PENTACOM INVESTMENTS SPAIN OPCO, S.L.U.

RISK MANAGEMENT FRAMEWORK

Date: December 2025

Version: 5.0

This document has been prepared for the use of PENTACOM INVESTMENTS SPAIN OPCO, S.L.U.

Risk Management Framework	
Date of issue:	December 10th, 2025
Date of approval:	December 10th, 2025
Responsible for editing and revision:	Juan María Gárate
Responsible for implementation:	Juan María Gárate
Distribution:	Open
Available languages:	English

Record of Revisions to the Risk Management Framework
The different revisions of this document will be recorded in the attached table, including the number and date of revision, the modifications carried out and the persons responsible for their review and approval.

Version	Date	Modifications	Reviewed By	Approved By
V 5.0	December 10th		Juan María Gárate	Board of Directors

Table of contents

1.0 INTRODUCTION

This document ("the Risk Management Framework") summarizes the risk management framework of PENTACOM INVESTMENTS SPAIN OPCO, S.L.U ("the Company").

The Company engages in the provision of fiber-to-the-home ("FTTH") connectivity to telecommunications operators in Spain.

This Risk Management Framework provides the Company's key policies and controls, including how these should be complied with by the employees of the Company when undertaking any activity on its behalf. This Risk Management Framework shall complement and not supersede the different processes and the Delegation of Authority approved by The Company's Board of Directors ("the Board") which may from time to time be updated.

This Risk Management Framework will be reviewed annually by the Board. The Board will also be obliged to confirm on an annual basis that the Risk Management Framework is being complied with, or to ascertain what remedial actions are required if there have been any breaches. When applicable, breaches of the Risk Management Framework, incidents, and areas of concern should be discussed at the next Board meeting.

The Risk Management Framework defines the Company's approach to operating in an ethical and considerate manner in relation to each policy theme.

The Company will ensure that all staff working for the Company are aware of the requirements under this Risk Management Framework.

The Risk Management Framework is also part of the Company's criminal compliance management system, implemented by Company to complay with article 31 bis of Spanish Criminal Code.

2.0 CODE OF ETHICS

The Code of Ethics and associated policies in this Risk Management Framework seek to define the Company's, and its employees, conduct during the course of its day-to-day activities.

The Company is committed to ensure compliance with regulatory requirements and legal frameworks in all the countries in which the Company operates. We are open and cooperative with our regulators.

The Company operates several internal policies to ensure that it is conducting business in an ethical and transparent manner.

Acting with integrity is a higher standard. It requires us to think about every action we take – before we take it – to ensure we are acting in the interests of our customers and clients and doing the right thing. The Company seeks to maintain the highest standards of propriety and professionalism and avoid being exposed to the suspicion of improper acts or compromising situations of a financial nature including receipt of extravagant hospitality.

The below policies are provided in this Risk Management Framework document and cover our ethical practices in these areas. The Code of Ethics should be read and adopted in conjunction with these policies.

- Anti-bribery and corruption policy
- Anti-Fraud policy
- Legal Matters policy
- Work, Health, Safety and Environment policy
- Human Rights policy
- Whistle-blower and grievance procedure
- Data protection policy
- Cyber security policy

The Board is assigned to implement the Risk Management Framework, monitoring compliance with it and ensuring that systems and procedure are effective and that it is not violated.

The Company responds promptly to questions, including providing relevant documentation and attending interviews. We will also adhere to all general notifications and the notification of breaches and disciplinary action requirements, including relevant breaches of our Risk Management Framework.

We (the employees of the Company) all have a responsibility to be aware of the requirements that apply to our roles, to comply with them and to seek advice if we are in any doubt.

The Company will also ensure employees feels comfortable to speak their mind, particularly with any policy concerns or breaches. Managers have a responsibility to create an open and supportive environment where employees feel comfortable raising such questions.

Managers have the responsibility to conduct themselves according to the Company's Code of Ethics and serve as examples to the people that report to them.

Examples of failing to achieve this can vary dependent each role, but could include:

- Failing to follow or ignoring processes and procedures;
- Failing to properly inform customers, clients or colleagues of something that could result in a detrimental outcome for them;
- Undertaking a task, making a recommendation, or providing advice without suitable training and/ or understanding;
- Carrying out an activity when you don't feel competent or trained.

The Company will investigate and take appropriate action if there's any reported issues where questionable or unethical behaviour is reported.

The Company aims to implement systems and controls to ensure where possible all and any external partners (suppliers, consultants, contractors and other engaged parties representing the Company (referred to as the "Third Parties")) are compliant with this Code.

.

3.0 ESG RISK MANAGEMENT POLICY

The Company believes an ESG Risk Management Policy is in the interests of the Company and its stakeholders and represents good industry practice.

This policy sets out the strategic and a structured approach to ESG Risk Management to identifying environmental, social and governance risks, including climate-related physical and transition risks, managing them, and ensuring that ESG Risk Management is an integral part in the governance at both a strategic and operational levels.

ESG risks, including climate-related risk, uncertainty, and change create potential risks for the Company need to be managed. Effective ESG Risk Management is an essential element of governance to meet the Company's strategic objectives.

With this purpose, we will seek to:

- Embed ESG Risk Management in our operational activities.
- Raise awareness of the need for ESG Risk Management.
- Manage ESG risks, including climate-related risks, to reduce impact and where possible likelihood of risk occurring.
- Maintain a robust process for identifying ESG risks and their likely impact to inform decision making.

ESG Risk Management includes the following stages:

3.1 Identify

Identifying risk is a systematic effort which in turn results in the creation of the risk register.

Identification can take place through, but is not limited to:

- Internal and external ESG audits
- Management and/or operational team meetings
- Feedback from stakeholders and other external organisations
- Advice from ESG advisors
- Board oversight

3.2 Assess

Risk analysis looks at the potential impact of a risk as well as the likelihood of occurrence. By multiplying impact by likelihood, a risk score is produced which can be used to determine an appropriate response.

This risk score tool is in-built into the risk register.

A risk can be closed on completion of mitigating actions, achievements of targets and/or when the Board is satisfied that there is no longer a risk to the Company.

3.3 Manage

Risk controls are those actions taken to reduce the likelihood of a risk event occurring, its frequency and the severity of the consequences should it occur.

Methods of risk management and control may include:

- Terminate - if the risk cannot be reduced to an acceptable level an option may be to stop the activity or course of action or find a different way of doing it
- Reduce - putting mitigating controls in place to reduce the likelihood of the risk occurring or the impact if it does arise.
- Tolerate - deciding to carry the risk as part of normal operations where the risk is unavoidable or more tolerable than alternatives.
- Change - move or let another party take on the risk such as an insurance Company.

3.4 Monitor and Report

Once identified and added to the risk register, the latter becomes the primary control document for subsequent analysis, control and monitoring of those risks.

Risk impact ranks from Low to Very High and is assigned score 1 to 5. Risk likelihood also ranks from Low to Very High and is assigned score 1 to 5. Overall risk score is calculated as indicated above by multiplying impact by likelihood, a traffic light approach is applied to group risk score between 1-9 as Green, low risks that the Company can Tolerate; between 9-16 as AMBER medium risks that the Company should aim to Reduce and/or Change where possible; above 16 as RED that can be classified as High and that the Company should consider whether there is an option to reduce the risk or if it would be appropriate/possible to Terminate and/or Change and activity generating the risk.

Risks are also monitored as NEW that appear from time to time as identified in section 1.3 above, ACTIVE that are ongoing and being tolerated and CLOSED that were subject to reduction, change and/or termination.

Risk assessment and monitoring is a continual process, the risk register is reviewed annually by the Board and reported accordingly to allow opportunity for consideration and discussion.

All ESG related risks, including climate-related risks, are documented within Annex 1 “ESG Risk Register” to this policy and are continuously monitored and updated.

3.5 Risk Appetite and Responsibility

Any such risk with a score over 12 that are identified will need to have a risk reduction plan implemented to return the risk to a tolerable level within an acceptable timescale.

Responsibility and accountability for managing the risks within the ESG Risk Register shall be managed by the SPV Management Team. The CEO shall decide which risks may need escalating to the Board of Directors.

3.6 Review

The Board of Directors will review this statement and the associated management systems annually.

4.0 EMERGENCY AND INCIDENT RESPONSE PROCEDURES

For our purposes, an incident is an event that:

- Could have financial or non-financial impact.
- Could involve any warranty or insurance claim or lawsuits.
- Could be a technical/engineering or non-technical event.
- Could be caused by natural disaster or change in regulation.
- Could be caused by human error or sabotage.
- Could have impact in the local community.
- Could cause damage to the environment, property or cause injury to any person.
- Could cause reputational damage.

The table below outlines possible incident types but should not be an exhaustive list:

Financial	Reputational	Regulatory	Internal control	WHSE / ESG	Legal	HR	Technology
Material financial incidents may include: • Unauthorised use of bank accounts • Duplicate or inaccurate payments (above €50,000) • Errors leading to the re-lodgement of financial statements or tax returns • An incident leading to a material economic loss to the business • Major deal or revenue opportunity lost or forfeited	Incidents leading to a loss or damage to reputation with clients or other external parties, including: • Adverse media coverage or parliamentary enquiry • Adverse impact to customers, clients no longer willing to deal with Pentacom or loss of key business opportunities	Any potential, or actual, breach of law, regulation or rule, including: • Expected/actual significant written warning and or fine from the regulator • Press statement required from/by the regulator • Breach of regulatory requirements resulting in revocation for restriction of license or authorization	Breakdowns in controls and processes, non-compliance with policies or evidence of improper behaviors, actions or decisions, including: • Major breach of internal policy reportable to senior management and/or major business or client impact and/or major breakdown in a critical control • Material fraud • Senior manager malpractice	Material incidents may include: • Fatalities and serious injuries or illnesses • Immediate or anticipated loss of key clients or business opportunities • Significant environmental damage to surrounding area with medium- or long-term consequence • Permanent damage to an area of cultural heritage significance • Significant impact on the surrounding social environment with serious health risks with high likelihood of class action	Material legal issues may include: • Any material litigation brought by or against Pentacom • Any matters that could give rise to action against any directors • Any incident that may affect permits or licenses or material contracts	Material incidents may include: • Any claims with the potential to cause reputational harm and/or media coverage, such as claims for sexual harassment, discrimination or multi-party claims • Any claims involving the management team, their direct reports and/or any Board members • Applications for or the establishment of any new relationships with unions or other employee representative bodies • Senior resignations or firings	Any event whereby: • A large number of staff are affected and/or not able to do their job • A large number of customers are affected and/or acutely disadvantaged in some way • Incident is a cybersecurity or data breach

If an incident occurs or if it is unclear whether an incident has occurred, the Shareholders Representatives (specified below) should be informed as soon as possible. The Shareholders Representatives would assess whether escalation to the Board is required. The Board would initiate the internal escalation processes if required.

Shareholders Representatives

- Raja Kanasalingam. Raja.Kanasalingam2@macquarie.com
- Carlos Fernández. carlos.fernandez@macquarie.com
- Marta de Juan Martinez. marta.dejuanmartinez@abrdn.com
- Maitane Aramburu. Maitane.Aramburu@abrdn.com
- Alex Shapiro. ashapiro@arjuninfrastructure.com
- Jack Kim. Kim@ArjunInfrastructure.com

5.0 ANTI-BRIBERY AND CORRUPTION

5.1 Definition :

The Company is committed to conducting its business in accordance with all applicable laws and regulations, and in a way that enhances its reputation in the market. The actual or attempted use of any form of bribery or corruption either directly or indirectly on behalf of the Company to advance its business interests or those of its associates is strictly prohibited.

The Company has adopted a Crime Prevention Manual and a Criminal Compliance Policy according to art. 31 bis of the Spanish Criminal Code, the purpose of this documents is also to demonstrate a commitment to the prevention of corruption and to define rules of conduct to prevent the commission of acts of corruption. The Anti Bribery and Corruption Policy is part of the organisation's criminal complaints system.

For the purposes of this policy:

- a bribe is anything of value given, offered, promised, accepted, requested, or authorized (in each case, directly or indirectly) with the intent that a person who is trusted or expected to act in good faith or with impartiality, performs that function improperly or in order to obtain or retain an advantage in the course of business.
- Indirect benefits, even though not cash, can also be considered bribes.
- Anything of value includes cash, gifts, hospitality, expenses, reciprocal favours, business or employment opportunities, political or charitable and a range of other direct or indirect benefits.
- Corruption is the misuse of public office or power for private gain, or misuse of private power in relation to business outside the realm of government. Contributions.
- A conflict of interest is case when private interests are conflicted or seem to be conflicted with the interests of the Company.

Further detail and explanation on the anti-bribery and corruption policy and definitions is contained in Appendix A.

The Company principle regarding the treatment of bribery and corruption is to:

Refuse to offer, give, or receive bribes or improper payments, or participate in any kind of corrupt activity, either directly or through any third party.

*The Anti Bribery and Corruption Policy of the Company is **never to**:*

- *participate in any form of corrupt behaviour;*
- *engage public officials to provide services without proper approval from the Company board;*
- *conceal or fail to record accurately and completely the true nature of our activities, or falsify or tamper with the Company's books or records;*
- *pay more than fair market value for goods and services;*
- *make facilitation payments (except where such payments are expressly permitted by written law);*
- *give or receive gifts or hospitality which could be, or be seen as, an improper inducement, or as creating a conflict of interest;*

- *give political donations and finance any lobbying activities in cash or in kind (membership fees, fundraising events) to any political parties, individuals standing for election, or non-profit organisations that support political parties or individuals standing for election;*
- *give charitable contributions (including sponsorships and other advantages) for improper purposes; or*
- *engage third parties to make improper payments or participate in any kind of corrupt activity on its behalf;*

always to:

- *seek to avoid even the appearance of wrongdoing, recognising that an allegation of bribery or corruption can seriously damage the Company's reputation;*
- *carry out appropriate anti-bribery due diligence when engaging or entering into contracts with third parties;*
- *ensure contract and procurement documents include appropriate anti-bribery measures and comply with Spanish Criminal Code;*
- *ensure Company staff and/or those persons operating on behalf of the Company receive training regarding Bribery and Corruption policy and procedures and understand the implications of non-compliance;*
- *ensure that the Company has in place adequate procedures for Company representatives to report instances or allegations of bribery or corruption;*
  through financial and governance procedures assess compliance with this policy; maintain a gifts and hospitality register to record all instances of gifts or hospitality (>€100) given or received, seeking approval in advance (if practicable) from the CEO.

Further; any charitable donations made by the Company and any donations made by the Company in supporting the communities in which it operates shall be approved by the Company's Board.

If a Company or Third-Party representative believes that there has been an incident related to political contributions, please refer to the Whistleblowing section below for further guidance on reporting serious concerns and contact details.

If a Company's representative, such as a relative or business partner who work for a Third Party and/or hold decision-making position with a Third Party and/or offer/receive gifts and hospitality because of such position such relationship should be disclosed to the CEO as this would be potentially considered a conflict of interest.

The Company's staff must be alert to the possibility that a benefit given or offered to an associate, such as a relative or business partner, or channelled through an agent or other intermediary, may be a bribe. Recklessness or wilful blindness to such incidences is likely to be in contravention of applicable laws and/or regulations and will amount to a breach under this policy.

The Company expects all its representatives and Third Parties' representatives to disclose any potential conflicts of interest so that these can be properly considered, and action taken if needed. Not declaring a potential conflict of interest can become a problem if an issue later arises.

If a Company or Third-Party representative believes that there has been a breach related to conflicts of interest, please refer to Whistleblowing section below for further guidance on reporting serious concerns and contact details.

Any employee, officer or Director of the Company must not give, offer, promise, accept, request or authorize a bribe whether directly or indirectly, on behalf of, or for the benefit of the Company. A bribe may be in the form of cash, gifts, entertainment or other benefits. The actual or attempted use of any form of bribery or corruption either directly or indirectly on the Company's behalf to advance our business interests or those of our associates is strictly prohibited.

From the date of implementation of this policy onwards, all material agreements with third parties must include the requirement for them to comply with relevant anti-money laundering and anti-corruption regulations.

All instances of actual, suspected or alleged acts of bribery, corruption, fraud or anti-social forces must be immediately escalated to the Board (or its shareholders if one or more of the Board members are deemed to be engaging in such acts). The Company's officers are not to investigate the acts themselves.

Further detail and explanation on the anti-bribery and corruption policy is contained in Appendix A.

6.0 ANTI-FRAUD POLICY

6.1 Background

The Company has a commitment to high legal, ethical, and moral standards. everyone working on the Company's behalf (directly employed or otherwise is expected to share this commitment. This policy is established to facilitate the development of procedures, which will aid in the investigation of fraud and related offences.

The Company does not tolerate fraud. Fraud is defined as a misrepresentation or omission made knowingly and intentionally by an individual or group of individuals in order to secure financial or personal gain.

The Company will stablish, where feasible, procedures through its management service provider that reduce the likelihood of fraud occurring. These include processes and systems of internal control and risk assessment. In addition, the Company to ensure that a risk (and fraud) awareness culture exists in this organisation.

This document is intended to provide direction and help to those officers and directors who find themselves having to deal with suspected cases of theft, fraud or corruption. These documents give a framework for a response and advice and information on various aspects and implications of an investigation. These documents are not intended to provide direction on prevention of fraud.

6.2 Fraud Policy

This policy applies to any irregularity, or suspected irregularity, involving employees as well as consultants, vendors, contractors, and/or any other parties with a business relationship with this Company. Any investigative activity required will be conducted without regard to any person's relationship to this organisation, position, or length of service.

Actions Constituting Fraud

Fraud comprises both the use of deception to obtain an unjust or illegal financial advantage and intentional misrepresentations affecting the financial statements by one or more individuals among management, staff or third parties.

Anti-competitive practices are a type of fraud that happens when a Company behaviour results in reduction of competition in a market. All Managers and Supervisors have a duty to familiarise themselves with the types of improprieties that might be expected to occur within their areas of responsibility and to be alert for any indications or irregularity.

If a Company or Third-Party representative believes that there has been an incident related to Anti-competitiveness and fraud by engaged Third Parties or supply chain, please refer to Whistleblowing section below for further guidance on reporting serious concerns and contact details.

The Board's Policy

The Board is absolutely committed to maintaining an honest, open and well-intentioned atmosphere within the Company. It is therefore also committed to the elimination of any fraudulent activity, and to the rigorous investigation of any such cases.

The Board wishes to encourage anyone having reasonable suspicions of fraud to report them. Therefore, it is also the Board's policy, which will be rigorously enforced, that no employee will suffer in any way as a result of reporting reasonably held suspicions (See the Whistleblower and Grievance Policy for further information).

Members of staff can therefore be confident that they will not suffer in any way as a result of reporting reasonably held suspicions of fraud. For these purposes reasonably held "suspicions" shall mean any suspicions other than those, which are raised maliciously and found to be groundless. The organisation will deal with all occurrences in accordance with the Public Interest Disclosure Act.

7.0 LEGAL MATTERS

7.1 Sanctions

The Company does not deal with, finance, advise, manage or provide services to names, entities or businesses prohibited by international organizations (such as the United Nations) and certain countries which the Company considers relevant, including Australia, the United Kingdom, the United States and the

countries included in the European Union. The Company will not deal with these names which can include specially designated nationals of those countries, terrorists, terrorist organizations, narcotics traffickers, proliferators of weapons of mass destruction and organizations engaging or supporting such criminals and their activities.

If the Company detects or identifies a client or a transaction fall under one of these prohibitions or require further guidance, it must be immediately escalated to the Board or (where appropriate) the shareholders of the Company.

7.2 Legal agreements

Prior to the finalization of contractual terms and execution of any material agreements, the Company must ensure that all legal risks relating to agreements are assessed and adequately addressed.

The Board has ultimate responsibility for ensuring that adequate legal review and, if appropriate or required by shareholders, external counsel is undertaken prior to entering into all contracts in conjunction with review and approval by the Board or its authorized delegate(s). Equally, internal or external compliance and tax advice must be received prior to entering into the agreement if there are material compliance or regulatory risks and indirect tax considerations. External counsel to be engaged by the Company must have the required expertise for the matters it is engaged and, where a matter may materially affect its substantial shareholding entities, appointment of counsel should be approved by the relevant shareholding entity(ies) or their directors, officers or employees.

The Company will not enter into agreements which may restrict the activities of, or have terms or conditions that could adversely affect, its substantial shareholding entities. Should any such agreements be considered, approval will be required by that shareholder.

Exclusivity, no circumvention and no poach agreements are examples that can restrict other areas of substantial shareholders. Debt contracts are examples where pledges and covenants, granting of security interests or default clauses could adversely impact other entities. Borrowing by the subsidiary should therefore be approved by the shareholders.

7.3 Regulatory approvals

The Company must take all reasonable steps to obtain and must comply in all material respects with the terms of, all governmental and other licenses and consents necessary for the conduct of its business.

7.4 Legal incidents

Any matter which may give rise to legal action against the Company, a director, an officer, an employee or a substantial shareholder, any material legal action against third parties taken by the Company or any engagement with or request for meeting or information by a law enforcement, prosecuting authority or regulator (other than certain agreed ordinary course of business matters) must immediately be advised to the shareholders and the Board.

8.0 FINANCIAL AND ADMINISTRATIVE CONTROLS

Financial management shall be conducted in accordance with the processes and Delegation of Authority implemented by the Company.

8.1 Delegation of Authority

This Delegation of Authority is designed to improve efficiency in managing the affairs of the Company. Any person delegated with authority herein shall nevertheless report to the Shareholders Representatives or the Board whenever there is any matter that he or she has approved in accordance with this policy and deems to be material.

8.2 Annual budget

The annual budget and accompanying business plan shall be prepared by the Company in advance of the start of each financial year and it shall cover all anticipated costs for the year. The annual budget shall initially be submitted to the Shareholders Representatives. Following that the proposed budget shall be presented to the Board and their approval and sign-off sought. On approval of the budget it shall become the operating budget against which reporting will be completed during the relevant year.

If the activities of the Company significantly change during the financial year and the operating budget is no longer deemed relevant with prior approval from the Board a revised budget can be proposed for acceptance by the Board. The revised budget shall be proposed in accordance with the process for the annual budget approval.

8.3 Accounting

8.3.1 Compliance with Spanish GAAP

The Company needs to comply with Spanish GAAP for statutory and regulatory reporting purposes.

.

8.3.2 General ledger and accounting books

The Company will maintain the accounting books and records (i.e., general ledger and subsidiary books, financial statements, tax related documents, etc.) and will retain the record for the period set forth in laws and regulations (i.e., six years pursuant to Article 30 of the Spanish Commercial Code), although the Board can decide to extend the record retention period. Accounting entries must be made in a timely manner with appropriate controls over systems access, segregation of duties and full audit trail.

8.4 Payment controls

1.1.1 Bank account management

Cash management

Cash management and management of bank accounts shall be handled by the Company. In order to prevent potential fraud and human error in relation to payments made by the Company, in making payments pursuant to existing agreement, the Company must ensure that:

- Each user of the bank account will have an individual access to the online banking portal with individual security tokens that are held securely at all times.
- User logins and passwords are not to be shared.
- Changes to user rights and accesses are dual approved by relevant authorized signatories.
- Any variations to banking arrangements can be made or varied only by dual signatories on the accounts.
- Invoices and payments must be reconciled to bank accounts by designated personnel at frequent and regular intervals (at least monthly) to ensure there are no errors or unauthorized banking activity.
- The personnel performing the reconciliation should be segregated from the payments process.
- The Company will conduct a review of user access at least every six months to ensure access to banks accounts remains appropriate.

The above requirements must be requested of, and adhered to by, any person or service provider processing payments on behalf of the Company.

Treatment of deposit surpluses or deficits

If any discrepancies between the bank balance in the account and the book are discovered, the party making the discovery should notify the Shareholders Representatives immediately and an investigation should be completed. If the discrepancy is not explained within two weeks the Board shall be notified.

1.1.2 Payment procedure

Payment process control

The aim of this procedure is to minimize the risk of losses through fraud and error by establishing a consistent and adequate baseline of controls throughout all payment processes including:

- Appropriate segregation of duties, no single person should be able to authorize, prepare, make, and receive a payment.
- Controls for data entry are in place, transaction authority, accuracy, completeness, error correction and audit trails are documented.

- Monitoring and reporting requirements set out in the anti-money laundering and counter-terrorism financing regulations are complied with, where applicable and all payments comply with antibribery and corruption policy.

Payment approval

- When invoices are received, a representative of the Company needs to review invoices to ensure that services have been performed properly and amounts are correct.
- It is the responsibility of the approvers to cross check to ensure the amount is within approved budget before allowing the expense to go through.
- All payments must be approved in accordance with the Delegation of Authority
- In the case of the Company making payments to Company staff that are not payroll or approved disbursements, approval should be provided by the Shareholders Representatives
- The approvers of any payments to be made on behalf of the Company must be different to the person responsible for preparing and making the payment.
- The Company must perform independent call-backs (i.e., independently source the number and call the recipient of a payment to authenticate bank account details) for payments to any new bank account, or to existing bank accounts for which the details have changed.
- Verified data is held in a restricted access master document and is shared in a non-editable format with banking approvers as part of back up for payments processing.
- For in-house payroll management there should be dual control over any amendments to payroll data (salary updates, changes to bank details, etc.) with a separate approver of the payroll required prior to payment processing.

8.5 Outsourced activities

Regarding the Financial area, the Company outsources certain accounting and tax, services which are summarized below. Any substantial change to these services must be approved by the Board.

At least every two years, the CFO will review both the performance of the relevant financial service provider and determine whether the scope of their services is still appropriate.

Accounting

- Preparation of accounting statement
- Issue of auxiliary breakdowns of accounts (i.e., bank movements)
- Issue of quarterly and year to date balance sheet, profit and loss account, and trial balances
- Preparation of annual accounts

Tax

- Preparation of the statutory quarterly corporate tax and VAT returns

- Preparation of the statutory annual corporate tax and VAT returns
- Electronic filing of tax returns

The Company secretarial services may be outsourced or not depending on the Company needs:

Company secretarial

- Drafting the minutes of the Board meetings
- Preparing the corresponding corporate documents for drafting, approval and submission to the Spanish Companies House
- Providing corporate book-keeping services

8.6 Procurement process compliance

Purchasing and contracting activities are subject to the following rules to ensure transparency, traceability and compliance.

Principles

For any purchase with a total contract value greater than €50,000 the following shall apply:

- A minimum of three proposals must be obtained.
- The transaction must be validated by the Requesting Area, Finance, Legal and the CEO.
- Anti-bribery and corruption policies must be complied with, including the disclosure and management of any conflicts of interest.

Procedure

1. Upon receipt of responses to the RFP, the Requesting Area will prepare a comparative summary of at least three proposals that includes, at a minimum:
   I. The business need that justifies the purchase along with a declaration of the absence of any conflict of interest.
   II. The technical assessment of the proposals, indicating adherence to requirements and identification of gaps and risks.
   III. The economic terms (pricing, duration, penalties, creditworthiness, etc.).
   IV. Liabilities and obligations.
   V. A justified recommendation for the award, highlighting the rationale.

2. The summary described in 1), together with the proposals received, shall be sent to the approval areas at least five business days before the Financial and Strategy Committee meeting.
3. At the Financial and Strategy Committee, the proposals will be reviewed and, as applicable, approved. The record of such approval shall form part of the minutes of the Committee.

4. Where urgency prevents waiting until the next Committee meeting, approval may be requested by email, provided that the requirements in points 1) and 2) are met. Such email approvals will be ratified at the following Committee meeting.

9.0 WORK HEALTH, SAFETY AND ENVIRONMENT

9.1 General WHSE commitment

The Company must comply with all applicable, state, regional and local legal requirements and act in accordance with good industry practice.

The Company is committed to promoting and implementing a proactive culture which places high importance on ensuring effective health, safety and environmental management systems are observed and proactive safety behaviours and leadership are encouraged.

The Company will not be directly engaged in any activities that do not involve office work but will engage a third-party WHSE consultant to assess the WHSE policies and procedures of the Company in charge of the operation and maintenance of the network.

9.2 WHSE when commuting and traveling

When commuting or traveling, the Company employees will determine the most appropriate method of transportation (train, car, plane, etc.). Where driving is selected, the following requirements are in place:

- Drivers will be in possession of a valid and appropriate driving license
- Employees are responsible to ensure their vehicle is appropriately maintained and safe to drive
- For long trips (>2 hours of continuous driving) appropriate rest breaks will be made
- Employees are required to comply with local driving rules and speed limits
- Employees will wear seat belts as required by law
- The driving policy prohibits the use of mobile phones or two-way radios when driving
- Any traffic incidents incurred when driving for work will be reported to management

9.3 WHSE at the office

The Company will ensure that office premises used by the Company staff are compliant with the relevant building safety codes, and staff are aware of all emergency and evacuation procedures.

10.0 HUMAN RIGHTS

We are a responsible Company that believes in fair competition and transparent business processes and operating in compliance with applicable law and regulations including compliance with the letter and spirit of tax laws and we expect our business partners to operate to the same standards. We believe that all people employed, either directly or indirectly, should be treated fairly and have their human rights fully respected.

We will take steps to ensure, as far as possible, that those people employed do not have their human rights infringed and if we become aware of any infringements we will take steps to address any adverse impacts.

The Company and our supply chain comply with the OECD Guidelines for Multinational Enterprises and the UN Guiding Principles on Business and Human Rights, including the principles and rights set out in the eight fundamental conventions identified in the Declaration of the International Labour Organisation on Fundamental Principles and Rights at Work and the International Bill of Human Rights.

In order to minimise the risks of working with suppliers that do not comply with our own standards and requirements we have adopted the following processes related to employment of new contractors:

Before entering into any new relevant and material contracts (those with contract value above 300k€ per year) involving the delivery of services to the Company we will undertake the following questionnaire:

1. We will check that the Company to be employed has a Whistle-blower and Grievance procedure.
2. We will check that the Company has Health & Safety Management system.
3. We will check that the Company has appropriate policies, and associated procurement and supply chain monitoring practices in place to protect employees and respect their human rights including freedom of association, inclusion and diversity, employee engagement, labour standards and working conditions.
4. We will check that the Company has an anti-bribery and corruption policy.
5. We will check for any evidence of breaches of the above policies and procedures and if found check whether they have been appropriately remediated and measures taken to avoid recurrence.
6. We will check if any convictions have been made against the Company including in relation to labour law, human rights, environmental law, tax payments, corruption and anti-competitive practices.
7. We will check that the Company to be employed has an Anti-slavery and Human Trafficking policy.

Any identified concerns or violations will be considered, and appropriate decisions and solutions will be approved by the Board of Directors and Sustainability Committee prior to signing the contract.

10.1 Anti- Slavery and Human Trafficking

Modern slavery and human trafficking are deemed criminal offence as are a violation of fundamental human rights.

Modern slavery means slavery, forced and compulsory labour, bonded and child labour where victims are forced against their free will into providing work or services.

Human trafficking comprises a situation where a person arranges or facilitates the travel of another person with a view to that person being exploited against their free will.

The Company does not tolerate slavery, human trafficking, or forced labour conditions of any kind.

The Company prohibits the use of modern slavery or human trafficking in the Company's operations and supply chain by means of rigid and transparent due diligence process, tender and procurement processes, and procedures.

If a Company or Third-Party representative believes that there has been an incident related to modern slavery and human trafficking by engaged Third Parties or supply chain, please refer to Whistleblowing section below for further guidance on reporting serious concerns and contact details.

We monitor the above on an ongoing basis within the organization. When contracting with key suppliers we distribute the sustainable procurement questionnaire that ensures the relevant policies in place.

11.0 INSURANCE

The Company must identify and appropriately manage insurable risks according to the following guidelines:

Identification of insurable risks

Insurable risks including property, business interruption, travel, etc. should be identified and reviewed annually and when key events occur.

Analysis of insurable risks

An assessment of the different insurable risks should be performed, including the following:

- Likelihood of occurrence of loss events.
- Magnitude of potential losses.
- Possible mitigants.
- Risk tolerance of the business.

Decision on risk retention or transfer

Following the analysis of insurable risks, a decision on which risks to retain and which to transfer via insurance should be made. When risks are insured, the following should be considered:

- Select appropriate excess (retention).
- Select appropriate limits.
- Match insurance cover to risk exposures.
- Comply with any specific insurance requirement.
- Select appropriate insurers.

On at least an annual basis, the Company will review its insurance requirements and the appropriateness of its existing policies.

Before the expiry of an active policy, the Company will determine whether to renew it or not.

12.0 WHISTLE-BLOWER AND GRIEVANCE PROCEDURE

12.1 Introduction

The Company is committed to the highest standards of openness, probity, and accountability in our activities.

An important aspect of accountability and transparency is a mechanism to enable staff and other members of the Company and stakeholders to voice concerns in a responsible and effective manner. It is a fundamental term of every contract of employment that an employee will faithfully serve his or her employer and not disclose confidential information about the employer's affairs. Nevertheless, where an individual discovers information which they believe shows serious malpractice or wrongdoing within the organisation then this information should be disclosed internally without fear of reprisal, and there should be arrangements to enable this to be done independently of line management (although in relatively minor instances the line manager would be the appropriate person to be told).

The Company is bound by national and international law for whistleblowing and grievance, which will apply, unless the requirements of this procedure are more stringent. In the case of the company the applicable law is the Spanish Whistleblowing Law 02/2023 (hereinafter altogether referred to as "Whistleblowing Law").

In compliance with the provisions of the Whistleblowing Law, the Company has implemented an Internal Reporting System (or Whistleblowing System), conceived as a comprehensive mechanism for the receipt of information regarding serious malpractice or wrongdoing within the organisation. This system encompasses both the internal reporting channel which is hosted on an online platform, as will be explained further below, and the figure of the Internal Reporting System Officer, who, in the case of the Company (as will be further detailed below), is the Criminal Compliance Committee, responsible for its overall management and supervision. The system is governed by this Whistleblower and Grievance Procedure, which regulates the processing, follow-up, and resolution of the reports submitted, while ensuring at all times the protection of the whistleblower and the rights of the individuals concerned.

The Company has endorsed the provisions set out below to ensure that no person should feel at a disadvantage in raising legitimate concerns.

It should be emphasised that this procedure is intended to assist individuals who believe they have discovered malpractice or impropriety. It is not designed to question financial, or business decisions, taken by the Company nor should it be used to reconsider any matters which have already been addressed under harassment, complaint, disciplinary or other procedures.

12.2 Scope of Procedure

This procedure is designed to enable stakeholders of the Company and employees of the Company (as applicable), to raise concerns internally and at a high level and to disclose information which the individual

believes shows malpractice or impropriety. This procedure is intended to cover concerns which are in the public interest and may at least initially be investigated separately but might then lead to the invocation of other procedures e.g., disciplinary. These concerns could include:

- Financial malpractice or impropriety or fraud.
- Failure to comply with a legal obligation or Statutes.
- Health & safety, human rights, other social, or environmental breaches or concerns.
- Criminal activity.
- Improper conduct or unethical behaviour.
- Attempts to conceal any of the above.

12.3 Safeguards

Protection - this procedure is designed to offer protection to those employees of who disclose such concerns provided the disclosure is made:

- in good faith
- in the reasonable belief of the individual making the disclosure that it tends to show malpractice or impropriety and if they make the disclosure to an appropriate person (see below). It is important to note that no protection from internal disciplinary procedures is offered to those who choose not to use the procedure. In an extreme case, malicious or wild allegations could give rise to legal action on the part of the persons complained about.

Confidentiality – will treat all such disclosures in a confidential and sensitive manner. The identity of the individual making the allegation may be kept confidential so long as it does not hinder or frustrate any investigation. However, the investigation process may reveal the source of the information and the individual making the disclosure may need to provide a statement as part of the evidence required.

Additionally, confidentiality will be guaranteed even when the disclosure is submitted through channels other than the officially established ones or to staff members not responsible for its handling. In such cases, personnel will have received appropriate training on the matter and will have been informed that breaching confidentiality constitutes a very serious offense. Furthermore, any recipient of such a disclosure is obligated to forward it immediately to the Criminal Compliance Committee responsible for handling the whistleblowing system.

Anonymous Allegations - This Procedure encourages individuals to identify their name when making a report. Concerns expressed anonymously have less credibility; however, the company will handle all anonymous reports received through the channels provided.

Untrue Allegations - If an individual makes an allegation in good faith, which is not confirmed by subsequent investigation, no action will be taken against that individual. In making a disclosure the individual should exercise due care to ensure the accuracy of the information. If, however, an individual makes malicious or vexatious allegations, and particularly if he or she persists with making them, if the individual is an employee of the Company disciplinary action may be taken against that individual.

Rights of the Affected Person - The Company also guarantees the rights of the Affected Person (understood as any natural or legal person named in a report and attributed responsibility for, or involvement in, the alleged serious malpractice or wrongdoing) to be informed of the actions or omissions attributed to them,

and to be heard at any time during the proceedings. Such communication shall take place at the time and in the manner deemed appropriate to ensure the proper conduct and outcome of the investigation. In all cases, the presumption of innocence and the right to honour of the Affected Person shall be fully respected throughout the process.

Data protection - All personal data processed in connection with a report — including that of the whistleblower, the Affected Person (considered a "data subject" in accordance with Article 4 of the General Data Protection Regulation), and any other individuals mentioned — shall be handled in strict compliance with the provisions of the UE General Data Protection Regulation (GDPR), the Spanish Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), and the Company's Data Protection Policy.

12.4 Procedures for Making a Disclosure

Where an individual discovers information or activities which they believe shows serious malpractice or wrongdoing, this should be disclosed internally without fear of reprisal.

To this end, the Company has established an online platform, available at the following link: https://onivia.factorial.es/complaints, which enables individuals to make a disclosure — either verbally or in writing — regarding any information or activities they reasonably believe constitute serious malpractice or wrongdoing.

The Company has appointed the Criminal Compliance Committee to be responsible for the Internal Reporting system. After disclosure, Criminal Compliance Committee shall manage the communications of infringement in accordance with the Whistleblowing Law and this Procedure. The Committee may rely on external experts to carry out the process of managing the whistleblowing case.

This process includes complaints of malpractice from contractors and service providers. On receipt of a complaint of malpractice, the member of staff who receives and takes note of the complaint, must pass this information as soon as is reasonably possible, to the Criminal Compliance Committee .

In any case, if there is evidence of criminal activity then the Criminal Compliance Committe should inform the police and/or the public prosecutor's office. The Company will ensure that any internal investigation does not hinder a formal police investigation.

Should none of the above routes be suitable or acceptable to the complainant, then the complainant may approach the following individuals who has been designated as an independent point of contact under this procedure.

12.5 Timescales

The Criminal Complaince Committee shall send an acknowledgement of receipt within a maximum of seven days of receipt of the notification and carry out the investigation within a maximum of three months. The Criminal Complaince Committee may extend the investigation for a further three months in the case of particularly complex whsitleblowing communications). The Criminal Compliance Committe should ensure

that the investigations are undertaken as quickly as possible without affecting the quality and depth of those investigations.

The Criminal Compliance Committe, should as soon as practically possible, send a written acknowledgement of the concern to the complainant and thereafter report back to them in writing the outcome of the investigation and on the action that is proposed. If the investigation is a prolonged one, the Criminal Compliance Committe should keep the complainant informed, in writing, as to the progress of the investigation and as to when it is likely to be concluded.

All responses to the complainant should be in writing and marked “confidential”.

12.6 Investigating Procedure

The Criminal Compliance Committee should follow these steps:

- Full details and clarifications of the complaint or issue should be obtained.
- If there is a complaint against a member of staff, the Criminal Compliance Committe should inform the member of staff against whom the complaint is made as soon as is practically possible. The member of staff will be informed of their right to be accompanied by a trade union or work colleague at any future interview or hearing held under the provision of these procedures. At the discretion of the Criminal Compliance Committe and dependant on the circumstances of the complaint or issue, an alternative representative may be allowed e.g. the individual’s legal representative.
- In the event that a communication gives rise to, or may give rise to, a conflict of interest involving any member of the Criminal Compliance Committe, the affected member shall immediately disclose the situation to the other member. The Committee shall then promptly inform the Board of Directors, which will appoint a person responsible for managing the complaint.
- The Criminal Compliance Committe should consider the involvement of the Company auditors and the Police at this stage and should consult with the Chairman / Board / Business Owner if appropriate.
- The allegations should be fully investigated by the Criminal Compliance Committe with the assistance where appropriate, of other individuals / bodies.
- A judgement concerning the complaint / issue raised and validity of the complaint / issue raised will be made by the Criminal Compliance Committe. This judgement will be detailed in a written report containing the findings of the investigations and reasons for the judgement. The report will be passed to the Chief Executive Officer .
- The Chief Executive Officer will decide what action to take. If the complaint / issue raised is shown to be justified, then they will invoke the disciplinary or other appropriate Company procedures.
- The complainant or individual should be kept informed of the progress of the investigations and, if appropriate, of the final outcome. Where necessary, the Criminal Compliance Committee may contact the complainant or individual to request additional information or clarification in relation to the report, while ensuring continued confidentiality and protection of their identity.
- If appropriate, a copy of the outcomes will be used to enable a review of Company procedures.
- The Committee will establish and maintain a Register (kept in electronic format with restricted access) recording all reports received and any internal investigations initiated as a result thereof. This Register will ensure full compliance with confidentiality requirements

and will contain sufficient information to identify and understand the circumstances surrounding the complaint or issue reported.

If the complainant or individual is not satisfied that their concern is being properly dealt with by the Criminal Compliance Committee, they have the right to raise it in confidence with other designated persons as described above.

If the investigation finds the allegations unsubstantiated and all internal procedures have been exhausted, but the complainant or individual is not satisfied with the outcome of the investigation, the Company acknowledges the lawful right of employees and ex-employees to make disclosures to external reporting channels which have been established by the Spanish Independent Whistleblower Protection Authority and/or by the competent authorities or bodies of the Spanish autonomous communities.

13.0 DATA PROTECTION POLICY

13.1 Privacy and data protection

This policy states the Company's commitment to fulfilling all obligations applicable to it in the field of personal data protection, as required by the Spanish Organic Law 3/2018, of 5 December, on the protection of personal data ("LOPDGDD") and the European Regulation 679/2016, of 27 April, on the protection of personal data ("GDPR") as well as any other legal or regulatory norms that affect, develop, or replace the aforementioned in this area.

The Company will take reasonable steps to keep personally identifiable information ("PII") of individuals (including its own employees) secure and protected from misuse, loss or unauthorized access, modification or disclosure.

Definitions:

Personal Information:	Information which relates to a living individual who can be identified from that information or from that and other information, which is in the possession of, or is likely to come into the possession of the Company or other data processor. It includes any expression of opinion about the individual and any indication of the intentions of any person or body in respect of the individual.
Data Protection Laws:	The GDPR and the LOPDGDD.
Data Controller:	The Company or another person or body who is subject to the requirements of the Data Protection Laws by determining the purposes for which and the way any personal information are, or are to be, processed.
Data Subject:	This term means a living individual who is the subject of personal information.

This policy applies to all Company employees and others who process personal information on the Company's behalf.

13.2 Records management

The GDPR regulates the use of information relating to living people (personal information), protecting and giving rights those to whom that information relates.

The GDPR requirements are based upon the eight Data Protection Principles.

These state that personal information shall:

1. Be obtained and processed fairly and lawfully and not be processed unless certain conditions are met.

2. Be obtained for a specified and lawful purpose and not be processed in any manner incompatible with that purpose.

3. Be adequate, relevant and not excessive for that purpose.

4. Be accurate and kept up to date where necessary.

5. Not kept for longer than is necessary for that purpose.

6. Be processed in accordance with the data subject's rights.

7. Be kept secure, safe from unauthorized access, accidental loss, damage or destruction.

8. Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal information.

The Company is committed to adhering to the above principles, ensuring the lawful, fair, and transparent processing of personal data, with a firm commitment to data minimization, accuracy, integrity, and confidentiality.

The Company is subject to a range of legal, regulatory and best practice requirements to retain and produce certain records, including documents, emails, voice recordings and other forms of communication. The Company must retain accurate and comprehensive information to evidence commercial transactions, to preserve corporate history, and to ensure that the Company can meet any legal and regulatory requirements that may exist or arise in relation to the retention and retrieval of records.

If any employee of the Company becomes aware of a privacy breach, he/she should contact the CEO and/or (where appropriate) the Board immediately, in addition to complying with the procedure for the notification and management of incidents and data security breaches that is available to the Company.

13.3 Policy Statements

Compliance with the applicable Data Protection Laws

13.3.1 The Company shall comply with the applicable Data Protection Laws and the eight Data Protection Principles.

Responsibility for Data Security

13.3.2 The Company may nominate individual for data security who is responsible for data security compliance and provides a point of contact for all data security issues ensuring:

- All users of personal information are made aware of good practice in data security;
- The provisions of adequate training for all staff responsible for personal information;
- That everyone handling personal information knows where to find further guidance;
- That queries about data security, internal and external to the Company, are dealt with effectively and promptly;
- The regular review of data protection procedures and guidelines within the Company; and
- All staff shall ensure that any personal information they process is appropriately secure and in compliance with the Company's policies covering information security.

Data Protection rights

13.3.3 The GDPR recognizes the rights of access, rectification, erasure, restriction, opposition, data portability and the right not to be subject to automated individual decisions of all data subjects.

The aforementioned rights give data subjects the ability to access, modify and delete personal data, as well as to demand their limitation for certain periods of time and to allow the data subject not to be subject to a decision based solely on automated processing. The rights recognized in the GDPR allow data subjects to defend their privacy and to control for themselves the use made of their personal data. Therefore:

13.3.4 The Company shall encourage informal exercise of data protection rights at a local level but shall have a formal procedure for the exercise and attention of data protection rights.

13. 3.5 The Company shall always require proof of identity for such requests and proof of authorisation where requests are made on the behalf of a data subject by a third party

13.3.6 The Company is committed to empowering data subjects by providing them with highly visible, easily accessible, and straightforward methods to exercise their rights. This commitment includes the implementation of clear, user-friendly procedures and forms, ensuring that data subjects can assert their rights under the applicable Data Protection Laws with minimal complexity and maximum efficiency.

13.3.7 The Company must make it possible to submit requests for the exercise of rights by electronic means.

13.3.8 Additional considerations and the detailed process for receiving and managing requests related to the exercise of data protection rights are outlined in the 'Procedure for the Exercise and Attention of Rights in Data Protection Matters.' This document is readily available to the Company and constitutes an essential resource that all employees must be familiar with and adhere to. Compliance with this procedure is imperative to ensure the effective and lawful handling of data subject rights requests, aligning with the Company's commitment to data protection and privacy.

Sharing and Disclosure of personal information

13.3.9 All disclosures of personal information shall be undertaken in accordance with such an agreement or in the case of ad hoc disclosures in compliance with the applicable Data Protection Laws and documented as such.

13.3.10 All data processors shall agree to conform to this policy and the applicable Data Protection Laws, and as far as possible, indemnify the Company against any prosecution, claim, proceeding, action or payments of compensation or damages without limitation and provide any personal information specified on request to the nominated individual responsible for the data protection matters of the Company and/or the Data Protection Officer, if appointed.

Policy Enforcement and sanctions

13.3.11 Compliance with this policy is the responsibility of all Company staff who process Personal Information on its behalf. Breach of the Data Protection Policy may lead to disciplinary action or withdrawal of facilities.

13.3.12 Any questions about the interpretation or operation of this policy should be referred to the nominated individual responsible for the data protection matters of the Company and/or the Company Data Protection Officer, if appointed.

Continuous improvementThe Company is committed to continuously reviewing and improving its data protection policies and practices to align with evolving regulations and best practices in data protection.

The Company's commitment to data protection is a central aspect of its operations. The Company pledges to uphold the highest standards of data privacy and to continuously work towards maintaining the trust of its clients, employees, and stakeholders.

13.4 Related Documentation

This Data Protection Policy is to be read in the context of the following legislation:

- Law 34/2002 of 11 July 2002 on information society services and electronic commerce ("LSSI").
- Law 11/2022 of 28 June, General Telecommunications Law ("LGT").
- Royal Decree 1720/2007, approving the Regulations implementing the Organic Law on the Protection of Personal Data (hereinafter, "RLOPD").
- Resolutions of the Spanish Data Protection Agency (hereinafter, "AEPD").
- AEPD Legal Reports, Guides and Procedures.
- Rulings of the Audiencia Nacional and/or Supreme Court on data protection.

14.0 CYBER SECURITY POLICY

14.1 Information risk policy

IT security risks threaten the confidentiality, integrity and availability of the Company's information systems, technology infrastructure, data and ultimately, the achievement of business objectives. The Company is currently designing a cyber-security plan seeks to ensure that: There is no disclosure of sensitive, personal and/or confidential information due to inadvertent or intentional misuse of IT systems.

- There is no misuse of IT systems from inappropriate access.
- The impact of potential security incidents can be minimized by incident response and recovery capability.

The Company shall comply with applicable cyber security and information security Laws.

14.2 Access management policy

There are several risks to the Company that could result from inadequate access management protection measures including:

- Unauthorized payments due to inadequate segregation of duties controls.
- Regulatory breach due to inadequate access controls over customer information.
- Reputational risk due to accidental disclosure of sensitive information.

The Company promotes and adheres to proper access management controls by having user authentication controls, password controls, access rights revocation for leavers, segregation of duties and periodic user access reviews.

14.3 Company commitments to cybersecurity

The Company may appoint a number of sub-contractors to discharge its obligations that are responsible for ensuring high standards of onsite and Cyber Security in the management, design, construction, operations, and maintenance of the site.

The Company believes that Cyber Security governance is the responsibility of all involved and shall be promoted as part of a normal culture within the business.

The Company expects its sub-contractors, advisors, and management team's Cyber Security governance to:

1. Regularly assess the risks associated with Cyber activity and implement policies and procedures to manage and protect their systems, networks, and information.

2. Ensure compliance with all relevant legislation

3. Identify the risks, mitigation strategies and procedures associated with:
- Remote system access
- Remote maintenance by individuals or third parties
- Transfer requests
- Vendors and other third parties
- Detection of unauthorised activity

4. Identify and manage the interface with client sharing information or systems and the management processes to ensure there is adequate protection.

5. Provide a written Cyber Security policy and business continuity plan for operations and evaluate and assess its supervisory, compliance and/or other risk management systems, policies and procedures on an on-going basis as Cyber Security threats evolve.

The Company will ask relevant sub-contractors to provide copy of their Cyber Security policies and procedures.

This policy will be displayed at our site office and made available to the Company sub-contractors and advisors.

The Company will review this policy on an annual basis to ensure its suitability and will implementa a security information management system.

15.0 BRANDING

15.1 Company branding

Any new brands must be approved by the Board before launch.

Where a third party is also involved or mentioned in a marketing or a media release, the relevant third party should also approve the relevant parts of the release.

15.2 Marketing

The Company may with approval from its shareholders, refer to them as shareholders of the Company provided that such communication does not state or imply that any shareholder has committed or will commit to any particular investment or opportunity.

The Company shall only promote the concepts, products and ideas previously agreed by the Chief Executive Officer or/and the Marketing Director; and adhere to any marketing guidelines that may be agreed by the Chief Executive Officer from time to time.

The Company shall notify the Board in advance of any material marketing campaign, publication or announcement proposed to be made or published by the Company.

15.3 Staff contact with the media

Any employee of the Company responding to or initiating media contact must have approval from the Chief Executive to do so. Contact with the media includes meetings, phone calls, text messages, emails, other electronic and digital communications methods such as audio or video messaging, social media or website comments and other electronic messaging systems.

Employees must not make unauthorized disclosures of confidential information or any non-approved representations of the Company.

Employees must not (unless required by law) make or publish any comment about the Company that may harm the reputation or public perception of the Company or its shareholders, its clients or staff, or present inaccurate or inappropriate information about the Company or its shareholders.

APPENDIX A – ANTI-BRIBERY AND CORRUPTION POLICY

A.1 General

A.1.1 Application of the policy

This Policy applies to all staff employed or engaged by the Company. The Company staff includes the Company employees and also agency workers, consultants and independent contractors, and directors of the Company.

A.1.2 Responsibility of ensuring adherence to the policy

The management and the Board of the Company have primary responsibility for ensuring adherence to this policy. All the Company staff are required to read, understand and comply with this policy and to follow the reporting requirements set out in this policy or in any associated policies.

A.1.3 Enquiries

Any questions relating to this, or any associated policies should be referred in the first instance to the Board or the Criminal Compliance Committe. If you are in doubt as to the propriety of a situation or proposed act, you should consult with the above at the earliest opportunity. This policy will be reviewed annually by the Criminal Compliance Committee.

A.2 Policy statement

The actual or attempted use of any form of bribery or corruption either directly or indirectly on the Company's behalf to advance its business interests or those of its associates is strictly prohibited.

The Company's involvement in activities which involve bribery and corruption is a key conduct risk faced by the Company, as it may have a negative impact on the Company's reputation, clients or counterparties. This policy is a key control to manage this risk. Bribery and corruption can have a significant, adverse impact on the Company's reputation for integrity as well as on communities where they occur. Bribery can occur in both the public and private sectors. Bribery and corruption are incompatible with the probity and integrity expected of all the Company staff.

This policy sets out requirements and must be read in conjunction with the Company's Risk Management Framework and any associated policies. In the event of a discrepancy or conflict between this policy and associated policies, the more restrictive requirements will apply.

Failure to comply with the requirements in this or any associated policy may result in disciplinary action, up to and including termination of employment or other contractual arrangements.

A.3 Bribery and corruption defined

A.3.1 What is bribery and corruption?

For the purposes of this policy:

A bribe is anything of value given, offered, promised, accepted, requested or authorized (in each case, directly or indirectly) with the intent that a person who is trusted or expected to act in good faith or with impartiality, performs that function improperly or in order to obtain or retain an advantage in the course of business.

Anything of value includes cash, gifts, hospitality, expenses, reciprocal favors, business or employment opportunities, political or charitable contributions and a range of other direct or indirect benefits.

Corruption is the misuse of public office or power for private gain, or misuse of private power in relation to business outside the realm of government.

Acts of bribery or corruption involve the undue influence of an individual in the performance of their duty, whether in the public or private sector.

Indirect benefits can be bribes.

The Company staff must be alert to the possibility that a benefit given or offered to an associate, such as a relative or business partner, or channeled through an agent or other intermediary, may be a bribe. This includes offers of business or employment opportunities. Recklessness or willful blindness to such incidences is likely to be in contravention of applicable laws and/or regulations and will amount to a breach under this policy.

A.3.2 Facilitation payments

Facilitation payments are payments made directly to a government official or employee for their personal benefit, to expedite or secure the performance of governmental action by a governmental agency (e.g., to facilitate the expedition of applications, minor licenses, etc.).

A.3.3 Other conduct

Other behavior which could constitute bribery and corruption includes political or charitable contributions/donations, sponsorship, offsetting arrangements and revolving doors arrangements, where such behavior seeks to improperly influence an individual or organization.

A.4 Types of bribery and corruption

A.4.1 Political and commercial corruption

There are two types of corruption: political corruption and commercial (or corporate) corruption.

Political corruption is the dysfunction of a political system or institution in which government officials, political officials or employees seek illegitimate personal gain through actions such as bribery, extortion, cronyism, patronage and embezzlement.

Commercial corruption occurs when bribes are requested by, or offered to agencies, institutions or individuals to win a contract or gain some other commercial benefit or advantage.

Acts of bribery or corruption commonly, but not always, involve public or government officials, their associates or anyone who is entrusted with power and/or information. Such persons could include (but are not limited to):

- A public official, whether domestic or foreign
- A political candidate, political party, or party official
- A representative of a government-owned or controlled organization
- An employee or representative of a public international organization
- Any other person(s) performing a function of a public nature

Throughout the Company's business dealings, opportunities for the act of bribery or corruption will usually present itself in one of two forms: when dealing with third parties, or when providing or receiving gifts and/or entertainment.

A.4.2 Dealing with and through third parties

Where third parties are engaged to perform services for or on behalf of the Company, their behavior and actions are likely to reflect on the Company, and in some cases the Company will be potentially liable for the acts of those third parties. Third parties performing services on or behalf of the Company must not give, offer, promise, accept, request or authorize a bribe, whether directly or indirectly.

For the purposes of this policy, third parties include intermediaries, agents, representatives, officials, external consultants (political or otherwise), brokers (introducing or otherwise), distributors, vendors, suppliers, contractors, lobbyists/activists or any other third party acting for or on behalf of or providing services to the Company.

It is important that when engaging a third party to act for, or on behalf of the Company, the appropriate steps are taken to ensure their actions and behaviour will not reflect poorly on the Company or expose the Company to potential criminal or other regulatory liability. Among other things, this means that sufficient due diligence must be undertaken on third parties to ensure that they are suitable to be associated with the Company, and that appropriate controls are implemented, designed to prevent and detect bribery and corruption.

For example, particular care must be taken with respect to arrangements with consultants, agents or third parties, who assist in securing business, arrange introductions to key business and government decision-makers, act according to local customs which are incompatible with this policy, or provide services in a higher risk jurisdiction.

Contractual warranties enhanced due diligence, communications, training, monitoring and auditing (e.g., expense reimbursements, especially for gifts and entertainment) should all be considered to ensure the

third parties the Company engages will not bribe or perform a corrupt act on the Company's behalf or for which the Company may be responsible or otherwise liable under anti-bribery or anti-corruption legislation.

A.4.3 Gifts and entertainment

The Company staff must take reasonable steps to avoid, giving or accepting gifts and entertainment that are intended to, or may, improperly influence them or others, or may be perceived to be improperly influencing others. The value of gifts and hospitality should be adjusted to local customs and practices to avoid being perceived as attempts at corruption or bribery. The Company will implement an internal register where gifts received and given, as well as hospitality offered to customers, suppliers and third parties will be recorded and will have an accounting entry to allocate these expenses.

All gifts and entertainment, including gifts or entertainment paid for by cash or personal credit cards which are provided on behalf of the Company, must be of an appropriate amount, does not give rise to any perceived or actual conflict of interest between the Company, its staff, clients or other third parties; and is properly authorized in accordance with the applicable relevant policies of each shareholder.

If you are uncertain whether a gift or entertainment is appropriate, you should consult with the Shareholders Representatives or the Criminal Compliance Committee who can assist you and provide guidance.

A.5 Prohibition on bribery and corruption

The Company staff must not give, offer, promise, accept, request or authorize a bribe, whether directly or indirectly.

Bribery and corruption are illegal under the laws of the jurisdictions in which the Company operates and may expose the Company and individual staff members to criminal penalties, significant fines and imprisonment. Additionally, the relevant staff member may be subject to internal disciplinary action, up to and including termination of employment or other business or contractual relationships.

Bribery and corruption are also incompatible with the general probity expected of all the Company staff.

The Company strictly prohibits the use of facilitation payments, regardless of whether such payments are legal in a particular jurisdiction. This prohibition also applies to third parties acting on the Company's behalf and it is important that this is clearly communicated to any such third party prior to their engagement.

Payments made through official government agency channels which are not for the direct personal benefit of an individual government official or employee (for example, a priority processing fee for a visa as part of a government agency's official tariff) are not examples of bribes, and are not prohibited for the purposes of this policy.

A.6 Acceptable conduct

The Company acknowledges when conducting normal business, staff will from time to time entertain clients, be entertained by service providers, or offer gifts of nominal value in appreciation of work performed. Such activities are acceptable within the boundaries of this and other related policies.

Reasonable expenditure on Company-branded gifts, meals and entertainment is permitted where the expenditure:

- Is for the purpose of general relationship building
- Cannot reasonably be construed as an attempt to improperly influence the performance of a relevant function
- Complies with all applicable laws and regulations
- Is otherwise lawful in the jurisdiction in which the expenditure is made and from which it is paid

It is not possible to be prescriptive as to the types of expenditures that are acceptable. Much will depend on the particular circumstances surrounding the proposed expenditure, its timing and value, including its relative value in the country where it is received. It is a matter that must be approached conservatively. There may also be specific rules relating to government departments, public bodies, private sector organizations and tender processes with which the Company is involved.

The Company should exercise caution regarding political contributions and charitable donations. All such significant activity must be assessed and approved by the Board.

A.7 Steps taken to prevent bribery and corruption

The Company has implement procedures in place to prevent bribery and corruption. The Company must apply controls tailored to manage the risks identified. These controls should include appropriate awareness to ensure the Company staff understand the bribery and corruption risks inherent within their business areas and obtain the necessary approvals for gifts, entertainment, payments relating to public officials, political contributions and charity contributions.

A.8 Reporting bribery and corruption

The Company staff must report suspected or actual instances of bribery or other corrupt practices to the Board or use the internal Whistleblowing channels. The Company staff members who make such reports will be protected from any victimization or detrimental action in reprisal for the making of a report.