HYDENLYNE
GLOBAL E&P SERVICES

Information Protection Policy

1. Introduction

This information security policy outlines the measures Hydenlyne has in place to ensure the security of all information provided to Hydenlyne and used within Hydenlyne as a company.

Hydenlyne is an E&P consultancy that provides consultants covering a range of skills to the offshore oil and gas industry. Hydenlyne works with a large number of Oil companies and Seismic companies. Hydenlyne ensures that all information gained from our clients and consultants is kept confidential. Hydenlyne is bound by the various applicable Privacy Acts worldwide and the privacy principles set out in them.

'Personal Information' is information or an opinion (whether true or not and whether recorded in material form or not) about an identified individual, or an individual who is reasonably identifiable.

This privacy policy outlines how Hydenlyne manages Personal Information, including the type of information, how it is collected and held, the purposes for which it is collected, held, used and disclosed and as well as how individuals can access their information and make enquiries, notifications or complaints about breaches of the legislation or privacy principles. Hydenlyne deals with Personal Information in accordance with the applicable legislation and this policy.

2. Objectives, Aim and Scope

2.1 Objectives

The objectives of Hydenlynes Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

2.2 Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information and information systems owned or held by Hydenlyne by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in

the organization.

- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organization a level of awareness of the need for Information Security as an integral part of the day to day business.

2.3 Scope

This policy applies to all information gained by Hydenlyne, its employees and its consultants, and all information kept within Hydenlynes information systems.

3. Responsibilities for Information Security

3.1 Ultimate responsibility for information security rests with the Managing Director of Hydenlyne, but on a day-to-day basis the line manager within the business shall be responsible for managing and implementing the policy and related procedures.

3.2 Line managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:-

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

3.3 All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

3.4 The Information Security Policy shall be maintained, reviewed and updated on an annual basis.

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

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

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

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

4. Legislation

4.1 Hydenlyne is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees of Hydenlyne who may be held personally accountable for any breaches of information security for which they may be held responsible. Hydenlyne shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The **General Data Protection Regulation** (GDPR) (EU) 2016/679

5. Policy Framework

5.1 Types of Personal Information

Hydenlyne collects Personal Information about individuals, e.g. candidates for employment and employees, clients and prospective clients, consultants, subcontractors, suppliers and industry participants.

This can include things such as name, address, telephone number, email address, date of birth, age, gender, marital status, banking details, driver's licence and other occupational licence details, passport number and/or passport copies, tax file number, information about financial status, credit history and insurances, proof of the right to work in certain countries, resumes, qualifications, next of kin, employment history, references and use of Hydenlyne services.

We aim to collect this information only as reasonably necessary to assist candidates to find employment, to provide proposals and services to our clients and candidates, to understand and forecast our business and to respond to requests for information.

5.2 How we collect and hold Personal Information

We will generally collect Personal Information directly from you, if you choose to provide this Personal Information to us via email. We will only collect Sensitive Information about you with your written consent and if authorised by law. By providing us with Personal and Sensitive Information, you consent to our collection and use of it for the purposes set out in this policy.

'Sensitive Information' is a sub-set of Personal Information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information, genetic information that is not otherwise health information, biometric information that is to be used for the purpose

of automated biometric verification or biometric identification or biometric templates.

Hydenlyne takes reasonable steps to hold Personal Information using appropriate physical and/or electronic security technology, settings and applications and by training staff who deal with Personal Information on our policies and procedures. These measures are designed to protect Personal Information from unauthorised access, modification or disclosure; and from misuse, interference and loss. Notwithstanding this, you should be mindful that the internet is generally not a secure environment.

5.3 Purposes for which Personal Information is collected, held, used and disclosed

Hydenlyne will only use Personal Information for the primary purpose for which we collect it, or a secondary purpose related to the primary purpose for which you would reasonably expect us to use the collected information.

We will not use your information for an unrelated secondary purpose unless we obtain your written consent and an exception applies (e.g. it is authorised by law; or it is impracticable to obtain your consent and we believe it is necessary to lessen a serious threat to the life, health or safety of any individual).

Some examples of the purposes for which we collect, hold and use Personal Information are to conduct business with or provide services (including providing your details to clients and to prospective employers if you are an applicant for employment or job placement) and otherwise administer clients' accounts, including responding to audit requests by clients, market or otherwise promote our services, disclose health information to health professionals in a medical emergency, record details of incidents for insurance purposes, contact family if requested or needed, improve our services through audits, surveys etc., obtain professional advice and comply with our obligations under applicable laws.

We may disclose Personal Information to third parties, such as professional advisers, courts, tribunals, regulatory authorities, other companies and individuals for the purposes such as complying with our obligations under contract or as required by law, having services performed such as delivering packages, addressing warranty claims, sending correspondence, obtaining searches from public records and processing payments and recovering unpaid debts. We may also disclose your information to our business associates, auditors, and financial services, IT or insurance providers, for them to provide or offer services to you. We will not authorise third parties to use your Personal Information for any other purpose. If we disclose your Personal Information to third parties, and where applicable under the applicable country-specific Privacy Act, we will make sure to enter into a processing agreement with such third parties, in order to protect the Personal Information we share with them.

5.4 Access to and correction of Personal Information

You are entitled at any time, upon request and subject to any exception under the applicable

country-specific Privacy Act and privacy principles to access your Personal Information held by us. We will respond within a reasonable time after the request is made and give access to the information in the manner requested by you, unless it is impracticable to do so. We will not disclose commercially sensitive information to you.

If any of the information we have about you is inaccurate, out-of-date, irrelevant, incomplete or misleading, or you request we correct any information, we will take reasonable steps to ensure the information held by us is accurate, up-to-date, complete, relevant and not misleading. If you request, we will notify the correction to recipients to whom we have disclosed the information, unless it is impractical or unlawful. If we refuse your request, we will explain the reasons for refusal and advise on the mechanisms to complain.

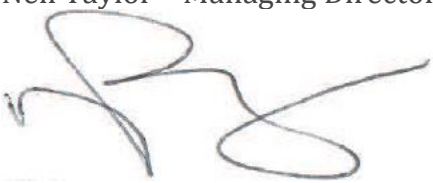
5.5 Data Leak procedure

Everyone is entitled to respect for and protection of their privacy and careful handling of their or personal data. This means that companies and governments must protect the personal data they process against loss and unlawful processing. If a data breach takes place regardless, Hydenlyne will report this to the relevant Data Protection Authority if the data breach leads to a considerable likelihood of serious adverse effects on the protection of personal data, or if the data breach has serious adverse effects on the protection of personal data. The data breach will also be reported to the data subjects if it is likely to adversely affect their privacy.

.

6. Policy approved by:

Neil Taylor – Managing Director



Date: 21/05/2018