DATA PROTECTION POLICY

1. Policy, scope and objectives

1.1 The Board of Directors of **Suro Consulting Limited**, located at (Address) are [within the context of its Information Security Policy] committed to compliance with all relevant UK and EU laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose information we collect in accordance with the General Data Protection Regulation (GDPR).

To that end, The Board of Directors/Principals has developed, implemented, maintains and continuously improves a documented personal information management system ('PIMS') for **Suro Consulting Limited**

1.2 Scope

The scope of the PIMS taking into account organisational structure, management responsibility, jurisdiction and geography.

1.3 Objectives of the PIMS

Suro Consulting Limited's objectives for the PIMS are

- that it should enable the firm to meet its own requirements for the management of personal information;
- that it should support organisational objectives and obligations; that it should impose controls in line with the firm's acceptable level of risk;
- that it should ensure that the firm meets applicable statutory, regulatory, contractual and/or professional duties; and that it should protect the interests of individuals and other key stakeholders.

1.4 **Suro Consulting Limited** is committed to complying with data protection legislation and good practice including:

a. processing personal information only where this is strictly necessary for legitimate organisational purposes;
b. collecting only the minimum personal information required for these purposes and not processing excessive personal information;
c. providing clear information to individuals about how their personal information will be used and by whom;
d. only processing relevant and adequate personal information;
e. processing personal information fairly and lawfully;
f. maintaining an inventory of the categories of personal information processed by the firm;
g. keeping personal information accurate and, where necessary, up to date;
h. retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;
i. respecting individuals' rights in relation to their personal information, including their right of subject access;
j. keeping all personal information secure;
k. only transferring personal information outside the EU in circumstances where it can be adequately protected;
l. the application of the various exemptions allowable by data protection legislation;
m. developing and implementing a PIMS to enable the policy to be implemented;

n. where appropriate, identifying internal and external stakeholders and the degree to which these stakeholders are involved in the governance of the firm's PIMS; and
o. the identification of workers with specific responsibility and accountability for the PIMS.

Notification

1.5 **Suro Consulting Limited** has notified the Information Commissioner that it is a data controller and that it processes certain information about data subjects. **Suro Consulting Limited** has identified all the personal data that it processes, and this is contained in the Data Inventory Register

1.6 A copy of the ICO notification details is retained by the appointed person with the firm (The Data Protection Officer) and the ICO Notification Handbook is used as the authoritative guidance for notification.

1.7 The ICO notifications are automatically renewed annually.

1.8 The Data Protection Officer is responsible, each year, for reviewing the details of notification, in the light of any changes to the firm's activities (as determined by changes to the Data Inventory Register and the management review) and to any additional requirements identified by means of data protection impact assessments.

The policy applies to all Employees [and interested parties] of **Suro Consulting Limited** such as outsourced suppliers. Any breach of the GDPR or this PIMS will be dealt with under the firm's disciplinary policy and may be a criminal offence, in which case the matter must be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for the firm, and who have or may have access to personal information, are expected to have read, understood and to comply with this policy.

No third party may access personal data held by the firm without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which the firm is committed, and which gives the firm the right to audit compliance with the agreement.

2. Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

3. Definitions used by the organisation (drawn from the GDPR)

Territorial scope – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour to data subjects who are resident in the EU.

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old. The processing of personal data of a child under 13 years of age is only lawful if parental or custodian consent has been obtained.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data, which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

4. Responsibilities under the General Data Protection Regulation

4.1 **SURO CONSULTING Limited** is a data controller and/or data processor under the GDPR.

4.2 Anyone in a managerial or supervisory roles throughout **Suro Consulting Limited** are responsible for developing and encouraging good information handling practices within the organisation; responsibilities are set out in individual job descriptions.

4.3 The Data Protection Officer a member of the senior management team, is accountable to Board of Directors/Principals of the firm for the management of personal information within the firm and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

- development and implementation of the PIMS as required by this policy; and
- security and risk management in relation to compliance with the policy.

4.4 The Data Protection Officer, who the Board of Directors/Principals considers to be suitably qualified and experienced, has been appointed to take responsibility for the firm's compliance with this policy on a day-to-day basis. In particular, has direct responsibility for ensuring that the firm complies with the GDPR, as do Line Managers in respect of data processing that takes place within their area of responsibility.

4.5 The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request procedure and are the first point of call for Employees seeking clarification on any aspect of data protection compliance.

4.6 Compliance with data protection legislation is the responsibility of all members of the firm who process personal information.

4.7 The firm's Training Policy sets out specific training and awareness requirements in relation to specific roles and to members of the firm generally.

4.8 Staff are responsible for ensuring that any personal data supplied by them, and that is about them, is accurate and up-to-date.

5. Risk Assessment

Objective: To ensure that the firm is aware of any risks associated with the processing of particular types of personal information.

SURO CONSULTING Limited has a process for assessing the level of risk to individuals associated with the processing of their personal information. Assessments will also be carried out in relation to processing undertaken by other organisations on behalf of the firm.

SURO CONSULTING Limited shall manage any risks, which are identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

Where a type of processing, using new technologies is likely to result in a high risk to the "rights and freedoms" of natural persons, the firm shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

A single assessment may address a set of similar processing operations that present similar high risks.

Where, as a result of a Data Protection Impact Assessment, it is clear that the firm is about to commence processing of personal information that could cause damage and/or distress to the data subjects, the decision as to whether or not the firm may proceed must be escalated for review to The Data Protection Officer.

The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the [supervisory authority].

Appropriate controls will be selected [from ISO27001 Annex A] and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the requirements of the GDPR.

6. Data protection principles

All processing of personal data must be done in accordance with the following data protection principles of the Regulation, and the firm's policies and procedures are designed to ensure compliance with them.

6.1 Personal data must be processed lawfully, fairly and transparently, **SURO CONSULTING Limited's** Fair Processing Procedure is set out in a separate document.

GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms".

Information must be communicated to the data subject in an intelligible form using clear and plain language. The specific information that must be provided to the data subject must as a minimum include:

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the Data Protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

6.2 Personal data can only be collected for specified, explicit and legitimate purposes.
Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of the firm's GDPR registration.

The firm's fair processing policy sets out the relevant procedures.

6.3 Personal data must be adequate, relevant and limited to what is necessary for processing.

- The Data Protection Officer is the GDPR Owner and is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.
- All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the the Data Protection Officer.
- The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by [internal audit/external experts] to ensure that collected data continues to be adequate, relevant and not excessive.
- If data is given or obtained that is excessive or not specifically required by the firm's documented procedures, Name is responsible for ensuring that it is securely deleted or destroyed in line with the firm's policy for disposal of storage media.

6.4 Personal data must be accurate and kept up to date.

- Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
- The firm are responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
- It is also the responsibility of individuals to ensure that data held by the firm is accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate at the date of submission.
- Staff should notify the firm of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the firm to ensure that any notification regarding change of circumstances is noted and acted upon.
- The Data Protection Officer is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
- On at least an annual basis, The Data Protection Officer will review all the personal data maintained by the firm, by reference to the Data Inventory Register. The DPO will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed in line with the firm's policy for disposal of storage media.
- The Data Protection Officer is responsible for making appropriate arrangements that, where third party organisations may have been passed inaccurate or out-of-date personal information it is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal information to the third party where this is required.

6.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

- Where personal data is retained beyond the processing date, it will be [minimised/encrypted/pseudonymised] in order to protect the identity of the data subject in the event of a data breach.
- Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.
- The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in the firms record retention procedure, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

6.6 Personal data must be processed in a manner that ensures its security

6.7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

These controls have been selected based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

Security controls will be subject to audit and review, following the

6.8 Personal data shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.

6.8.1 Safeguards

An assessment of the adequacy by the data controller considering the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

6.8.2 Binding corporate rules

SURO CONSULTING Limited may adopt approved Binding Corporate Rules for the transfer of data outside the EU. This requires submission to the relevant Supervisory Authority for approval.

6.8.3 Model contract clauses

SURO CONSULTING Limited may adopt approved model contract clauses for the transfer of data outside of the EU. If the firm adopts the model contract clauses approved by the relevant Supervisory Authority there is an automatic recognition of adequacy.

6.8.4 Exceptions

In the absence of an adequacy decision, including binding corporate rules, a transfer of personal data to a third country, or an international organisation, shall take place only on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.
  A list of countries that satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.*

6.9 Accountability

The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR.

Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs (Data Processing Impact Assessment), comply with requirements for prior notifications, or approval from supervisory authorities and appoint a Data Protection Officer if required.

7. Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the GDPR. To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

7.1 To request the ICO to assess whether any provision of the GDPR has been contravened.

7.2 The right for personal data to be provided to them in a structured, commonly used and

7.3 machine-readable format, and the right to have that data transmitted to another controller.

7.4 The right to object to any automated profiling without consent.

Data subjects may make data access requests as described in the our subject access request procedure this procedure also describes how the firm will ensure that its response to the data access request complies with the requirements of the Regulation.

Complaints

Data Subjects who wish to complain to **SURO CONSULTING Limited** about how their personal information has been processed may lodge their complaint directly with the Data Protection Officer. The Data Protection section of you client facing material will need to be modified to include a GDPR complaints section.

If operating a website the firm will need create a form, usually on the 'Contact Us' section of the website, into which data subjects can enter the details of their complaint. They will need to be shown the Fair Processing Notice at this point.

Data subjects may also complain directly to the ICO and the DPO in writing.

Where data subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint to the Data Protection Officer. The right to do this will be included in the GDPR section of our complaints procedure.

8. Consent

SURO CONSULTING Limited understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

SURO CONSULTING Limited understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties, which demonstrate active consent.

Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances, consent to process personal and sensitive data is obtained routinely by the firm using standard consent documents.

Where the firm provides online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit – which may be no lower than 13.

9. Security of data

All Employees are responsible for ensuring that any personal data, which the firm holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the firm to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. You should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or
- Stored on (removable) computer media, which are encrypted.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees of **SURO CONSULTING Limited**. All Employees are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit [written] authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with [procedure reference].

Personal data may only be deleted or disposed of in line with the Data Retention Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

10. Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held by the firm in electronic format and manual records, which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the firm, and information obtained from third-party organisations about that person.

Subject Access Requests are dealt with as described in the relevant procedure

11. Disclosure of data

SURO CONSULTING Limited must ensure that personal data is not disclosed to unauthorised third parties, which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees should exercise caution when asked to disclose personal data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the firm's business.

The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer

12. Retention and disposal of data

Personal data may not be retained for longer than it is required. Once a member of staff has left **SURO CONSULTING Limited**, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

Disposal of records

Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the secure disposal procedure