TORQUAY HOLDINGS TRADING AS MVIS LTD AND BARTCO UK LTD

DATA POLICY HANDBOOK

DATA PROTECTION POLICY & PROCEDURES

1. POLICY STATEMENT

Torquay Holdings Limited Trading as MVIS Ltd and Bartco UK Ltd *(hereinafter referred to as the **"Company"**)* needs to collect data to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, customers, suppliers and clients and includes *(but is not limited to),* name, address, email address, date of birth, IP address, identification numbers, private and confidential information, sensitive information and bank/credit card details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the ***General Data Protection Regulation (GDPR)***, ***UK data protection laws*** and any other relevant data protection laws and codes of conduct *(herein collectively referred to as **"the data protection laws"**).*

The Company has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities and we are proud to operate a ***'Privacy by Design'*** approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

2. PURPOSE

The purpose of this policy is to ensure that the Company meets its legal, statutory and regulatory requirements under the general data protection laws (**GDPR**) (EU) 2016/679) and to ensure that all personal and special category information is processed compliantly and, in the individuals, best interest.

The data protection laws include provisions that promote accountability and governance and as such the Company has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third parties on the responsibilities of handling and accessing personal data and data subject requests.

3. SCOPE

This policy applies to all staff within the Company (*meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and*

agents engaged with the Company in the UK or overseas). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

3.1 DEFINITIONS

- ***"Biometric data"*** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.
- ***"Binding Corporate Rules"*** means personal data protection policies which are adhered to by the Company for transfers of personal data to a controller or processor in one or more third countries or to an international organisation.
- ***"Consent"*** of the data subject 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 relating to him or her.
- ***"Cross Border Processing"*** means processing of personal data which: -
    - takes place in more than one Member State: or
    - which substantially affects or is likely to affect data subjects in more than one Member State
- ***"Data controller"*** means, 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 processor"*** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- ***"Data protection laws"*** means for the purposes of this document, the collective description of the GDPR, Data Protection Bill and any other relevant data protection laws that the Company complies with.
- ***"Data subject"*** means an individual who is the subject of personal data
- ***"GDPR"*** means the *General Data Protection Regulation (EU) (2016/679)*
- ***"Genetic data"*** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- ***"Personal data"*** means 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.

- ***"Processing"*** means 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"*** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- ***"Recipient"*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- ***"Supervisory Authority"*** means an independent public authority which is established by a Member State
- ***"Third Party"*** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

4. NATIONAL DATA PROTECTION LAW

As the Company is in the UK, we are obligated under the ***General Data Protection Regulation (GDPR) (EU)2016/679)*** and the **UK's Data Protection Bill [HL] 2017-19** that implements the GDPR into UK law. Our data protection policies and procedures adhere to both the GDPR and Data Protection Bill requirements, as applicable to our business type.

4.1 General Data Protection Regulation (GDPR)

As the Company processes personal information regarding individuals (*data subjects*), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

4.2.1 PERSONAL DATA

Information protected under the GDPR is known as *"personal data"*: -

The Company ensures that a high level of care is afforded to personal data falling within the GDPR's **'special categories'** *(previously **sensitive personal data***), due to the assumption that this type of

information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the GDPR advises that: -

"Processing of 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 the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies."

4.2.2 THE GDPR PRINCIPLES

Article 5 of the GDPR requires that personal data shall be: -

a) processed lawfully, fairly and in a transparent manner in relation to the data subject

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation')***

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality').***

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles'* ***('accountability')*** and requires that firms ***show***

how they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

4.3 The Information Commissioners Office (ICO)

The Information Commissioners Office (ICO) is an independent regulatory office who report directly to Parliament and whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes: -

- The Data Protection Act 1998 *(pre-25th May 2018)*
- General Data Protection Regulation *(post-25th May 2018)*
- The Privacy and Electronic Communication (EU Directive) Regulations 2003
- Freedom of Information Act 2000
- The Environmental Information Regulations 2004

The ICO's mission statement is *"to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals"* and they can issue enforcement notes and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the data protection laws the ICO, as the UK's data protection authority (*Supervisory Authority*), will have a similar role as previously, when it comes to oversight, enforcement and responding to complaints with regards to the data protection laws and those firms located solely in the UK.

The Company are registered with ICO and appear on the Data Protection Register as a data controller of personal information.

Our Data Protection Registration Number is ZA293688 Bartco UK, ZA8225872 MVIS Ltd, ZA8225879 Torquay Holdings Ltd

5. OBJECTIVES

We are committed to ensuring that all personal data processed by the Company is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

The Company has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

The Company ensures that: -

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws
- Every business practice, function and process carried out by the Company, is monitored for compliance with the data protection laws and its principles
- Personal data is only processed where we have verified and met the lawfulness of processing requirements
- We only process special category data in accordance with the GDPR requirements and in compliance with the Data Protection Bill Schedule 1 conditions
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested
- All employees are competent and knowledgeable about their GDPR obligations
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary
- We monitor any GDPR news and updates, to stay abreast of changes, notifications and additional requirements
- We have controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection
- We have appointed **Data Control Officers - Anne Ashman and Dominic Bridge** who will take responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR
- We have a Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued compliance
- We provide clear reporting lines and supervision with regards to data protection
- We store and destroy all personal information, in accordance with our **retention policy** and schedule which has been developed from the legal, regulatory and statutory requirements and suggested timeframes
- Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- We have developed appropriate technical and organisational measures and controls for personal data security and have a robust Information Security program in place

6. GOVERNANCE PROCEDURES

6.1 ACCOUNTABILITY & COMPLIANCE

Due to the nature, scope, context and purposes of processing undertaken by the Company, we carry out information audits to identify, assess, measure and monitor the impact of such processing. We have implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the data protection laws and can evidence such measures through our practices.

Our main governance objectives are to: -

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all employees
- Identify key stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance and ensure that the designated person(s) has sufficient access, support and budget to perform the role
- Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures that the Company has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated information security policies.

6.1.1 PRIVACY BY DESIGN

We operate a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We have developed controls and measures *(detailed below*), that help us enforce this ethos.

Data Minimisation

Under Article 5 of the GDPR, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of our minimalist approach. We only ever obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Measures to ensure that only the necessary data is collected includes: -

- Electronic collection *(i.e. forms, website, surveys etc*) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include *'optional'* fields, as optional denotes that it is not necessary to obtain
- Physical collection *(i.e. face-to-face, telephone etc*), only that which is relevant and necessary is collected
- We have documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement
- Forms, contact pages and any documents used to collect personal information are reviewed annually to ensure they are fit for purpose and only obtaining necessary personal information in relation to the legal basis being relied on and the purpose of processing

Restriction

Our *Privacy by Design* approach means that we use company-wide restriction methods for all personal data activities. Restricting access is built into the foundation of the Company's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information. Special category data is restricted at all levels and can only be accessed by **senior management or directors.**

6.2 Legal Basis for Processing *(Lawfulness)*

At the core of all personal information processing activities undertaken by the Company, is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company
- Processing is necessary for the purposes of the legitimate interests pursued by the Company

or by a third party (*except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).*

6.2.1 PROCESSING SPECIAL CATEGORY DATA

Special categories of Personal Data are defined in the data protection laws as: -

Processing of 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 the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.

Where the Company processes any personal information classed as special category or information relating to criminal convictions, we do so in accordance with Article 9 of the GDPR regulations and in compliance with the Data Protection Bill's Schedule 1 Parts 1, 2, 3 & 4 conditions and requirements.

We will only ever process special category data where: -

- The data subject has given explicit consent to the processing of the personal
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

Schedule 1, Parts 1, 2 & 3 of The Data Protection Bill provide specific conditions and circumstances when special category personal data can be processed and details the requirements that organisations are obligated to meet when processing such data.

Where the Company processes personal information that falls into one of the above categories, we have adequate and appropriate provisions and measures in place prior to any processing. ***Measures include: -***

- Having an appropriate policy document in place when the processing is carried out, specifying our: -
    - policies as regards the retention and erasure of personal data processed in reliance on the condition
    - retention periods and reason *(i.e. legal, statutory etc)*
    - procedures for reviewing and updating our policies in this area

6.2.2 RECORDS OF PROCESSING ACTIVITIES

As an organisation with ***less than*** 250 employees, the Company does not maintain records of our processing activities. However, we continually review all such activities and company size to ensure that we will begin to record such information as detailed in GDPR Article 30 where: -

1. We employee 250 or more employees
2. Processing personal data could result in a risk to the rights and freedoms of individual
3. The processing is not occasional
4. We process special categories of data or criminal convictions and offences
5. Such records are maintained in writing, are provided in a clear and easy to read format and are readily available to the Supervisory Authority upon request.

6.3 THIRD-PARTY PROCESSORS

The Company utilise external processors for certain processing activities *(where applicable*). We use information audits to identify, categorise and record all personal data that is processed outside of the company, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. ***Such external processing includes*** *(but is not limited to**): -***

- IT Systems and Services, Hosting or Email Servers
- Legal Services
- Debt Collection Services
- Payroll
- Credit Reference Agencies
- Direct Marketing/Mailing Services

We have strict due diligence in place and review, assess all processors prior to forming a business relationship. We obtain company GDPR polices and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

The continued protection of data subjects' rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

The Processor Agreement and any associated contract reflects the fact that the processor: -

- Processes the personal data only on our documented instructions
- Seeks our authorisation to transfer personal data to a third country or an international organisation (*unless required to do so by a law to which the processor is subject*)
- Shall inform us of any such legal requirement to transfer data before processing
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to security the personal data at all times
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists the Company in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments
- When requested, deletes or returns all personal data to the Company after the end of the provision of services relating to processing, and deletes existing copies where possible
- Makes available to the Company all information necessary to demonstrate compliance with the obligations set out in the agreement and contract
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract
- Informs the Company immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

6.4 DATA RETENTION & DISPOSAL

The Company have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects *(e.g. shredding, disposal as confidential waste, secure electronic deletion)* and prioritises the protection of the personal data in all instances.

7. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

The Company does not currently carry out any processing activities that are defined as requiring a DPIA.

8. DATA SUBJECT RIGHTS PROCEDURES

8.1 CONSENT & THE RIGHT TO BE INFORMED

The data protection law defines consent as; *'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 relating to him or her'.*

Where processing is based on consent, the Company have reviewed and revised all consent mechanisms to ensure that: -

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes
- Consent is always given by a statement or a clear affirmative action (*positive opt-in*) which signifies agreement to the processing of personal data
- Consent mechanisms are upfront, clear, granular (*in fine detail*) and easy to use and understand
- Pre-ticked, opt-in boxes are **never** used
- Where consent is given as part of other matters (*i.e. terms & conditions, agreements, contracts*), we ensure that the consent is separate from the other matters and is **not** be a precondition of any service (*unless necessary for that service)*
- Along with our company name, we also provide details of any other third party who will use or rely on the consent
- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case
- We keep detailed records of consent and can evidence at a minimum: –
    - that the individual has consented to the use and processing of their personal data
    - that the individual has been advised of our company name and any third party using the data
    - what the individual was told at the time of consent
    - how and when consent was obtained
- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it

and is available through multiple options, including: -

- Opt-out links in mailings or electronic communications
- Opt-out process explanation and steps on website and in all written communications
- Ability to opt-out verbally, in writing or by email

- Consent withdrawal requests are processed immediately and without detriment
- Controls and processes have been developed and implemented to refresh consent, especially those relating to parental consents
- For special category data, the consent obtained is explicit *(stated clearly and in detail, leaving no room for confusion or doubt*) with the processing purpose(s) always being specified

8.1.1 CONSENT CONTROLS

The Company maintain rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent and is documented in all instances.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from those matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorised by the Data Control Officer prior to being circulated.

Consent to obtain and process personal data is obtained by the Company through: -

- Face-to-Face
- Telephone
- Email/SMS
- Electronic *(i.e. via website form*)

Electronic consent is always by a non-ticked, opt-in action, enabling the individual to provide consent after the below information has been provided.

Privacy Policies are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

8.1.2 INFORMATION PROVISIONS

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc*), we provide when requested the below information in all instances, **in the form of a privacy Policy: -**

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of our Data Control Officer
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- Where the processing is based
- If applicable, the fact that the Company intends to transfer the personal data to a third country or international organisation and the existence/absence of an adequacy decision by the Commission
    - where the Company intends to transfer the personal data to a third country or international organisation without an adequate decision by the Commission, reference to the appropriate or suitable safeguards the Company has put into place and the means by which to obtain a copy of them or where they have been made available
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

The above information is provided to the data subject when requested and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent, unless there is a legal requirement to keep the information longer.

8.2 PRIVACY POLICY

The Company defines a Privacy Policy as a document, form, webpage or pop-up that is provided to individuals at the time we collect their personal *data (or at the earliest possibility where that data is obtained indirectly)*.

Our Privacy Policy includes the Article 13 (*where collected directly from individual*) or *14 (where not collected directly)* requirements and provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

We have a link to our Privacy Policy on our website and provide a copy of physical and digital formats upon request. The Policy is the customer facing policy that provides the legal information on how we handle, process and disclose personal information.

The Policy is easily accessible: -

- Via our website

With lengthy content being provided in the privacy Policy and with informed consent being based on its contents, we have tested, assessed and reviewed our privacy Policy to ensure usability, effectiveness and understanding.

Where we rely on consent to obtain and process personal information, we ensure that it is: -

- Displayed clearly and prominently
- Asks individuals to positively opt-in
- Gives them sufficient information to make an informed choice
- Explains the different ways we will use their information
- Provides a clear and simple way for them to indicate they agree to different types of processing
- Includes a separate unticked opt-in box for direct marketing

8.3 EMPLOYEE PERSONAL DATA

As per the data protection law guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Staff Handbook which informs them of their rights under the data protection laws and how to exercise these rights.

8.4 THE RIGHT OF ACCESS

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data*

Subjects), in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

8.4.1 SUBJECT ACCESS REQUEST

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has or will be disclosed to a third country or international organisation and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where personal data has not been collected by the Company from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Subject Access Requests (SAR) are passed to the **Data Control Officer** as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

SARs are always completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

Please refer to our external ***Subject Access Request Procedures*** for the guidelines on how an SAR can be made and what steps we take to ensure that access is provided under the data protection laws.

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

8.5 RECTIFICATION & ERASURE

8.5.1 CORRECTING INACCURATE OR INCOMPLETE DATA

Pursuant to Article 5(d), all data held and processed by the Company is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The **Data Control Officer** is notified of the data subjects request to update personal data and is responsible for validating the information and rectifying errors where they have been notified.

The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

8.5.2 THE RIGHT TO ERASURE

Also, known as *'The Right to be Forgotten'*, the Company complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by the Company is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

8.7 THE RIGHT TO RESTRICT PROCESSING

There are certain circumstances where the Company restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subjects request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit.

Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

The Company will apply restrictions to data processing in the following circumstances: -

- Where an individual contest the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
- Where an individual has objected to the processing (*where it was necessary for the performance of a public interest task or purpose of legitimate interests*), and we are considering whether we have legitimate grounds to override those of the individual
- When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure
- Where we no longer need the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

The Data Control Officer reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third parties. Where data is restricted, and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

8.8 OBJECTIONS AND AUTOMATED DECISION MAKING

Data subjects are informed of their right to object to processing in our Privacy Policy's and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material. ***Individuals have the right to object to: -***

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority *(including profiling*)
- Direct marketing (*including profiling*)
- Processing for purposes of scientific/historical research and statistics

Where the Company processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on *'grounds relating to their particular situation'*. We reserve the right to continue processing such personal data where: -

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, the Company will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

9. OVERSIGHT PROCEDURES

9.1 SECURITY & BREACH MANAGEMENT

Alongside our *'Privacy be Design'* approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred.

We carry out information audits to ensures that all personal data held and processed by us is accounted for and recorded. We have implemented adequate and appropriate technical and organisational measures to ensure a level of appropriate security.

Whilst every effort and measure are taken to reduce the risk of data breaches, the Company has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

10. Transfers & Data Sharing

The Company takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimisation methods.

We use approved, secure methods of transfer and have dedicated points of contact with each Member State organisation with whom we deal.

11. Audits & Monitoring

This policy and procedure document details the extensive controls, measures and methods used by the Company to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the data protection laws and associated laws and codes of conduct. In addition to these, we also carry out regular audits and compliance monitoring processes, with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The Data Control Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable. Data minimisation methods are frequently reviewed and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the Data Control Officer and are made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to: -

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data
- To monitor compliance with the data protection laws and demonstrate best practice

12. TRAINING

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. New and existing employees are trained, assessed and supported and include: -

- GDPR Workshops & Training Sessions
- Assessment Tests
- Coaching & Mentoring
- 1:1 Support Sessions
- Scripts and Reminder Aids
- Access to GDPR policies, procedures, checklists and supporting documents

Employees are continually supported and trained in the data protection laws requirements and our own objectives and obligations around data protection.

13. PENALTIES

The Company understands its obligations and responsibilities under the data protection laws and recognises the severity of breaching any part of the law or Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. ***We recognise that: -***

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations (*Chapter IX*) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

14. RESPONSIBILITIES

The Company has appointed **Data Control Officers** whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DCO will work in conjunction with the senior management to ensure that all processes, systems and staff are operating compliantly and within the requirements of the data protection laws and its principles.

The DCO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledge for the role they undertake.

ASSET DATA MANAGEMENT POLICY

1 INTRODUCTION

Asset Management is the process of identifying, classifying, managing, recording and coordinating a firm's assets (*physical, IT and information*) to ensure their security and the continued protection of any confidential data they store or give access to.

For the purposes of this policy and associated asset management processes, **Torquay Holdings Trading as MVIS Ltd and Bartco UK Ltd** *(hereinafter referred to as the **"Company"**)* defines an ***'Asset'*** as any item, system, application or entity that has potential or actual value to our organisation. Such assets include, but are not limited to: -

- Information (*including personal data*)
    - Paper records
    - Electronic records
    - Files and folders
    - Software licenses
- Systems
- Computers or Workstations
- Networks
- Servers
- Hardware
- Software
- Telephony Systems
- Equipment
- Databases
- Technology
- Printers/Scanners
- Fax Machines

Assets can be both tangible and intangible and are of value to a company based on their importance, function and use. Whilst information is one of the Company's most valuable assets, we understand the association and importance of the IT and physical assets that use, process, store and provide access to such information. As such, all forms of assets recorded by the Company are valued and afforded a high level of protection and governance.

1.1 Definition

For the purposes of our Information Security program and the references in this policy, when we refer to '***Information Assets'*** we are collectively describing all assets within the Company that are identified, recorded and secured. Most of our assets, including IT and physical are in place with the main purpose

of holding and protecting personal information and as such we refer to all assets collectively as ***'Information Assets'***.

2 POLICY STATEMENT

The Company understands the importance of identifying, recording and classifying our assets and utilise an Information Asset Register (IAR) to retain a complete list of all current assets, their location, value, access and other vital data. We have a responsibility to manage our physical and information assets, stemming from various legal, regulatory, contractual and business obligations: -

- General Data Protection Regulation (GDPR)
- Data Protection Bill
- Contractual (*client agreements, business objectives etc*)
- Security Requirements (*e.g. encryption, backups, updates etc*)
- Equipment Management (*service, replacement, disposal*)

The Company ensures that all assets used and retained during business, are properly documented, are assigned an owner and are subject this policy and subsequent procedures. Managing our assets is paramount to the continuity of our business and to the Company's reputation. Assets are protected where applicable, further aiding in the protection of personal information and confidential data.

3 PURPOSE

The purpose of this policy is to achieve and maintain appropriate protection of organisational assets (*tangible and intangible*) and to document those assets to ensure knowledge and understanding of their value, purpose, risk and location. The Company ensures that all assets are assigned an owner who has overall responsibility for managing, updating, recording and destroying the asset.

The nature and value of every asset is documented and understood, better enabling the Company to restrict access where applicable, develop effective recovery and continuity programs and protect the interests and assets belonging to customers and clients.

Understanding the Company's assets, enables us to manage our organisation's information and systems and the risks associated with them. For this purpose, we utilise an Information Asset Register (IAR) to identify, document and map all information assets and assign them an owner.

4 SCOPE

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas)*. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

5 OBJECTIVES

The Company is committed to ensuring compliance with the rules, standards and regulations with regards to asset management and the protection of the personal information in our remit. We have strict aims and objectives for achieving and maintaining the appropriate protection of all organisational assets.

The Company's objectives regarding asset management are to: -

- Develop and maintain a defined and robust Asset Management Policy
- Ensure that compliance all information assets have been identified
- Document all assets on the **Information Asset Register (IAR)** and assign each one an owner for monitoring and accountability
- Define the access to each asset and apply restrictions where applicable
- Maintain an up-to-date **Retention Policy**
- Ensure that all staff are aware of the regulations and their obligations regarding asset management and to provide sufficient and adequate support and training in this regard

6 GUIDELINES AND PROCEDURES

The Company takes several measures and steps to ensure that asset management is effective and adequate for managing and protection information. This policy is disseminated to all staff, who are aware of the value and importance of good records when it comes to the information held and processed by us.

6.1 Unclassified & Short-Term Information Assets

Due to the volume of information assets used by the Company during business, there are some assets which are considered minor and as such are not subject to being classified or documented. This is only applicable where the asset has no security value and will not result in any internal or external risk if accessed. Such assets are also not assigned an owner or inventoried due to their limited nature.

The Company operates under the GDPR and as such complies with the principle to never retain any information where there is no longer a purpose or reason to do so, however some records and information assets must be retained by law for specific retention periods and may come under our non-classification policy.

There is also a requirement due to the nature of our business, to obtain some information assets for limited and short-term periods. Such assets can include letters, spreadsheets, temporary files and reports. These are needed during business but are not classified or inventoried. All staff are aware of

their responsibility for the documents they create, and this is further highlighted in our ***Data Retention Policy.***

6.2 Remote Access & Bring Your Own Device (BYOD)

The Company employees have a requirement to use company assets (*physical and information*) outside of the office. Such instance can include during business trips, remote working, client visits and during travel. There are also facilities for using a self-owned device in the workplace, such as mobile phone. We understand the important of asset management for non-company devices and company assets used away from the office and have a robust ***Remote Access & BYOD Policy*** in place.

Regarding asset management when working remotely, it is the Company's aim to protect our staff, other people (*clients, service providers, customers, suppliers etc*), organisational assets and systems when they are off-site. Our **Information Security Program** consists of several policies and procedures that overlap in this area and provide our robust and structured approach, controls and measures for protecting assets and access whilst off-site.

These documents include, but are not limited to:

- Risk Management Policy & Procedures
- Access Control & Password Policy
- Data Breach Policy
- Remote Access & BYOD Policy
- Asset Management Policy
- Clear Desk & Screen Policy
- Data Protection Policy & Procedure

Please refer to the Company's ***Remote Access & BYOD Policy*** for full guidance on measures and controls for off-site use of assets.

6.3 Acceptable Use of Information Assets

Information assets are pivotal to the services offered by The Company and to ensure a secure and effective environment. Employees and third parties are provided with access and use of such assets to aid business functions and client assistance. This use is governed by our Acceptable Use standards and failure to comply with these principles will result in contract termination.

The Company has documented and implemented this acceptable use section in our Asset Management Policy to reiterate and provide guidelines on using our own and client assets. This information is disseminated to all employees, third parties and visitors to the Company and forms part of our agreements and terms. All assets, with emphasis on client assets are used in a professional, lawful and ethical manner at all times and are audited on a monthly basis to ensure adherence to this ethos.

Such acceptable use covers all assets and includes, but is not limited to: -

- Email systems
- Internet usage
- Telephones (*including mobiles*)
- Computers & laptops
- VPN Access, networks and portals
- Microsoft Teams
- Zoom
- Online chat on website

Specific emphasis is placed on adhering to this policy for employees who work from home and/or off-site and use or have access to information assets.

6.3.1 Acceptable Use Standards

The Company has documented and disseminated the below acceptable use standards to provide guidance and rules for using assets. These standards are adhered to by all employees and are a contractual part of any client visit or third-party access to the Company's information assets.

Employees, third parties and visitors are informed that they: -

- Must not do anything to jeopardise the integrity of the systems, information assets or physical assets
- Are not permitted to damage, change, reconfiguring or move any system or information asset with written authorisation and management supervision
- Are not permitted to remove any information asset from the Company building without written permission
- Must not attempt to access, delete, modify or disclose Information Assets belonging to other people without their permission
- Are not authorised to use any external systems, applications or technology with existing assets without permission and supervision
- Cannot disable or in any way alter system firewalls, anti-virus software or software/hardware protection applications
- Must not move any physical asset without written permission, including, but not limited to desktop PCs, printers, scanners, monitors or fax machines
- Are not permitted to load any unauthorised software onto The Company systems
- Must not connect to the Company network or any equipment other than in approved circumstances
- Must not create, download, store or transmit unlawful or indecent material

- Are not authorised to purchase or otherwise acquire any technology assets without the knowledge and authorisation of a director.
- Always agree to abide by these rules and confirm that the installation of any software on desktop PCs or laptops must only be carried out by IT
- Observe the Company's Data Protection and Information Security policies and guidance in all instances

6.3.2 Internet & Email Usage

The internet is a pivotal part of the services offered by the Company and as such, must be accessible to all employees during their work hours. However, we recognise the security risks of using the internet and so access is only available through the Company's local network or secured wireless network with the appropriate infrastructure and firewall protection. The internet is not permitted for personal use without prior permission from the Commercial & Operations Director. The Company have also restricted the sharing of files on certain systems and for some individuals, dependant on their need to use such facilities.

Email is necessary for the service provision offered by the Company and is afforded to all employees. This is our main communication tool and enables quick and effective access to clients, customers and other service providers. Email is accessible via secured connection and the sending of files or personal information is restricted to a user required level. Encryption methods are used and are detailed in our **Encryption Policy**, along with secure credentials.

6.4 Removable Media

The Company defined *'removable media'* as any type of storage device or object that is physically able to be disconnected and removed from a system or computer whilst it is active. Such media types include, but are not limited to USB's, Media Cards, CDs, DVDs and SD cards.

We strictly control the use and oversight of removable media due to their nature and increased access and security risk. Removable media makes it easy for a person to move programs, data and content from one computer to another and as such, the Company ensures that all employees and third parties abide by this policy and our removable media rules. Documented guidance for using removable media provides working practices for the Company that can be adopted by all users, ensuring the safe storage, use and transfer of information.

We control the use of removable media devices, to enable us to: -

- Ensure the access to information is limited and restricted dependant on its purpose and content
- Maintain the integrity of the data and protect its owner and/or source
- Prevent risks and/or security breaches through loss of assets
- Comply with regulations, laws and contractual obligations
- Provide a safe and effective workplace for employees and clients

- Maintain high standards of securing and restricting personal information.
- Prohibit the disclosure of information, both for best practice and as applicable to the data protection laws

6.4.1 Using Removable Media Devices

Unless provided to an employee directly by the Company, we prohibit the use or possession of any removable media devices on-site. Employees sign an agreement to this effect as part of their employment contact and agree to be searched entering and leaving the premises to enforce this rule. Removable media devices pose a serious risk to the information held by the Company and here there is a need for using such devices, these will be owned, controlled and provided by the Company directly.

Where an employee requires a removable media device for use internally or externally, they must request this directly with the Commercial & Operations Director. All requests must be in writing and should state: -

- The removable media device required
- The purpose of the device
- Duration needed for
- How it will be secured and protected during use
- Where the device will be used
- What assets the device will be connected to

All removable media devices and any associated equipment and software are only available through the Company's purchasing department, who will place orders and take receipt of any such devices. Where removable media is used to store important, essential or personal information, this will be done so as a backup format and is never the sole location of such data. Removable devices can become corrupt or inaccessible and there must be alternate and secure backups of all information.

For removable media devices that are needed for use outside of the Company office, please see our Remote Working Policy for use and guidelines. Strict encryption software is use don removable media devices that partition the media and enable a secure, segregated data section that is only accessible via login credentials and authentication.

The Company uses the latest virus and malware checking software on all assets to ensure that where removal media devices are being used, these are scanned are authorised prior to allowing access to any networks, systems or servers.

Whilst removable media are in transit, they are secured through internal credential authentication and external security measures. These including being in a locked container that is only accessible to the user and the use of additional encryptions during transit.

6.5 Information Classification

When the Company documents information assets on our Information Asset Register (IAR), each asset is given a classification to help describe the use, purpose, content and risk level associated with it. ***We utilise 5 main classification types: -***

1. **Unclassified** - assets not of value and/or retained for a limited period where classification is not required or necessary
2. **Public** - information that is freely obtained from the public and as such, is not classified as being personal or confidential
3. **Internal** - physical or information assets that are solely for internal use and do not process external information or permit external access
4. **Personal** - information or a system that processes information that belongs to an individual and is classed as personal under the data protection laws
5. **Confidential** - private information or systems that must be secured at the highest level and are afforded access restrictions and high user authentication

When each asset is obtained, they are added to the IAR and are assessed and classified by the owner according to their content. The classification is then used to decide what access restriction need to be applied and the level of protection afforded to the asset. The classification along with the asset type, content and description are then used to assess the risk level associated with the information and mitigating action can then be applied.

6.6 Non-Disclosure & Confidentiality Agreements

The Company uses a robust and predefined non-disclosure agreement with all employees as part of their employment contract.

6.7 Handling and Disposal

6.7.1 Disposal of Assets

How we dispose of assets is of paramount importance due to the nature of our business and services. We handle small volumes or personal data and utilise systems that retain and process such data daily. Please refer to our ***Retention & Erasure Policy*** which details how we dispose of all data, hardware, devices and records.

Reformatting of systems and hardware is our default position, however great care is always exercised when disposing of any equipment which has been used in the processing of information, as there is always a possibility that some information may remain.

7 RESPONSIBILITIES

The Company will ensure that all staff are provided with the time, training and support to learn, understand and implement the Asset Management Policy and that direct asset owners are trained and supported in their role. Asset Management at the Company is a top-down approach and every employee understands the importance of the information and assets in our possession.

7.1 Information Asset Owners (IAO)

IAO's act as the nominated owner of specific assets within the Company and are responsible for maintaining the correct information on the IAR and for documenting and understanding how the asset is used, access and of value to the company. Any process or function that affects an asset must first be authorised by the IAO.

7.1.1 Managers and Supervisors

Supervisors and managers are held responsible for ensuring that any employee who reports to them is aware of this policy and has been provided with adequate time and resources to understand its contents and meaning.

Any documented manual, handbook, policy or procedures that is related to asset management must be accessible to all employees and managers must be approachable and available should employees have questions regarding assets or their management. Line managers are also responsible for liaising with the IAO(s) to ensure that effective and adequate training is provided to new starts and existing staff on a rolling basis regarding assets, with emphasis on information assets.

DATA BREACH POLICY & PROCEDURES

5 POLICY STATEMENT

Torquay Holdings Trading as MVIS Ltd and Bartco UK Ltd *(hereinafter referred to as the **"Company"**)* are committed to our obligations under the regulatory system and in accordance with the GDPR and maintain a robust and structured program for compliance and monitoring. We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary. However, we recognise that breaches can occur, hence this policy states our intent and objectives for dealing with such incidents.

Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from any risks associated with processing data. The protection and security of the personal data that we process is of paramount importance to us and we have developed data specific protocols for any breaches relating to the GDPR and the data protection laws.

6 PURPOSE

The purpose of this policy is to provide the Company's intent, objectives and procedures regarding data breaches involving personal information. As we have obligations under the GDPR, we also have a requirement to ensure that adequate procedures, controls and measures are in place and are disseminated to all employees; ensuring that they are aware of the protocols and reporting lines for data breaches. This policy details our processes for reporting, communicating and investigating such breaches and incidents.

7 SCOPE

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

8 DATA SECURITY & BREACH REQUIREMENTS

The Company's definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Alongside our *'Privacy be Design'* approach to protecting data, we also have a legal, regulatory and business obligation to ensure that personal information is protected whilst being processed by the Company. Our technical and organisational measures are detailed in our Data Protection Policy & Procedures and Information Security Policies.

We carry out information audits to ensure that all personal data processed by us is adequately and accurately identified, assessed, classified and recorded. We carry out risk assessments that assess the scope and impact of any potential data breach; both on the processing activity and the data subject. We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risks, including *(but not limited to*): -

8.4 Pseudonymisation and encryption of personal data

8.5 Restricted access and biometric measures

8.6 Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services

8.7 Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

8.8 Audit procedures, assess, review and evaluate the effectiveness of all measures in compliance with the data protection regulations

8.9 Frequent and ongoing data protection training programs for all employees

8.10 Staff assessments and regular knowledge testing to ensure a high level of competency, knowledge and understanding of the data protection regulations and the measures we have in place to protect personal information

8.11 Reviewing internal processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal; it is rechecked and authorised by the Data Protection Officer

5.5 OBJECTIVES

5.5.1 To adhere to the GDPR and UK Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches

5.5.2 To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information

5.5.3 To utilise information audits and risk assessments for mapping data and to reduce the risk of breaches

5.5.4 To have adequate and effective risk management procedures for assessing any risks presented by processing personal information

5.5.5 To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes set out in any regulations, codes of practice or handbooks

5.5.6 To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring

5.5.7 To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected

5.5.8 To protect consumers, clients and employees; including their information and identity

5.5.9 To ensure that where applicable, the Data Control Officer is involved in and notified about all data breaches and risk issues

5.5.10 To ensure that the Supervisory Authority is notified of any data breach (*where applicable*) with immediate effect and at the latest, within 72 hours of the Company having become aware of the breach

9 DATA BREACH PROCEDURES & GUIDELINES

The Company has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below. Our documented breach incident policy aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

- ## BREACH MONITORING & REPORTING

The Company has appointed a **Data Control Officer** who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to this person with immediate effect, whereby the procedures detailed in this policy are followed.

All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to a data breach, revision to any such process is recorded in the Change Management and Document Control records.

- ## BREACH INCIDENT PROCEDURES

  - ### IDENTIFICATION OF AN INCIDENT

As soon as a data breach has been identified, it is reported to the direct line manager and the reporting **Control Officer** immediately so that breach procedures can be initiated and followed without delay.

Reporting incidents in full and with immediate effect is essential to the compliant functioning of the Company and is not about apportioning blame. These procedures are for the protection of the Company, its staff, customers, clients and third parties and are of the utmost importance for legal regulatory compliance.

As soon as an incident has been reported, measures must be taken to contain the breach. Such

measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organisation, customer, client, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident form in all cases.

- **BREACH RECORDING**

In cases of data breaches, the **Data Control Officer** is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on Entropy and making any relevant and legal notifications. The completing of the Breach on Entropy is only to be actioned after containment has been achieved.

A full investigation is conducted and recorded on Entropy, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed Entropy NCR is filed for audit and documentation purposes.

If applicable, the Supervisory Authority and the data subject(s) are notified in accordance with the GDPR requirements (*refer to section 6 of this policy*). The Supervisory Authority protocols are to be followed and their '***Security Breach Notification Form'*** should be completed and submitted. In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

- **BREACH RISK ASSESSMENT**

- **HUMAN ERROR**

Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee(s) held.

A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed in accordance with the Company's Risk Assessment Procedures. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause.

Resultant employee outcomes of such an investigation can include, but are not limited to: -

- Re-training in specific/all compliance areas
- Re-assessment of compliance knowledge and understanding
- Suspension from compliance related tasks
- Formal warning *(in-line with the Company's disciplinary procedures)*

- **SYSTEM ERROR**

Where the data breach is the result of a system error/failure, the IT team are to work in conjunction with the **Data Control Officer** to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Entropy NCR.

Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident: -

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Removing an employee from their tasks
- The use of back-ups to restore lost, damaged or stolen information
- Making the building secure
- If the incident involves any entry codes or passwords, then these codes must be changed immediately and members of staff informed

- **ASSESSMENT OF RISK AND INVESTIGATION**

The **Data Control Officer** should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

The lead investigator should look at: -

- The type of information involved
- It's sensitivity or personal content
- What protections are in place (e.*g. encryption*)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident

The appointed lead should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

10 BREACH NOTIFICATIONS

The Company recognises our obligation and duty to report data breaches in certain instances. All staff have been made aware of the Company's responsibilities and we have developed strict internal

reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay.

5.1 SUPERVISORY AUTHORITY NOTIFICATION

The Supervisory Authority is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, would lead to significant detrimental effects on the individual.

Where applicable, the Supervisory Authority is notified of the breach no later than 72 hours after the Company becoming aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the **DCO** and deemed to be ***unlikely*** to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

The notification to the Supervisory Authority will contain: -

- A description of the nature of the personal data breach
- The categories and approximate number of data subjects affected
- The categories and approximate number of personal data records concerned
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

Breach incident procedures are always followed and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Supervisory Authority if requested.

Where the Company acts in the capacity of a processor, we will ensure that controller is notified of the breach without undue delay. In instances where we act in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obligated to notify us without delay after becoming aware of a personal data breach.

5.2 DATA SUBJECT NOTIFICATION

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

The notification to the Data Subject shall include: -

- The nature of the personal data breach
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it *(i.e. encryption, data masking etc*) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

11 RECORD KEEPING

All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the **Data Control Officer** and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

12 RESPONSIBILITIES

The Company will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

The **Data Control Officer** is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.

CLEAR DESK POLICY

5 POLICY STATEMENT

As a company obligated under the Data Protection laws as well as having legal and contractual responsibilities for information security, **Torquay Holdings trading as MVIS Ltd and Bartco UK Ltd** *(hereinafter referred to as the **"Company"**)* protects and secures all forms of personal data pertaining to natural and legal persons.

It is the Company's policy to operate a clear desk approach with regards to paper and confidential materials and staff are aware that they should never leave personal or sensitive information on their desks or in any area that it may be seen or access by an unauthorised person.

6 PURPOSE

The purpose of this policy is to ensure that staff are aware of the reasons for operating a clear desk environment and to protect any personal information held or processed by the Company. The Company occasionally has external visitors to our offices, such as clients, suppliers and regulators and it is therefore important to prevent personal or confidential information from lying around unattended.

We also adhere to our Environmental Policy which restricts the printing of materials to only those that are necessary. Having a clear desk provides a professional outlook and helps to maintain a safe environment for our employees, buy reducing clutter and preventing accidents

We are committed to the protection of personal information, including that of customers, clients and employees and as such utilise electronic systems for data reading and access where possible. Due to the nature of our business, it necessary for the Company to retain some sensitive information and a large amount of personal information relating to customers. Our **Data Protection Policy & Procedures** provide exact controls and measures for securing this type of information.

7 SCOPE

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas),* and pertains to the processing of personal

information. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

8 OBJECTIVES

The Company is committed to ensuring compliance with the rules, standards and regulations as laid out by its regulating and governing bodies and our own company objectives. Having a Clear Desk Policy enables it to maintain efficiency and an effective workplace and secures the personal information that we must hold owing to the nature of our business. As a company, we have a full understanding of the requirements to protect personal information and we believe that having a clear desk environment is pivotal to this end.

7.2 The Company's objectives regarding clear desks are to: -

8.2 Improve information security and the protection of personal data

8.3 Abide by GDPR requirements and Principles

8.4 Ensure that personal and/or confidential information is locked away where there is a requirement to print it or where it has been received in a paper format

8.5 Redact paper information as far as possible when it pertains to personal information that exceeds our requirements and needs

8.6 Demonstrate an effective and efficient workplace to visitors, clients and regulators

8.7 Protect employee information and employee rights

8.8 Prevent accidents resulting from clutter and an untidy workplace

8.9 Create a stress-free, clean and tidy environment for our employees

8.10 Reduce paper use and recycle where possible

8.11 Reduce the use of toner inks for the printer

8.12 Reduce the storage space for paper information and archiving resources

9 MEASURES AND CONTROLS

Staff are continuously reminded that personal information should not be printed unless necessary, however, due to the nature of the Company's business and services, paper formats of confidential information are received on occasion. In such instances, where they are required to be on a desk for any duration of time (*i.e. for administration or data entry purposes*), ensure they lock items away before leaving their desk. Staff are aware that clear desks are in operation at all times and when leaving the office for any period of time, paper information is either locked away or destroyed.

At the end of the working day, all employees are expected to tidy their desk and to tidy away all office papers into locked desk drawers and filing cabinets. The line manager will also do an office walk round to ensure that paper data has been locked away or destroyed before leaving the office.

We have a ***Retention & Erasure*** **Policy** that outlines how paper information is destroyed and records our retention periods for all information.

It is not just personal information relating to customer or employees that are bound by the clear desk approach. All paper formats, including those used to write information down can be considered private or personal information and are subject to the same policy governance rules. Such documents can include, ***but are not limited to: -***

9.2 Telephone notes

9.3 Printed emails

9.4 Notices and minutes of meetings

9.5 Disciplinary letters

9.6 References

9.7 Accounting paperwork

9.8 Draft letters

9.9 Report and Management Information

9.10 Polices & Procedures

9.11 Corrective Action Plans

9.12 Registers and Visitor Sign-in Books

9.13 Publications

9.14 Manuals

9.15 Training Handbooks

5.1 GUIDELINES

Staff are provided with guidelines for keeping their workspace and office clean, tidy and paper free. They understand their obligations under the data protection law and do not keep personal information for longer than is necessary. The Company uses **[confidential waste bins and a secure waste disposal service/confidential shredding sacks]** where paper information is no longer required, and this is destroyed securely by a third-party supplier. Paper waiting to be shredded is secured in a locked cabinet until destruction.

Staff are afforded regular timeslots to clear their desks of unnecessary clutter such as old diaries, notebooks and filing paperwork that is no longer needed and are each provided with secure A4 lock boxes for securing personal information in paper formats that must be retained on their desk for any period or whilst they are absent from the office.

10 RESPONSIBILITIES

The Company will ensure that all staff are provided with the time, training and support to learn, understand and implement the Clear Desk Policy and subsequent or associated procedures. Management are responsible for a top down approach and in ensuring that all staff are included and have the support needed to meet the regulatory requirements in this area.

BYOD (Bring Your Own Device) & Remote Access Policy

5 INTRODUCTION

Torquay Holdings trading as MVIS Ltd and Bartco UK Ltd *(hereinafter referred to as the **"Company"**)* operates a controlled approach to remote access (*or teleworking*) and Bring Your Own Devices (BYOD) and understands that due to the nature of our business, working from outside of the office and enabling the use of personal devices within the Company is a necessity. However, we also appreciate the additional risk posed by remote access, working off-site and BYOD and as such, have documented procedures and rules that must be followed.

For the purposes of this policy, ***'remote access'*** refers to any work that takes place off-site and requires the use of any the Company information assets. This includes working from home, using the Company laptops, access to the Company network or taking personal information off-site.

Where client visits and travel are often a necessity, being able to access the Company information systems are an important part of our service, however we have strict protocols for security and restriction that apply to all employees and managers.

Bring Your Own Device (BYOD) refers to employees, clients or third parties *(collectively referred to as 'users'*), using their personally owned devices for business purposes within the Company building. This specifically refers to using a device for business use and not just having such a device on the person. Restrictions apply to personal phones, laptops and tablets, which are only permissible with prior company authorisation and in accordance with the security measures and rules of this policy.

Many of the measures and controls in effect for remote access and BYOD overlap and are covered generically in this policy, however where specific protocols are provided for either/or, they are noted as such. BYOD mainly refers to a user's own, personal device that is used within the Company building, but not externally. Remote access utilise devices provided by the Company for teleworking or working from home. This enables the Company to secure, register and monitor such devices.

6 POLICY STATEMENT

It is the Company's policy to permit remote access and BYOD where there is a genuine business need, but only with prior permission and in accordance with the rules of this policy. Security measures must be enforced, and all employees agree to the terms of this document when working off-site or bringing personal devices into the office.

Regardless of who owns the device being used or where the access happens from, the Company remains the data controller in all instances and recognises its legal obligation to abide by the data protection laws. We place a high value on the information assets within our remit and aim to protect them at all times. All users are expected to adhere to the standards in this policy and agree to keeping data and devices secure, updated and safe.

7 PURPOSE

The purpose of this policy is to outline the Company's approach, objectives and guidelines for remote access and BYOD activities. It documents acceptable devices, methods of access and reasons for using personal devices and/or remote access and places restrictions on these functions to ensure effective security for the Company, its clients and our employees, as well as protecting the personal data that we hold.

8 SCOPE

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas)*. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

The Company authorises remote access and BYOD on a case by case basis and reserves the right to refuse, prevent or withdraw access to users at any time.

9 OBJECTIVES

The Company permits the use of remote access and BYOD to better serve our clients and customers and to offer more flexibility to employees when they need to access the Company systems off-site. We also value the flexibility that using a personal device can afford, especially with reference to laptops and smartphones for visiting clients or service providers who may need to utilise their own devices or access the Company networks/wireless connections to carry out business functions.

However, due to these devices and practices needing additional security and running the risk of control being lost around their purpose and use, the Company have developed and abide by this policy to provide guidance and requirements of both functions.

7.3 *With regards to BYOD and remote access, the Company ensures that: -*

9.1 It has a robust and maintained Remote Access & BYOD Policy that is compliant and disseminated

9.2 All users are made aware of this policy and understand their responsibility and commitment to its rules

9.3 All mobile devices accessing company networks or being brought onto the Company premises must be registered

9.4 The Company reserves the right to check that any mobile devices are using up-to-date and effective firewalls, malware and anti-virus software

9.5 Where a mobile device is predominately used for the Company purposes, installing software not authorised or approved by the Company is forbidden

9.6 We utilise strong encryption and secure access connections for all remote access and mobile devices

9.7 Where a user from a remote access location or connection via a mobile device uses unrecognised credentials 3 times, their device and access will be blocked until authentication by the IT Manager

9.8 All mobile devices and remote access connections are secured with passwords and must follow the Company's strong password policy

9.9 The IT Manager can restrict access instantly and erase connections and data on a mobile device

9.10 Any information or asset belonging to a client is never accessed or used via remote access or personal devices unless express written permission has previously been obtained

5.1 BRING YOUR OWN DEVICE (BYOD) GUIDELINES & PROTOCOLS

The Company grants its employees and third-parties the privilege of using personal smartphones, laptops and tablets for their convenience, but reserve the right to revoke this privilege at any time or if users do not abide by the requirements and guidelines of this policy.

Protecting the information and assets controlled and processed by the Company is paramount to our business and promotes trust with our clients and customers. Controlling the use of BYOD enables us to maintain a secure and robust infrastructure and protects the integrity of the company.

All users must agree to the below terms to be able to use and connect their devices to the Company network. ***All users are required to: -***

5.1.1 Consider the requirement of using their own device and only do so where there is a specific business need or requirement

5.1.2 Enable and keep up to date all security features and software on the device

5.1.3 Utilise strong credentials for login authentication and adhere to our Password Policy for any changes

5.1.4 Activate the lock screen function whenever the device is left or not in use and ensure that unlock necessitates a re-login

5.1.5 Keep the device updated with operating system and software updates

5.1.6 Only use a secure The Company network connection for remote access and do so via a secure link (VPN) and only with prior authorisation

5.1.7 Activate and use encryption services and anti-virus protection on all devices

5.1.8 Turn off any camera and/or microphones

5.1.9 Refrain from carrying out any external business activities

5.1.10 Users are expected to use their devices in an ethical manner at all times and adhere to The Company's acceptable use terms

5.1.11 Remove any The Company information stored on their device once finished with, including copies of emails, attachments, downloaded documents and temporary files

5.2 REMOTE ACCESS PROTOCOLS

Employees and on occasion, clients, are required to access the Company assets and/or networks whilst off-site. Such remote access is heavily governed and controlled to prevent additional security risks and to protect the device being used, the Company network and infrastructure and the information being accessed.

Remote access is only available via a secure network and with prior approval and usually utilise devices provided by the Company (*as opposed to a user's own device*). Connection is via authentication and is setup on a restricted and limited basis by the IT Manager.

7.4 *All users via remote access are required to: -*

5.2.1 Only utilise the Company's provided devices for remote access

5.2.2 Obtain written authorisation from the Company to connect via remote access

5.2.3 Take appropriate security measures to protect the device and the information being accessed

5.2.4 Protect their device from being seen, used or copied by unauthorised individuals

5.2.5 Access the network via the authenticated network using secure connections

The Data Officer has overall responsibility for any devised used off-site and connecting to the Company network via remote access. ***The [designated person] must: -***

5.2.6 Secure the device used for remote access with a firewall, anti-virus software and

secure password login

5.2.7 Register each remote access device and log who it has been supplied to

5.2.8 Maintain control of the device and access connection at all times and be able to withdraw access immediately

5.2.9 Secure all devices when not in use through security cables, locked cabinets or in a secure, access restricted room

5.2.10 Never leave remote access devices or equipment unattended

5.2.11 Where a system requires a PIN number and a VPN *'security token'*, store both separately and restrict access to them

5.2.12 Ensure that a virtual private network (VPN) is used for all remote access connections

5.2.13 Ensure that all devices used for remote access require a username and password

5.2.14 Activate and keep updated effective anti-virus software, malware and a firewall

5.2.15 Destroy remote access devices once no longer in use, by following the ***Data Retention Policy***
protocols

5.3 OFF-SITE WORKING

It is not just BYOD and remote access that can pose an additional security risk to the Company and the information retained by us. Where employees are permitted to work from home or off-site (*e.g. on client visits or service provider audits*), this can also require taking information assets off-site, such as paperwork, reports, emails etc.

Where employees are required to take hard copy information off-site, this is required to be in a locked case during transit and to be in a secure, locked cabinet whilst at home. Hard copy information must be kept on the personal at all times if not locked aware and is not to be disclosed to any person without prior written permission and a signed non-disclosure agreement.

If the paperwork is no longer required, it must be brought back to the Company for archiving or destruction. All employees are expected to abide by this policy, its rules and guidelines.

5.3.1 USING AND SECURING BYOD AND REMOTE ACCESS

Using a personal device or using a Company device to connect via remote access pose additional security risks and as such are governed by the protocols and guidelines below. The following content refers to all forms of remote access, off-site working and use of external devices.

Secure remote access is always achieved through VPN set up by the IT Manager and approved by a manager or Director. Written permission to work off-site or bring/use a personal device on-site is always required and is retained for evidence and auditing purposes.

Where a Company device us used for remote access, this is restricted to only information that is essential for the purpose of the remote working and is configured to the minimum level required to perform the activities authorised for.

Remote devices are assigned to a sole employee are remotely wiped if the device is lost, compromised or the employ has their employment terminated (*or resigns*). Any device lost or stolen must be reported to the IT Manager within 2 hours.

10 RESPONSIBILITIES

The Company will ensure that all staff are provided with the time, training and support to learn, understand and implement the BYOD and Remote Access Policy and subsequent procedures.
Management are responsible for a top down approach and in ensuring that all staff are included and have the support needed to meet the regulatory requirements in this area.

ACCESS CONTROL & PASSWORD POLICY

•POLICY STATEMENT

It is **Torquay Holdings Limited Trading as MVIS Ltd and Bartco UK Ltd** *(hereinafter referred to as the **"Company"**)* policy to protect and secure the information and systems within our remit and we take this function very seriously. We have developed and implemented several physical, logical and procedural measures and controls to enforce our approach. We understand that it is vital to protect the systems and information held and used by us from unauthorised use or access and are fully aware of how such access can affect security, personal information and individuals. ***The types of measures and controls used by The Company are: -***

- **Physical Access Controls** ensuring the availability of systems and information is restricted to authorised persons only, thus preventing locations and information from being accessible to non-authorised individuals.
- **Logical Access Controls** utilise tools and protocols for identification, authentication and authorisation of our computer information systems (*including remote access, laptops and phone systems*). The Company's logical access controls enforce access measures to our systems, programs, processes, and information and include password protocols, user authentication methods, data and authentication credentials encryption and network, system and user-level firewalls.
- **Procedural Access Measures** include our defined policies and procedures that are followed by all staff and third parties and provide the steps for areas such as access control, information security, password protocols and clear desk measures.

•PURPOSE

The purpose of this policy is to ensure that system based and physical access to any information, location and/or system is controlled and where applicable restricted using controls and procedures that protect the associated information systems and data. The Company is committed to the security of the information and assets within our remit and enforce and stress test all access measures to ensure their functionality, effectiveness and purpose.

This Access Control & Password Policy aims to restrict access to controlled information and/or

systems to only those staff or third parties who are authorised or have written permission from the Company. Where temporary and/or partial access to information or systems is required, we follow strict protocols to only enable access to the information or for the duration required by the activity.

•SCOPE

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas)*. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

•OBJECTIVES

The Company is committed to ensuring compliance with the rules, standards and regulations as laid out by its regulating and governing bodies and confirms that it has developed and implemented the appropriate procedures, systems, controls and measures to manage and mitigate against risk.

For systems containing restricted and personal information and data, an access control matrix must be developed to record role based authorised access recorded on an individual basis. Authorisation procedures must be in place for managers to authorise all access (*including short term and temporary access*) recorded on the matrix. The access matrix must be continually updated and maintained to reflect accurate records of access.

As a company, we have a full understanding of the compliance standards that we are obligated to meet and confirm that we have in place effective and efficient tools and controls for meeting these obligations under the current regulatory system.

The Company's objectives regarding compliance are to: -

- To gain access to specific systems and information, employees follow a formal request process which are submitted in writing to the **Commercial & Operations Director.**
- Generic logons are not permitted across the Company systems, however, use of generic

accounts under 'controlled' circumstances can be permitted at the discretion of the **Commercial & Operations Director.**

- To ensure relevant company, contractual, regulatory and legislative security standards are met and adhered to, employee screening checks, including DBS and referencing are undertaken if required.
- The appropriate level of access to systems and information will be determined based on the user-level, role-based requirements and ad-hoc job functions and roles.

- If authorisation to use systems and information is granted, unique logon credentials and password will be provided to the employee, utilising the strong password controls detailed in this policy.
- Access for remote users shall be subject to authorisation by line managers via the request form to the **Commercial & Operations Director**.

•PROCEDURES, CONTROLS AND MEASURES

It is pivotal to operating our business and providing services to clients that the Company use computers, telephone systems, software, hardware devices and data storage systems. Due to the nature of our business, such systems are often used to store information and assets that are of a personal and confidential nature. It is therefore essential that we protect and secure such information and therefore access to the systems using a variety of access controls and measures.

We take a multi-tiered approach when securing systems and restricting access and detail in this policy the procedures and methods used throughout the Company. This information is disseminated to all employees and forms part of our information security program.

○ LOGICAL ACCESS CONTROL

Access to systems within the Company are governed by our tiered logical access control measures. Access to any system is classified as one of the below access levels and restrictions are implemented at the user level. Levels can be changed at the discretion of the **Commercial & Operations Director** and pending a completion of an access change form. ***Considerations for granting access is assessed based on: -***

- An employee or user's need of access to complete their job and/or task
- Duration of access
- Level of access
- Information types located on the system in questions
- Security measures in place if access is granted
- Ability to remove access at a predetermined time
- Access is decided and allocated on a case by case basis and can only be assigned by the

Commercial & Operations Director.

- **ROLE-BASED ACCESS**

Users are identified as being part of a group (*such as employee)* and their level of access is generic to all required areas. This level of access is inherited by all group members and is controlled by the **Commercial & Operations Director**. Such group access is considered necessary for each employee to enable them to carry out their job and includes access to areas such as email, printers, The Company collection system and phone system. The **Commercial & Operations Director** can authorise/assign role-based access.

- **MANAGER ACCESS**

System access is granted at a higher level for managers and Directors who can access more system areas than generic employees. Such access is deemed essential to their oversight role and enables managerial staff to carry out functions and processes that require access to personal information, secure systems or data. Manager access is not inherited by the group and only the **Commercial & Operations Director** can assign Manager Access.

- **INDIVIDUAL ACCESS**

System access is granted at the required level based on a business and/or legal requirement and is only granted to the individual(s) who require access (*i.e. if an employee is granted extended access, this is not inherited by any other role-based group member*). Individual Access is usually granted for a limited period by the **Commercial & Operations Director** and is deactivated after a

set period. Such access may include a role-based user needing access to sensitive information or restricted systems to perform a task or one-off project.

○ PASSWORDS

Passwords are a key part of the Company's protection strategy and are used throughout the company to secure information and restrict access to systems. We use a multi-tiered approach which includes passwords at user, management, device, system and network levels to ensure a thorough and encompassing approach.

Passwords afford a high level of protection to resources and data and are mandatory requirements for all employees and/or third parties who are responsible for one or more account, system or have access to any resource that requires a password.

i. PASSWORD CREATION & CHANGE

Only those authorised to access specific devices, information and systems are provided with the relevant passwords and such provisions are reviewed as part of the audit process to ensure that access is still valid and required. Employees may never share their passwords with anyone else in the company, including co-workers, managers or IT staff and unique passwords are used for all employees and access to systems and devices.

Employees are made aware that strong passwords are required for all systems and user-access and that a strict non-disclosure protocol applies to passwords. Where applicable to the system or device being used, The Company utilises software to enforce the use of strong passwords. Employees are not allowed to share or disclose any password.

Strong passwords are enforced on systems and by users and must be: -

1. More than 8 characters
2. Include letters, numbers
3. Not be easily recognisable *(i.e. no names, dates of birth, places etc*)
4. Must include upper and lowercase letters

If a password is forgotten, only the **Commercial & Operations Director or Operations Manager** can reset the passwords. Passwords that have been forgotten are changed by default and cannot be reset to use the same password. A force change of password is also affected if the user

suspects that the password has been compromised.

ii. DEFAULT PASSWORDS

It is occasionally necessary to set up default password at the Commercial & Operations Director level. This is usually only when a new system or user are being set up and a password change will be promoted from the first user use. Default passwords are changed as soon as is possible and where applicable, access to information is restricted until a strong password has been created.

Where new systems, devices or software is purchased, default passwords are immediately changed and reset to use the strong variables indicated above.

iii. PROTECTING PASSWORDS

The Company is aware that viruses, software and phishing scams can attempt to obtain passwords at a user level. Whilst Firewalls are used to secure and protect systems and software, employees are instructed to never disclose their passwords in a physical or online environment. This includes not disclosing passwords to third-parties, clients or representatives who may have a legitimate need to access a system.

Password fields are always displayed in a hash or star format (*i.e. ### or ***)* so that clear text is not present when a password is typed. This helps to prevent unauthorised access or password disclosure by copy & paste or electronic printing methods.

○ PRIVILEGED ACCOUNTS

The Company understands the extreme importance of securing and restricting access to privileged accounts. Such accounts enable direct access to our network, servers, firewalls, routers, database servers, systems and software and as such are treated with the utmost security and protection.
Employees and third parties are never given access to privileged accounts, unless they have been assigned responsibility for a direct function. If this the case, access is only given to the exact system or infrastructure required to complete their take.

○ AUTHORISED ACCESS

The Company keeps an Access Register and details which employees or third parties have access to which systems and information. The register also notes when the access was given, when it will

be restricted (*if temporary access*), the type of data or system being accessed and the reason for access.

- **LOGIN CONTROLS**

Systems can only be accessed by secure authentication of user validation, which consists of a username and password at the role-based user level. All staff are aware that if they leave their workstation, their system is to be locked. All computers are closed- down at the end of the day and are not allowed to be left running out of business hours.

- **CREDENTIALS & ROLES**

Access to any systems within the Company (*including sending email*), utilises authentication based on the valid credentials being used. Each user is assigned unique credentials and are not allowed to share or disclose them to any other employee or third-party. It is necessary for credentials to be stored so that when they are used to access a system, database or send an email, the authentication process works. All authentication credentials are encrypted when stored and transmitted and access is restricted to the **Commercial & Operations Director.**

As the Company is an SME, many roles are carried out by the Commercial & Operations Director or validated staff, which means that having separate roles for areas such as authorised access or setting up accounts is not always possible. However, all requests for access are verified by the **Commercial & Operations Director** and employees are never allowed to set up their own access, disclose credentials or bypass validations. An access request form is completed for all individual access requirements and is verified by the **Commercial & Operations Director** before being authorised.

- **PHYSICAL ACCESS CONTROLS**

Access to the Company building, office sections and secure rooms are protected by our building access controls. These increase building, information and employee security and safety and ensure that no unauthorised access is possible.

- **OUTSIDE OPENING HOURS**

When the building has been vacated at the end of working hours, the alarm system is activated and secures all windows and doors. The building is *'locked down'* after **17:30** and any alarm trigger will immediately notify the Security Services who have a contact tree.

- **DIRECT ACCESS**

The use of keys to any buildings, rooms, secure cabinets, safes etc are always controlled and recorded and keys are only provided to employees who require them for business and/or legal reasons. When not in use, keys are stored in a secure, locked cabinet and only the **designated person/Commercial & Operations Director/Managers** have access. Locations of keys are known at all times and if there is any suspicion that a key has been lost or compromised, lock and access points are changed immediately and monitored until the change is affected.

Visitors are not permitted to access server, network or confidential information areas without prior authorisation. Where authorisation has been given, visits are always escorted by a **manager** or the **designated person.**

- **LEAVERS & END OF CONTRACT**

As the Company is a small company, monitoring end of contracts with third parties and identifying employees who are leaving is straightforward. We operate an immediate deactivation process of any credentials and access rights on termination and reactivation is only possible via a written request to the **Commercial & Operations Director** for authorisation.

Leavers are required to turn in all company keys before exiting the building.

Where a project or service contract ends, any access or credentials provided during the contract are deactivated and any keys are returned and signed back into the logbook.

•RESPONSIBILITIES

The **Commercial & Operations Director and Operations Manager** is responsible for ensuring that all staff and managers are aware of security policies, including access control and secure passwords and the Company operates a top-down approach. Managers need to be aware they have a responsibility to ensure staff have sufficient, relevant knowledge concerning the security of information and systems and new starters and existing staff training workshops are run on an annual basis covering the access control and password policies and objectives.

SUBJECT ACCESS REQUEST PROCEDURES

8 INTRODUCTION

This procedure document supplements the subject access request (SAR) provisions set out in **Torquay Holdings Limited Trading as MVIS Ltd and Bartco UK Ltd** *(hereinafter referred to as the **"Company"**)* Data Protection Policy & Procedures and provides the process for individuals to use when making an access request, along with the protocols followed by the Company when such a request is received.

The Company needs to collect personal information to effectively and compliantly carry out our everyday business functions and services and in some circumstances, to comply with the requirements of the law and/or regulations.

As the Company processes personal information regarding individuals (*data subjects*), we are obligated under the General Data Protection Regulation (GDPR) and Data Protection Bill to protect such information, and to obtain, use, process, store and destroy it, only in compliance with the GDPR and its principles.

8.1 The General Data Protection Regulation

The General Data Protection Regulation (GDPR) gives individuals the right to know what information is held about them, to access this information and to exercise other rights, including the rectification of inaccurate data. The GDPR is a standardised regulatory framework which ensures that personal information is obtained, handled and disposed of properly.

As the Company are obligated under the GDPR and UK data protection laws, we abide by the Regulations' principles, ***which ensure that personal information shall be: -***

- processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ***('purpose limitation')***
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ***('storage limitation')***
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality').***

The Regulation also requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the GDPR principles'* ***('accountability')***. The Company have adequate and effective

measures, controls and procedures in place, that protect and secure your personal information and guarantee that it is only ever obtained, processed and disclosed in accordance with the relevant data protection laws and regulations.

9 What is Personal Information?

Information protected under the GDPR is known as "personal data" and is defined as: -

"Any information relating to an identified or identifiable natural person; 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."

Further information on what constitutes personal information and your rights under the data protection regulation and laws can be found on the Information Commissioners Office (ICO) **website**.

10 The Right of Access

Under Article 15 of the GDPR, an individual has the right to obtain from the controller, confirmation as to whether personal data concerning them is being processed. We are committed to upholding the rights of individuals and have dedicated processes in place for providing access to personal information. ***Where requested, we will provide the following information: -***

- the purposes of the processing
- the categories of personal data concerned
- the recipient(s) or categories of recipient(s) to whom the personal data have been or will be disclosed
- If the data has been transferred to a third country or international organisation(s) (*and if applicable, the appropriate safeguards used)*
- the envisaged period for which the personal data will be stored (*or the criteria used to determine that period)*
- where the personal data was not collected directly from the individual, any available information as to its source

10.1 How to Make a Subject Access Request (SAR)?

A subject access request (SAR) is a request for access to the personal information that the Company holds about you, which we are required to provide under the GDPR *(unless an exemption applies*). The information that we provide is covered in section 3 of this document.

You can make this request in writing using the details provided in section 7, or you can submit your access request electronically. Where a request is received by electronic means, we will provide the requested information in a commonly used electronic form *(unless otherwise requested by the data subject).*

10.2 What We Do When We Receive an Access Request

Identity Verification

Subject Access Requests (SAR) are passed to the **[Data Protection Officer/Compliance Officer]** as soon as received and a record of the request is made. The person in charge will use all reasonable measures to verify the identity of the individual making the access request, especially where the request is made using online services.

We will utilise the request information to ensure that we can verify your identity and where we are unable to do so, we may contact you for further information, or ask you to provide evidence of your identity prior to actioning any request. This is to protect your information and rights.

If a third party, relative or representative is requesting the information on your behalf, we will verify their authority to act for you and again, may contact you to confirm their identity and gain your authorisation prior to actioning the any request.

Information Gathering

If you have provided enough information in your SAR to collate the personal information held about you, we will gather all documents relating to you and ensure that the information required is provided in an acceptable format. If we do not have enough information to locate your records, we may contact you for further details. This will be done as soon as possible and within the timeframes set out below.

Information Provision

Once we have collated all the personal information held about you, we will send this to you in writing (*or in a commonly used electronic form if requested*). The information will be in a concise, transparent, intelligible and easily accessible format, using clear and plain language.

11 Fees and Timeframes

We aim to complete all access requests within 30-days and provide the information free of charge. Where the request is made by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

Whilst we provide the information requested without a fee, further copies requested by the individual may incur a charge to cover our administrative costs.

The Company always aim to provide the requested information at the earliest convenience, but at a maximum, 30 days from the date the request is received. However, where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months. If this is the case, we will write to you within 30 days and keep you informed of the delay and provide the reasons.

12 Your Other Rights

Under the GDPR, you have the right to request rectification of any inaccurate data held by us. Where we are notified of inaccurate data, and agree that the data is incorrect, we will amend the details immediately as directed by you and make a note on the system *(or record)* of the change and reason(s).

We will rectify any errors within 30-days and inform you in writing of the correction and where applicable, provide the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or data completion, we will always provide a written explanation to you and inform you of your right to complain to the Supervisory Authority and to seek a judicial remedy.

In certain circumstances, you may also have the right to request from the Company, the erasure of personal data or to restrict the processing of personal data where it concerns your personal information; as well as the right to object to such processing. You can use the contact details in section 7 to make such requests.

13 Exemptions and Refusals

The GDPR contains certain exemptions from the provision of personal information. If one or more of these exemptions applies to your subject access request or where the Company does not act upon

the request, we shall inform you at the earliest convenience, or at the latest, within one month of receipt of the request.

Where possible, we will provide you with the reasons for not acting and any possibility of lodging a complaint with the Supervisory Authority and your right to seek a judicial remedy. Details of how to contact the Supervisory Authority are laid out in section 7 of this document.

14 Submission & Lodging a Complaint

To submit your SAR, you can contact us at **anne@m-vis.co.uk**. You can also submit your request in writing using the ***form in Appendix 1***, sending the request to: -

Anne Ashman or Dominic Bridge

MVIS ltd or Bartco UK Limited

Units 6-8 Brookfield Way

Tansley

Matlock

DE4 5ND

01629 580570

14.1 Supervisory Authority

If you remain dissatisfied with our actions, you have the right to lodge a complaint with the Supervisory Authority. ***The Information Commissioner's Office (ICO) can be contacted at: -***

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Telephone: 0303 123 1113 *(local rate)* or 01625 545 745 *(national rate)*

Fax: 01625 524 510 Email: enquiries@ico.org.uk

Subject Access Request Form

Under the General Data Protection Regulation, you are entitled as a data subject to obtain from the Company, confirmation as to whether we are processing personal data concerning you, as well as to request details about the purposes, categories and disclosure of such data.

You can use this form to request information about, and access to any personal data we hold about you. Details on where to return the completed form can be found at the end of the document.

1. Personal Details:			
Data Subject's Name:		**DOB:**	___ / ___ / _____
Home Telephone No:		**Email:**	
Data Subject's Address:			
Any other information that may help us to locate your personal data:			
2. Specific Details of the Information Requested:			
3. Representatives *(only complete if you are acting as the representative for a data subject)* ***[Please Note:*** *We may still need to contact the data subject where proof of authorisation or identity are required]*			
Representative's Name:		**Relationship to Data Subject:**	

Telephone No:		**Email:**	
Representative's Address:			
I confirm that I am the authorised representative of the named data subject: **Representative's Name:** _____ **Signature:** _____			
4. Confirmation			
Data Subject's Name: _____ [print name] **Signature:** _____ **Date:** ____ /____ /_____			
5. Completed Forms			
For postal requests, please return this form to: **Anne Ashman or Dominic Bridge** **MVIS ltd or Bartco UK Limited** **Units 6-8 Brookfield Way** **Tansley** **Matlock** **DE4 5ND** ***For email requests, please return this form to***: anne@m-vis.co.uk			

DATA RETENTION & ERASURE POLICY

15 POLICY STATEMENT

Torquay Holdings Limited Trading as MVIS Ltd and Bartco UK Ltd (*hereinafter referred to as the **"Company"**)* recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the organisation.

This policy and related documents meet the standards and expectations set out by contractual and legal requirements and has been developed to meet the best practices of business records management, with the aim of ensuring a structured approach to document control.

Effective and adequate records and data management is necessary to: -

- Ensure that the business conducts itself in a structured, efficient and accountable manner
- Ensure that the business realises best value through improvements in the quality and flow of information and greater coordination of records and storage systems
- Support core business functions and provide evidence of conduct and the appropriate maintenance of systems, tools, resources and processes
- Meet legislative, statutory and regulatory requirements
- Deliver services to, and protect the interests of, employees, clients and stakeholders in a consistent and equitable manner
- Assist in document policy formation and managerial decision making
- Provide continuity in the event of a disaster or security breach
- Protection personal information and data subject rights
- Avoid inaccurate or misleading data and minimise risks to personal information

- Erase data in accordance with the legislative and regulatory requirements

Information held for longer than is necessary carries additional risk and cost and can breach data protection rules and principles. The Company only ever retains records and information for legitimate or legal business reasons and always comply fully with the data protection laws, guidance and best practice.

16 Purpose

The purpose of this document is to provide the Company's statement of intent on how it provides a structured and compliant data and records management system. We define ***'records'*** as all documents, regardless of the format; which facilitate business activities, and are thereafter retained to provide evidence of transactions and functions.

Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

17 Scope

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

18 Personal Information and Data Protection

The Company needs to collect personal information about the people we employ, work with, have a business relationship with, to effectively and compliantly carry out our everyday business functions and activities, and to provide the products and services defined by our business type. This information can include *(but is not limited to),* name, address, email address, data of birth, IP address, identification number, private and confidential information, sensitive information and bank details.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the ***General Data***

Protection Regulation, UK data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

Our Data Retention Policy and processes comply fully with the GDPR's fifth Article 5 principle: -

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation').***

19 OBJECTIVES

A record is information, regardless of media, created, received, and maintained which evidences the development of, and compliance with, regulatory requirements, business practices, legal policies, financial transactions, administrative activities, business decisions or agreed actions. It is the Company's objective to implement the necessary records management procedures and systems which assess and manage the following processes: -

- The creation and capture of records
- Compliance with legal, regulatory and contractual requirements
- The storage of records
- The protection of record integrity and authenticity
- The use of records and the information contained therein
- The security of records
- Access to and disposal of records

Records contain information that are a unique and invaluable resource to the Company and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information contained in them, as well as the individuals such information refers to. Records are also pivotal in the documentation and evidence of all business functions and activities.

The Company's objectives and principles in relation to Data Retention are to: -

- Ensure that the Company conducts itself in an orderly, efficient and accountable manner
- Support core business functions and providing evidence of compliant retention, erasure and destruction
- To develop and maintain an effective and adequate records management program to ensure effective archiving, review and destruction of information
- To only retain personal information for as long as is necessary
- Comply with the relevant data protection regulation, legislation and any contractual obligations
- Ensure the safe and secure disposal of confidential data and information assets
- Ensure that records and documents are retained for the legal, contractual and regulatory period stated in accordance with each bodies rules or terms.
- Ensure that no document is retained for longer than is legally or contractually allowed
- Mitigate against risks or breaches in relation to confidential information

20 GUIDELINES & PROCEDURES

The Company manage records efficiently and systematically, in a manner consistent with the GDPR requirements and regulatory Codes of Practice on Records Management. Records management training is mandatory for all staff as part of the Company's statutory and compliance training programme and this policy is widely disseminated to ensure a standardised approach to data retention and records management.

Records will be created, maintained and retained to provide information about, and evidence of the Company's transactions, customers, employment and activities. Retention schedules will govern the period that records will be retained and can be found in the ***Record Retention Periods*** table at the end of this document.

It is our intention to ensure that all records and the information contained therein is: -

1. **Accurate** - records are always reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document

2. **Accessible** - records are always made available and accessible when required (*with additional security permissions for select staff where applicable to the document content*)

3. **Complete** - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document

4. **Compliant** - records always comply with any record keeping legal and regulatory requirements

5. **Monitored** – staff, company and system compliance with this Data Retention Policy is regularly monitored to ensure that the objectives and principles are being complied with at all times and that all legal and regulatory requirements are being adhered to.

20.1 Retention Period Protocols

All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All company and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines.

For all data and records obtained, used and stored within the Company, we: -

1. Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain
2. Establish periodical reviews of data retained
3. Establish and verify retention periods for the data, with special consideration given in the below areas: -

1. the requirements of the Company
2. the type of personal data
3. the purpose of processing
4. lawful basis for processing
5. the categories of data subjects

4. Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, the Company will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices
5. Have processes in place to ensure that records pending audit, litigation or investigation are not destroyed or altered

6. Transfer paper based records and data to an alternative media format in instances of long retention periods (*with the lifespan of the media and the ability to migrate data where necessary always being considered*)

20.2 Designated Owners

All systems and records have designated owners (IAO) throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Owners are assigned based on role, business area and level of access to the data required. The designated owner is recorded on the Retention Register and is fully accessible to all employees. Data and records are never reviewed, removed, accessed or destroyed with the prior authorisation and knowledge of the designated owner.

20.3 Document Classification

The Company have detailed Asset Management protocols for identifying, classifying, managing, recording and coordinating the Company's assets (*including information*) to ensure their security and the continued protection of any confidential data they store or give access to. We utilise an ***Information Asset Register (IAR)*** to document and categorise the assets under our remit and carry out regular Information Audits to identify, review and document all flows of data within the Company.

We also carry out regular Information Audits which enable us to identify, categorise and record all personal information obtained, processed and shared by our company in our capacity as a controller and processor and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Retention periods
- Access level (*i.e. full, partial, restricted etc*)

Our information audits and registers enable us to assign classifications to all records and data, thus ensuring that we are aware of the purpose, risks, regulations and requirements for all data types.

We utilise 5 main classification types: -

6. **Unclassified** - information not of value and/or retained for a limited period where classification is not required or necessary
7. **Public** - information that is freely obtained from the public and as such, is not classified as being personal or confidential
8. **Internal** - information that is solely for internal use and does not process external information or permit external access
9. **Personal** - information or a system that processes information that belongs to an individual and is classed as personal under the data protection laws
10. **Confidential** - private information or systems that must be secured at the highest level and are afforded access restrictions and high user authentication

The classification is used to decide what access restriction needs to be applied and the level of protection afforded to the record or data. The classification along with the asset type, content and description are then used to assess the risk level associated with the information and mitigating action can then be applied.

20.4 Suspension of Record Disposal for Litigation or Claims

If the Company is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against our firm, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

20.5 Storage & Access of Records and Data

Documents are grouped together by category when stored and/or archived. Documents are always retained in a secure location, with authorised personnel being the only ones to have access. Once the retention period has elapsed, the documents are either reviewed, archived or confidentially destroyed dependant on their purpose, classification and action type.

21 Expiration of Retention Period

Once a record or data has reached its designated retention period date, the designated owner should refer to the retention register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymise the data in accordance with the GDPR requirements or to archive records for a further period.

21.1 Destruction and Disposal Of Records & Data

All information of a confidential or sensitive nature on paper, card, microfiche or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, clients and customers.

The Company is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

21.1.1 Paper Records

Due to the nature of our business, the Company may retain paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner. The Company utilise Data Shred (**A Professional Shredding Service Provider)** to dispose of all paper materials.

Confidential waste sacks are made available throughout the building and where we use a service provider for large disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

All home working staff do not have paper records, any that do must return them to the office and placed in the bins to be securely shredded.

21.1.2 Electronic & IT Records and Systems

The Company uses numerous systems, computers and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active, this disposal is handled in an ethical and secure manner.

The deletion of electronic records must be organised in conjunction with Resolve (IT Company) who will ensure the removal of all data from the medium so that it cannot be reconstructed. When records or data files are identified for disposal, their details must be provided to the designated owner to maintain an effective and up to date a register of destroyed records.

Only the Commercial & Operations Director can authorise the disposal of any IT equipment and must accept and authorise such assets from the department personally. Where possible, information is wiped from the equipment through use of software and formatting, however this can still leave

imprints or personal information that is accessible and so we also comply with the secure disposal of all assets.

In all disposal instances, a disposal form must be completed and confirm successful deletion and destruction of each asset. This must also include a valid certificate of disposal from the service provider removing the formatted or shredded asset. Once disposal has occurred, the purchasing Department is responsible for liaising with the information Asset Owner and updating the Information Asset Register for the asset that has been removed.

It is the explicit responsibility of the asset owner and Commercial & Operations Director to ensure that all relevant data has been sufficiently removed from the IT device and backed up before requesting disposal and/or prior to the scheduled pickup.

21.1.3 Internal Correspondence and General Memoranda

Unless otherwise stated in this policy or the retention periods register, correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support *(i.e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed*).

Where correspondence or memoranda that do not pertain to any documents having already be assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content ceases or at a maximum, 2 years.

Examples of correspondence and routine memoranda include (but are not limited to): -

1. Internal emails
2. Meeting notes and agendas
3. General inquiries and replies
4. Letter, notes or emails of inconsequential subject matter

22 ERASURE

In specific circumstances, data subjects' have the right to request that their personal data is erased, however the Company recognise that this is not an absolute *'right to be forgotten'*. Data subjects only have a right to have personal data erased and to prevent processing if one of the *below conditions applies: -*

1. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
2. When the individual withdraws consent
3. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
4. The personal data was unlawfully processed
5. The personal data must be erased in order to comply with a legal obligation

Where one of the above conditions applies and the Company received a request to erase data, we first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, this is carried out by the Data Control Officer in conjunction with any department manager to ensure that all data relating to that individual has been erased.

These measures enable us to comply with a data subjects right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed: -

1. The request is allocated to the Data Control Officer and recorded on the Erasure Request Register
2. The DCO locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -

1. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
2. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
3. the data subject objects to the processing and there are no overriding legitimate grounds for the processing

4. the personal data has been unlawfully processed
5. the personal data must be erased for compliance with a legal obligation

4. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
5. The DCO writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
6. Where the Company has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. ***Such refusals to erase data include: -***

1. Exercising the right of freedom of expression and information
2. Compliance with a legal obligation for the performance of a task carried out in the public interest
3. For reasons of public interest in the area of public health
4. For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
5. For the establishment, exercise or defence of legal claims

22.1 Special Category Data

In accordance with GDPR requirements and Schedule 1 Part 4 of The Data Protection Bill, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data and criminal convictions etc.

Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, as noted on our retention register schedule.

23 Compliance and Monitoring

The Company are committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving and retention. Information asset owners are tasked with ensuring the continued compliance and review of records and data within their remit.

24 Responsibilities

Heads of departments and information asset owners have overall responsibility for the management of records and data generated by their departments' activities, namely to ensure that the records created, received and controlled within the purview of their department, and the systems (*electronic or otherwise*) and procedures they adopt, are managed in a way which meets the aims of this policy.

Where a DCO has been designated, they must be involved in any data retention processes and records or all archiving and destructions must be retained. Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with the Company's protocols.

25 Retention Periods

Section 12 of this policy contains our regulatory, statutory and business retention periods and the subsequent actions upon reaching those dates. Where no defined or legal period exists for a record, the default standard retention period is 6 years plus the current year (*referred to as 6 years + 1*).

RECORD	RETENTION PERIOD	ASSET OFFICER	ACTION	NOTES
Information, data or record	*Period for retaining record & accompanying notes*	*Who is responsible for reviewing periods*	*Destroy, archive, review etc*	
One year				
CV's/ Application forms and interview notes (*for unsuccessful candidates)*	1 year from date of interview	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	
Memberships, certification and/or accreditation with professional associations	End of membership/accreditation + 1 year	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	
Two Years				
Immigration Checks	2 years from termination of employment	*Anne Ashman - COD*	Data shred to destroy/electronic copy to be deleted	
Marketing, promotion, press releases	2 years after last action	*Sean Brown - MM*	Data shred to destroy/electronic copy to be deleted	
Annual Leave	2 years from date made	*Anne Ashman - COD*	Data shred to destroy/electronic copy to be deleted	BrightHr updates automatically

Working Time Records	2 years from date made	*Anne Ashman – COD/Dom Bridge - OM*	Data shred to destroy/electronic copy to be deleted	Sage timesheets automatically updates
Three Years				
Accident books, accident records/reports	3 years from last entry	*Anne Ashman – COD*	Data shred to destroy/electronic copy to be deleted	
Accounting & Tax records	3 years for private companies	*Anne Ashman COD*	Data shred to destroy/electronic copy to be deleted	
Income tax and NI returns Income tax records IR correspondence	At least 3 years after the end of the financial year to which they relate	*Mitchells Accountants/Anne Ashman COD*	Data shred to destroy/electronic copy to be deleted	
Paternity, shared leave, paternity leave, adoption	3 years from the end of the tax year	*Anne*	Data shred to destroy/electronic copy to be deleted	
Statutory Maternity Pay records, calculations, certificates & related medical evidence	3 years after the end of the tax year in which the maternity period ends	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	

PAYE & NI	3 years from the end of the tax year	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	
National minimum wage records	3 years + current year after the end of the pay reference period	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	Electronically held on Sage
HMRC correspondence	3 years from the related tax year	*Anne/Accountant*	Data shred to destroy/electronic copy to be deleted	
Four years or over				
Complaints, records, letters, responses & customer communications received by an FCA regulated firm	5 years for complaints relating to MiFID business or collective portfolio management services	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	
Records documenting the firm's relationships and responsibilities to statutory and/or regulatory bodies and its legal responsibilities	Permanent	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	
Business documents, policies, procedures, strategies etc	Superseded + 6 years *(then reviewed for archive value purposes)*	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	

Supplier, business relationship documents, contracts, SLA's, audits, reviews etc	End of relationship + 6 years	*Dom Bridge*	Data shred to destroy/electronic copy to be deleted	
Reviews, analysis, compliance monitoring, quality assurance, operational performance etc	5 years +1	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	
Records of tests & examinations of control systems and protective equipment under COSHH	5 years from the date of the test	*Tom Hooton*	Data shred to destroy/electronic copy to be deleted	
Wage/salary records, overtime, bonus & expenses	6 years	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	Electronically held on Sage
Personnel files and training records (including recruitment, disciplinary records and working time records)	6 years after date employment ceases	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	
Redundancy details, calculations of payments & refunds	6 years from the date of redundancy	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	
Statutory Sick Pay records, calculations, certificates & self-certificates	6 years	*Anne Ashman*	Data shred to destroy/electronic copy to be deleted	

Tax returns, annual & quarterly	6 years from end of last company financial year	*Mitchells*	Data shred to destroy/electronic copy to be deleted	