The Data Protection Act 1998 came into force on March 1st 2000. This Act implements the European Data Protection Directive in the UK. The Company has compiled this Data Protection Policy to ensure that it complies with the above Data Protection Act. The data held, will only be stored whilst relevant, and will not be disclosed to any person without prior written consent from the individual concerned, unless required by law.

The personal data referred to in this policy will only be released as appropriate and in accordance with this policy.

Please refer to Appendix A for a Glossary of Terms & Definitions.

4.0 RIGHTS AND RESPONSIBILITIES
4.1 The Company

The Company is committed to upholding the following principles:

- Personal data will be processed fairly and lawfully.
- The amount of personal data held will be adequate, relevant and not excessive in relation to the purposes for which it is held.
- Personal data will be accurate and, where necessary, kept up to date.
- Personal data will be obtained only for specific and lawful purposes and will not be further processed in any manner incompatible with the purpose.
- Personal data will only be held for so long as it is necessary to enable specific and lawful purposes to be achieved.
- Personal data will be secured against unauthorised or unlawful processing, accidental loss, destruction or damage.
- Personal data may in relevant circumstances be transferred to a country outside of the European Economic Area which does not provide an adequate level of protection to the individual concerned. Where this is the case we will endeavour to treat such data in compliance with this policy.
- Sensitive and other personal data relating to an individual will only be processed by the Company as far as this may be required in connection with the employment of that individual by the Company and, if by the Data Processor, or in cases where ITM Monitoring Ltd. is the Data Processor, in accordance with any requirements or instructions imposed by the Data Controller (refer to Appendix A for Glossary of terms and definitions).
- If personal data is retained or processed, employees will be informed by the Company by way of its policies; employee handbooks, where applicable, and declarations completed when joining the Company of:

This literature will inform:

- The purpose for which data is being retained.
- To whom such data may be disclosed.
- The source of such data and who will have access to it, in an intelligible form upon request.
- How to have such data corrected or erased where appropriate.

4.2 Data Controller

- To submit applications for notification to the Information Commissioner. (SOCOTEC UK Ltd.)

4.3 Data Processors

- To inform the Data Controller of required details when establishing a new set of data or to utilise personal data in a manner not already covered in this policy (refer to section 5.7).

4.4 Company Data Protection Officer (DPO)

- SOCOTEC will act as the companies' DPO;
- To be the custodian of this policy.
- To ensure applications for notification are submitted to the Information Commissioner.

4.5 The Line Manager

- To ensure this policy is applied within their area of the business.
- To consult any queries raised in relation to this policy with the Human Resources Department before any action is taken.
- To forward all data requests to the HR department (for employee/supplier/customer).

4.6 Human Resources Department

- To assist the Line Manager and employee in answering any queries on the application or the interpretation of this policy prior to any action being taken.
- To keep a record of all data requests.

4.7 The Employee

- To comply with the terms of this policy.
- To forward all data requests to the HR department (for employees/supplier/customer).

4.8 Individual Rights

The Data Protection Act gives a number of rights to individuals in respect of data held about them. These rights are as follows:

- The right of the Data Subject to access their personal data.
- The right to be told by the Data Controller of the purposes or purpose for which the processing of the personal data is being undertaken.
- The right to prevent processing likely to cause any damage or distress (this is subject to certain exemptions).
- The right to prevent processing for the purposes of direct marketing.
- The right not to be subject to a decision that is based solely on automated decision-making.
- The right to compensation if the individual suffers damage by any contravention of the Act by the Data Controller or the Company.
- The right to rectify, block, erase or destroy inaccurate data.

5.0 LEGAL OBLIGATIONS
5.1 Consent to Process Data

The Company will only collect personal information about employees when that information is required for a legitimate business or legal reason. Under normal circumstances, personal data will only be obtained from the employee with his/her personal consent. Where appropriate to consult sources other than the employee, he/she will be informed that this is taking place.

Personal data may only be processed if one or more of the following conditions are met:

- The Data Subject has given his/her consent.
- The processing is necessary for performance of a contract, or entering into a contract.
- The processing is necessary for the administration of justice or to comply with any legal obligation to which the Company or employee is subject to.
- The processing is necessary to protect the vital interests of the employee.
- Without prejudice to the Data's Subject rights, freedoms or legitimate interests, when processing is necessary for the purpose of legitimate interests pursued by the Company or by a third party to whom data is disclosed.

A distinction is made between the need for "explicit" consent for the processing of Sensitive Personal Data, as opposed to the consent needed for other personal data.

"Explicit" consent includes consent given in writing.

"Explicit" consent should be obtained on each occasion the need arises to process sensitive personal data, e.g. a request for medical records or for a report on a medical condition.

In order to process personal data in accordance with the Data Protection Act, the Company requires employees to sign a Contract of Employment acknowledging that the Company will be processing personal data for all purposes relating to the employment. The Contract of Employment will be issued to potential employees at the time an offer of employment is made by the Company.

If any employee or potential employee considers that the information is not strictly necessary to the needs of personnel administration he/she should record his/her concerns with their Line Manager and Human Resources Department. The concern will be considered and may need to be referred to the Data Protection Officer for a decision to be made. The act of failing to supply information will not disadvantage the employee in any manner.

5.2 Retention of Personal Data
5.2.1 Storage

All documents relating to employment are contained in either electronic or paper files, in an individual file for each employee. These files will be held in the Finance Office.

The only exemptions are where paper copies of the following are retained:

- Next of Kin details.
- Current appraisal and objective performance review documentation – kept by the Line Manager within the employee's department, irrespective of whether the personnel file is held by Human Resources.
- Training and Development records – kept in Uckfield.
- Health and Safety assessments – kept by SHEQ Manager in Uckfield
- Medical Records and Health Screening Assessments – kept either by the Occupational Health provider or within the employee's Personnel Files.
- Pension information – kept by Human Resources and the nominated external Pension Provider.

Hard copy records may not be removed from the department in which they are kept without prior authorisation of a Human Resources Manager.

In addition, the Company in some cases stores and processes sensitive and other personal data electronically on the Payroll Database.

The Company will take due care with regard to the storage and protection of data provided by software and hardware security measures. Every effort will also be taken to ensure the reliability and confidentiality of managers authorised as responsible for maintenance of such information.

Similar standards of care will be required of all external third parties such as Career Development (Outplacement) Agencies or Benefits Providers appointed to process information on behalf of the Company.

5.2.2 Retention Period

The amount of data retained will be regularly reviewed so that only an appropriate amount is kept on record. This will be done in line with the Government Data Protection Act 1998.

However, in order to meet legal requirements, it is necessary to retain employee information for a considerable period after an employee has left the Company, in line with the Data Protection Code of Practice.

5.2.3 Accuracy of Information

The Company will take such reasonable action as necessary to ensure the accuracy of information. Data is deemed inaccurate if it is either incorrect or misleading as to any matter of fact.

In addition to the requirement for accuracy from a data protection perspective, information held is important for the correct administration of employee benefits and other detail, such as telephone numbers and contact details of the next of kin; it is also needed for Health and Safety reasons. For these and other employment reasons, it is a condition of employment that any change to the employee's circumstances, e.g. Home address, Personal telephone number, Next of Kin details etc., must be updated by the employee on the HR portal.

5.3 Access to Personal Data

All employees may request to see and have a copy of sensitive and other personal data held by the Company other than for:

- Management information if the release of such information could prejudice the Company's business interests.
- Information relating to negotiations with the Company if the disclosure would prejudice those negotiations.
- Information required for the purpose of Management forecasting and planning if the release of such information could prejudice the conduct of the business.
- Confidential references given by the Company before they are provided to a third party.

Employees do not have the right of access to information relating to another individual, or information identifying that individual as the source of the information sought by the employee, unless:

- The individual has given his/her consent for the information to be disclosed or
- It can be taken, in all circumstances that the individual has dispensed with their consent.

Employees should be aware that, in addition to members of the department in which the information is held, a manager or direct/indirect Line Manager responsible for their work activities might, in certain circumstances, also have access to their personal data.

Any employee who is concerned as to the nature or existence of any personal data may request access to the personal data (other than as stated above) held by the Company by applying in writing to the Human Resources Department, specifying the information that is required.

The Company will supply the information within 40 days, but it should be noted that if the original copy of the information held cannot be removed from its place of storage, the requesting individual will be accompanied by a member of the relevant department whilst viewing the requested information.

The individual may also request a copy of the information for retention but the Company reserves the right to charge an administration fee for the expense incurred in the supply of the information (currently £10.00).

Similarly, Managers may not remove the original copy of personal information held by the Company about their staff, from its normal place of storage, without prior authorisation from the relevant Human Resources Manager or Director and only after providing a written acknowledgment of the receipt of information.

5.4 Personal Data Storage

Sensitive and other personal data collected for employment purposes will only be used for such purposes. No important decisions will be made with regard to any individual using or referring to data that was collected for any other purpose.

Disclosure of information will only be permitted as referred to in this policy or if the individual has provided his/her consent.

Where the processing of data by automated means is likely to constitute the sole basis for any decision affecting the individual, such as is the case with certain psychometric tests, the individual will be informed of the logic involved in the decision making process.

Personal data will not be transferred to a country outside of the European Economic Area without the individuals consent to the transfer of the data and providing that the country's laws provide similar protection to the individual concerned.

5.5 References

Confidential references provided by the Company are exempt from the access provisions of the Data Protection Act. This includes references supplied for the following purposes:

- Education
- Training
- Employment
- Appointment to office
- Provision of any service

This means that employees may not see a reference supplied by the Company before it is sent. However, the exemption is not applicable and employee may have access to references the Company receives and/or to references sent by the Company once the intended third party has received them.

All referencing relating to past and current employees must be written either by a member of that Human Resources Function or by the Line Manager who will discuss the detail with their Human Resources Manager, when necessary. Factual references will be supplied by the Company, which confirm details such as length of service, position held and reason for leaving. Subjective statements will not be included within references supplied by the Company.

Should a Manager wish to provide a "Character Reference" for a former employee or a current employee, it must explicitly state that the reference is a personal reference from the individual concerned; it must not be sent on Company letterhead stationary and should not in any circumstances be considered to be the views of the Company.

5.6 Medical Records

For details of the right of access to any medical report prepared by a Medical Practitioner relating to employment, the employee must request the details from the Medical Practitioner concerned or the Human Resources Department.

Details of employees' rights under the Medical Reports Act 1988 are specified prior to any pre-employment or an employment medical being requested.

Any employee or any person authorised in writing by that employee, may also apply to receive details of any health record obtained by the Company. Similarly, should the Company wish to apply for details of employees' medical records retained by their General Practitioner the employees consent will be requested beforehand.

5.7 Notification

It is the responsibility of the Data Processors to ensure that they have informed the Data Protection Officer of the following details whenever they establish a new set of data or wish to utilise personal data in a manner that is not already notified:

- A description of the personal data and the purposes for which it is to be held and/or used.
- The source from which the data is to be obtained.
- Details of the person to whom the data may be disclosed.
- The names of any countries outside the UK to which the data may be transferred.

It must be noted by all Data Processors (or persons authorised by the Data Controller) that it is a criminal offence, subject to an unlimited fine, to knowingly or recklessly hold personal data of any description other than that specified in the notification entry, or to process the data in breach of the entry.

Misuse or lack of notification is therefore a disciplinary offence that may ultimately, subject to the terms of the Company's Disciplinary Policy and Procedure, result in the dismissal of an employee from the Company's employment.

5.8 Direct Marketing Activities

The Company will obtain individual consent using the Data Subject's contact information for marketing purposes.

5.9 Data Sharing Within the Company

Internal distribution of personal data collected and maintained by the Company i.e. distribution through directories, routine sharing of personal data within a group service line, should adhere to the following rules:

- Personal data should only be shared on a need to know basis.
- Passwords and other access controls should be employed to prevent unauthorised access and disclosure of personal data.
- Individual business contact information, such as name, email address, business phone, office position etc. may be distributed unless the individual reasonably objects.
- More confidential information such as; personal financial data, National Insurance number, home contact details, membership (Union, political, religious etc.), criminal record, physical or mental health, sexual orientation or race should not be shared without explicit individual consent.

6.0 EXEMPTIONS

Specific sets of information are exempt from the Data Protection Act and are therefore excluded from this policy. Information exempt from the Act is as follows:

- Information that the Company is required by law to make public.
- Information that the Company is required to make known in connection with legal proceedings.
- Information relating to national security.
- Personal data processed for the prevention of crime or prosecution of offenders or for the collection of Tax.
- Information relating to any regulatory activity.
- Information relating to special purposes, which may be one or more of the following:
- The purposes of journalism.
- Artistic purposes.

- Literary purposes.
- Confidential references given by the Company (refer to point 5.5).
- Management forecasts/Management planning (refer to point 5.3).
- Information relating to negotiations to the extent that such information would prejudice negotiations.

7.0 COMPLIANCE

Compliance with this policy is the responsibility of all employees. Any deliberate or reckless breach of this policy may lead to Disciplinary action and where appropriate, legal proceedings. Any questions or concerns about the interpretation or operation of this policy should be taken up with the relevant Human Resources Department through the employee's Line Manager.

Any individual who considers that the policy has not been followed in respect of personal data about him/herself, should raise the matter with the relevant Human Resources Manager initially. If the matter is not resolved, the employee should refer to the Grievance Policy.

Revision of Policy

The Company reserves the right to amend and/or withdraw this policy from time to time for any reason, including without limitation, to take account of changes in the law, best practice and/or business requirements.

As Managing Director, I am not only committed to a maintaining a robust Data Protection Policy but also passionate that it embodies everything ITM stands for as a business. As such, I will ensure that our system is communicated and understood at all levels and continues to deliver our customers' objectives and to meet the needs of the company.

Jon Scott
Managing Director

Next Review Date:
31/12/2018

==========

Please complete the required fields below and sign, agreeing to the content and requirements of this Privacy Policy.

Name :

Job Title :

Department :

Signature :

Date :

Please return this signed form to Sonia Ortela SHEQ Manager.

Appendix A

GLOSSARY OF TERMS AND DEFINITIONS

The following terms are used throughout the policy and its application. These definitions comply with those used within the Data Protection Act. Each term is therefore defined as follows:

"DATA"

Information which:
- Is processed by equipment operating automatically in response to instructions given for that purpose.
- Is recorded with the intention that it should be so processed.
- Is recorded as part of a relevant filing system.

"DATA CONTROLLER"

The Company (SOCOTEC UK) who determines the purposes for and the manner in which personal data is to be processed.

"DATA PROCESSOR"

Any person who processes the data on behalf of the Data Controller.

"DATA SUBJECT"

The individual who is the subject of the personal data.

"EEA"

European Economic Area – Any country that is within the European Economic Community.

"EMPLOYEE"

May include past, present and potential employees.

"Information Commissioner's Office"

The UK's independent public body set up to promote access to official information and protect personal information.

"OTHER DATA SUBJECTS and THIRD PARTIES"

May include contractors, suppliers, contacts, referees, friends or family members.

"PERSONAL DATA"

Data consisting of information that relates to a living individual who can be identified from that information, or from that and other information in possession of the Data Controller, including any expression of opinion about the individual and any indications of the intention of the Data Controller or any other person in respect of that individual.

"PROCESSING"

Obtaining, recording, holding or carrying out any operation on data; such as the organisation, adaptation, alteration, retrieval, disclosure, dissemination, rearranging or destruction of the information or data.

Please note: It is irrelevant whether the information is stored as a manual record or is automatically processed (i.e. computer or word processed).

"RELEVANT FILING SYSTEM"

Any set of information that is not processed by means of equipment, but is structured in such a way that specific information relating to a particular individual is readily accessible.

"SENSITIVE PERSONAL DATA"

Personal data consisting of information as to racial or ethnic origins; political, religious or other opinions/beliefs of a similar nature; physical or mental health; sexual life; criminal offences or alleged criminal offences and past sentences; and whether he/she is a member of a Trade Union.