INFORMATION PROTECTION AND SECURITY POLICY STATEMENT

This document sets out the data protection arrangements we have established for MIRIS International Limited, all subsidiaries and associated companies (hereinafter referred to as 'MIRIS').

The need to retain and protect personal data varies widely with the type of data held by the MIRIS. Some personal data can be immediately deleted while other data will need to be retained into the future. This policy seeks to describe MIRIS's policy for specific data retention, protection and deletion.

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media.

1. PURPOSE

Information is a major asset that MIRIS has a responsibility and requirement to protect. The protection of information assets is not simply limited to covering the stocks of information (electronic data or paper records) that MIRIS maintains, it also addresses the people that use them, the processes they follow and the physical computer equipment used to access them.

This Information Protection Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained. The following policy details the basic requirements and responsibilities for the proper management of information assets at MIRIS. The policy specifies the means of information handling and transfer within the Business.

2. SCOPE

This Information Protection Policy applies to all the systems, people and business processes that make up the Business's information systems. This includes all Directors, Employees, contractual third parties (in particular PC Support Group) and sub-contractors who have access to Information Systems or information used for MIRIS purposes.

MIRIS collects personal data such as name, address, phone number, email address, and bank details which are used by us in the course of employment for legitimate interests under GDPR. We only collect the personal data we need, and we shall ask employees for their formal permission to do so when they commence employment with us.

3. REGULATION

MIRIS is required to comply with the General Data Protection Regulation 2016 (GDPR), the Data Protection Act 1998 and the Data Protection (Amendment) Act 2003. In August 2017, the Government passed the Data Protection Bill which brought GDPR into UK law in May 2018. There are some instances, however, where other legislation and regulations will supersede the GDPR and these are detailed below.

In the event of a data loss, destruction or transmission, MIRIS will be obliged to report this to the individual or company affected, as well as the Information Commissioner's Office (ICO) which has power to impose a financial penalty for a breach up to €20 million or 4% of worldwide turnover. There

is a mandatory requirement to report the breach to the individual and to the ICO within 72 hours of MIRIS becoming aware of it.

The ICO has advised that all UK businesses will need to comply with GDPR despite Brexit. This is because it will affect all data subjects in Europe or carrying out processing of data in Europe or about European data subjects.

MIRIS recognises that there are risks associated with users accessing and handling information in order to conduct official business.

In addition to GDPR, MIRIS shall comply with the following legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001

4. RISKS

This policy aims to mitigate the following risks:

- non-reporting of information security incidents
- inadequate destruction of data
- loss of direct control of user access to information systems and facilities.
- security of client systems utilised by deployed sub-contractors
- uses of portable information systems for example hard drives and USB drives

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our clients.

5. POLICY COMPLIANCE

If any user is found to have breached this policy, they may be subject to MIRIS disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the appropriate manager.

6. POLICY GOVERNANCE

The following table identifies who within MIRIS is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

Responsible – the person(s) responsible for developing and implementing the policy.

Accountable – the person who has ultimate accountability and authority for the policy.

Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.

Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Shawn Lowe, Senior Operations Manager (SOM)
Accountable	Mike Williams, Chief Executive Officer (CEO)
Consulted	
Informed	All employees and sub-contractors

Ultimate responsibility for information security rests with the CEO of MIRIS, but on a day-to-day basis the SOM/OM will be responsible for managing and implementing the policy and related procedures

Line Managers are responsible for ensuring that permanent staff and contractors are aware of:

i. The information security policies applicable in their work areas

ii. Their personal responsibilities for information security

iii. How to access advice on information security matters

Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard.

Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

7. POLICY FRAMEWORK

7.1. Management of Security

At board level, responsibility for Information Security shall reside with the CEO.

MIRIS SOM shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

7.2. Information Security Awareness Training

Information security awareness training shall be included in the staff induction process.

An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

7.3. Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.

Information security expectations of staff shall be included within appropriate job definitions.

7.4. Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

7.5. Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

7.6. User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

7.7. Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

7.8. Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

7.9. Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

7.10. Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by PC Support Group.

7.11. Information security events and weaknesses

All information security events and suspected weaknesses are to be reported to the CEO. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

7.12. Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission. Users breaching this requirement may be subject to disciplinary action.

7.13. User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of CEO before they may be used on MIRIS systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

7.14. Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

MIRIS reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime

- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.
- Any monitoring will be undertaken in accordance with the above act and the Human Rights Act

7.15. Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the before they commence operation.

7.16. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the CEO.

7.17. Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the CEO. Users shall not install software on the organisation's property without permission. Users breaching this requirement may be subject to disciplinary action.

7.18. Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

7.19. Reporting

The SOM shall keep the CEO informed of the information security status of the organisation by means of regular reports and presentations.

8. PERSONAL DATA

MIRIS collects personal data such as name, address, phone number, email address, and bank details which are used by us in the course of employment for legitimate interests under GDPR. We only collect the personal data that we need, and we shall ask employees for their formal permission to do so when they commence employment with us.

8.1. Employment by MIRIS

To comply with our contractual, statutory, and management obligations and responsibilities, we process personal data, including 'sensitive' personal data, from job applicants and our employees. Such data includes information relating to health, employment history and any criminal convictions.

In certain circumstances, we may process personal data or sensitive personal data, without explicit consent. Further information on what data is collected and why it's processed is given below.

Contractual responsibilities include those arising from the contract of employment. The data processed to meet contractual responsibilities includes data relating to payroll, bank account, postal address, sick pay, annual leave, maternity/paternity pay, pensions and emergency contacts.

Statutory responsibilities are imposed through law on MIRIS as an employer. The data processed to meet our statutory responsibilities includes data relating to tax, national insurance, statutory sick pay, statutory maternity/paternity pay, family leave, work permits, equal opportunities monitoring.

Management responsibilities are related to the functioning of MIRIS. The data processed to meet management responsibilities includes data relating to recruitment and employment, training and development, absence for whatever reasons, disciplinary matters, email address and telephone number.

8.2. Sensitive Personal Data

GDPR defines 'sensitive personal data' as information about racial or ethnic origin, political opinions, religious beliefs or other similar beliefs, trade union membership, physical or mental health, sexual life, and criminal allegations, proceedings or convictions.

In certain limited circumstances, we may legally collect and process sensitive personal data without requiring the explicit consent of an employee.

- We will process data about an employee's health where it is necessary, for example, to record absence from work due to sickness, to pay statutory sick pay, to make appropriate referrals to our Occupational Health Provider, and to make any necessary arrangements or adjustments to the workplace in the case of disability. This processing will not normally happen without the employee's knowledge and, where necessary, consent.

- We will process data about, but not limited to, an employee's racial and ethnic origin, their sexual orientation or their religious beliefs only where they have volunteered such data and only for the purpose of monitoring and upholding our equal opportunities policies and related provisions.

- Data about an employee's criminal convictions will be held as necessary.

9. SHARING DATA WITH THIRD PARTIES

In order to carry out our contractual and management responsibilities, we may, from time to time, need to share an employee's personal data with one or more third party supplier.

To meet the employment contract, we are required to transfer an employee's personal data to third parties, for example, to end user clients requesting information about contracted service providers, or, to pension providers and HM Revenue & Customs. To fulfil our statutory responsibilities, we're required to give some of an employee's personal data to government departments or agencies e.g. provision of salary and tax data to HM Revenue & Customs.

10. DATA RETENTION

It is not practical or cost-effective to save all data. Some data must be retained to protect MIRIS's interests, preserve evidence and audit trails, while generally conforming to good business practices. Reasons for data retention include:

- Litigation.
- Accident Investigation.
- Regulatory requirements.
- HMRC requirements.
- Intellectual property preservation.

When identifying and classifying MIRIS's data it is important to understand where that data is stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information. All data will be held within the MIRIS Data Management System and on individual terminals.

11. DATA RETENTION REQUIREMENTS

This section sets out the agreed guidelines for retaining the different types of company data that are held by MIRIS:

- Customer data will be held for as long as the organisation remains a customer of MIRIS, plus 6 years.
- Personal and sub-contract employee data will be held for the duration of employment and then for 6 years after the last date of contractual employment.
- Employee contracts will be held for 3 years after the last day of contractual employment.
- Company and employee tax related payment records will be held for 6 years.
- VAT records will be held for 6 years.
- Recruitment details including interview notes and CVs for qualifying candidates will be held for 1 year after the interview. This personal data will then be destroyed. All personal data will be destroyed for those candidates who do not display the qualities or standards required by MIRIS on completion of an open day.

If any data retained under this policy is stored in an encrypted format the encryption keys must be retained as long as the data key to decrypt is retained. Reference to the CEO should be made if there is any doubt as to how data should be encrypted, and keys retained.

12. DATA DESTRUCTION/RETENTION

Data destruction is a critical part of the data retention policy. Data destruction ensures that MIRIS uses data efficiently thereby making data management and data retrieval more cost effective. There are good reasons to delete data after a reasonable amount of time. These include the following:

- It is easier to keep more limited amounts of data secure.
- It is easier to find specific data in a response to a Subject Access Request, or when searching data for other purposes.
- It is consistent under GDPR to securely delete data that is no longer required for its original purpose.
- If it is retained for a long period, it is more likely to be inaccurate and out of date.

When the above timeframe expires, company staff must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, they should identify the data to their line manager so that an exception to the policy can be considered. Exceptions may only be approved by the CEO of MIRIS.

At present there is no automated facility by which emails, and files can be automatically destroyed. It will be necessary to carry out these tasks manually. Consideration should be given to mapping data flows in a Data Privacy Impact Assessment (DPIA) to identify the different locations and format of data held.

If security is not maintained and there is a data loss, the fact that excessive data has been retained, and therefore put at risk, is a factor which the ICO will take into account when considering whether to impose a civil penalty and the level of that penalty. The breach is more likely to be regarded as serious if no old data has ever been deleted, if there is no data retention policy, or if no thought has been given to whether old data should be deleted.

MIRIS specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to themselves is expressly forbidden, as is destroying data in an attempt to cover up a violation of law or company policy.

13. ENFORCEMENT

This policy will be enforced by the CEO of MIRIS. Violations will result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, MIRIS may report such activities to the applicable authorities.

14. SUBJECT ACCESS REQUESTS (SAR)

If you would like further information on your rights or wish to exercise them, please contact the SOM. You will be asked to provide the following details:

- The personal information you want to access.
- Where it is likely to be held or how MIRIS came into possession of the data.

- The date range of the information you wish to access.

We will also need you to provide information that will help us confirm your identity. If we hold personal information about you, we will give you a copy of the information in an understandable format together with an explanation of why we hold and use it. Once we have all the information necessary to respond to your request we'll provide your information to you within one month. This timeframe may be extended by up to two months if your request is particularly complex.

15. DATA BREACH PROCESS

If you become aware of a breach of the Data Protection Act, the GDPR or its obligations under a client contract, you must inform the CEO immediately who will report the incident immediately to the client and/or the ICO. A Data Breach Report must be completed and passed to the CEO.

A data breach will include, but not be limited to:

- Any loss, destruction or inappropriate transmission of personal data.
- This will relate to both client/contractor data and Company employees.

The CEO is responsible for any investigation, escalation and resolution measures deemed necessary as the result of an incident and will maintain a log of all security incidents.

When a security incident is reported, a decision will have to be made to whether an investigation into the incident will be carried out and who will be tasked to carry out the investigation.

Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal) evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

The CEO will advise on the appropriate course of action and any further actions to be taken. Security investigations must address the following:

- What happened and its impact?
- Root cause analysis of why it happened and how?
- What needs to be done immediately to prevent further damage and facilitate initial recovery?
- What needs to be done in the longer term to prevent a further occurrence?
- Identify if any person is culpable and whether disciplinary action is necessary.

For all investigations, a record must be maintained throughout the conduct of the investigation and the resolution of the breach. Investigation records must include:

- Nature of the breach.
- When, how and who discovered the breach?

- To whom and when was the breach escalated?
- Details of actions taken, when, and by whom, together with results.
- Details of any emergency measures implemented to contain the exposure.
- Details of agreed permanent solution.
- Impact assessment.

A decision on the need to inform the client and the ICO will be taken by the CEO. Under GDPR, both the client and the ICO must be informed of any personal data breach within 72 hours of MIRIS becoming aware of it.

16. CHANGES TO THIS DATA PROTECTION POLICY

The CEO may amend this policy to ensure it remains up to date and reflects how and why we use your personal data and new legal requirements. You will be advised of any future changes and asked to confirm your understanding and acceptance.

…….

Michael Williams

Chief Executive Officer

August 2022