OUR COMMITMENT TO INTEGRITY

Who must follow this code?

All employees must adhere to the principles and requirements contained in this code and should consult the code for guidance when acting on behalf of Consortio Security.

Employees must not use a third party to perform any act which conflicts with this code. Employees who engage third parties such as contractors, agents or consultants to work on behalf of Consortio Security must seek to ensure that these parties are made aware of the code and should seek their co-operation in adhering to the code – including, where possible, a contractual requirement to act consistently with the code when working on our behalf. You must report any breaches or inconsistent behaviour by these third parties.
The duties of those who supervise others

Those who supervise others have additional responsibilities under the code. They must:

- Promote compliance and ethics by demonstrating through their behaviour what it means to act with integrity;
- Make sure that those who report to them understand the code's requirements and have the resources to meet them;
- Monitor compliance and ethics of the people they supervise;
- Enforce the code consistently; and
- Support employees who, in good faith, raise questions or concerns.

Your personal commitment to doing the right thing

This code represents a commitment to doing what is right. By working for Consortio Security, you are agreeing to uphold this commitment. Understand the requirements of the code and the standards, instructions and processes that apply to your job – and always follow them. Those who fail to follow the code put themselves, their co-workers, and Consortio Security at risk.

Your duty to speak up

You must report any breaches or potential breaches of Consortio Security's compliance and ethics commitments of which you become aware – whether these relate to yourself, direct reports or others. You must similarly seek advice if you are ever unsure about the proper course of action.

If you are in any doubt about whether to speak up, ask yourself some simple questions:

- Is the action you are concerned about legal?
- Does it comply with the Consortio Security code of conduct?
- Is it in line with Consortio Security's core values?
- Does it expose Consortio Security to any unacceptable risks?
- Does it match our commitments and guarantees that we have made to others?
- What would others think about this action – your manager, colleagues or family?
- How would this look if reported in the newspapers?

- Does it feel right? It may seem easier to keep silent or look the other way. But our commitment to integrity means we must never ignore a legal or ethical issue that needs to be addressed.

Where to go for help

Any employee, who in good faith seeks advice, raises a concern or reports misconduct is following this code and is doing the right thing. Consortio Security takes claims of retaliation very seriously and will not tolerate retaliation against that person. Allegations of retaliation will be investigated and appropriate action taken. Anyone responsible for reprisals against individuals who report suspected misconduct or other risks to the business will be subject to disciplinary action up to and including dismissal.

For legal and business conduct issues a good place to start is your line manager or your HR representative. Your line manager and HR representative will maintain the strictest confidentiality and your concerns will be addressed at a senior level in a fair and consistent manner.

Every effort will be made to give your call a quick response and to deal with your question or concern promptly, especially when circumstances make it time critical.

Review of group compliance & ethics

- All breaches shall be discussed at board level and actions identified to prevent recurrence.
- The board will undertake regular assessment of compliance risks and ensure that internal controls are responsive to these risks.
- Line management will provide support to help employees comply with the code of conduct and applicable laws.
- The board commits to ensure that internal investigation processes remain objective and unbiased.
- The board commits to consistent disciplinary procedures for breaches of the code and the incorporation of compliance and ethics into performance appraisal processes.

HEALTH, SAFETY, SECURITY AND THE ENVIRONMENT (HSSE)

The goals of our business are:

- To prevent all accidents at the workplace;
- To provide a safe and healthy working environment; and
- To eliminate the use of products and practices found to have an adverse effect on people, equipment or the environment.

Consortio Security will achieve our goals by regular reviews of the working environment and empowerment of every staff member, promoting ownership of an individual's responsibilities to HSE throughout the business.

We will develop a policy of co-operation between clients, suppliers, employees and other stakeholders to support our compliance with HSSE legislation.

We will use this co-operation to build a clear structure, effective communication and identifiable training.

We will record the results of risk assessments and of arrangements for the effective planning, organisation, control, monitoring and review of the preventative and protective measures.

This policy statement will be reviewed annually by the board of the Consortio Security.

We will ensure that Health and Safety is maintained as a core value in the organisation.

Simply obeying safety rules is not enough. Consortio Security's commitment to safety means each of us needs to be alert to safety risks as we go about our jobs.

Basic rules you must always follow:

- Comply with the requirements of the law, health and safety management system at your work location, including the use of relevant standards, instructions and processes;
- Stop any work that becomes unsafe;
- Only undertake work for which you are trained, competent, medically fit and sufficiently rested and alert to carry out;
- Make sure you know what to do if an emergency occurs at your place of work;
- Help ensure that your colleagues as well as our contractors and other third parties act in accordance with our health and safety commitments;
- Promptly report any accident, injury, illness, unsafe or unhealthy condition, so that steps can be taken to correct, prevent or control those conditions immediately. Never assume that someone else will report a risk or conditions; and
- If you are unclear about your HSSE obligations or have a concern about a potential or actual breach of health and safety law or internal company policies seek advice.

Never

- Undertake work when your performance is impaired by alcohol or other drugs, legal or illegal, prescribed or otherwise;
- Possess, use or transfer illegal drugs or other substances on company premises; and
- Use threats, intimidation or other violence at work, or bring weapons including those carried for sporting events onto company premises.

Will I be penalized if I stop work when I have concerns about HSSE?

Consortio Security is committed to providing a safe place of work for everyone that includes stopping work if we ever have concerns about HSSE. We will not tolerate retaliation against anyone who in good faith stops work for HSSE issues.

EMPLOYEES

At Consortio Security we seek to build a workplace that is safe, professional, and supportive of teamwork and trust. Everyone who works for Consortio Security contributes to our success and to creating a great company. Working together, drawing from our diverse talents and perspectives, we will stimulate new and creative opportunities for our business.

We are committed to creating a work environment of mutual trust in which diversity and inclusion are valued and where everyone who works for Consortio Security is treated with dignity and respect. Employees will be recruited, selected, developed and advanced on merit, irrespective of race, colour, religion, gender, age, national origin, sexual orientation, gender identity, marital status or disability. They will be entitled to feel included as part of an organisation of people from diverse backgrounds.

We will seek to work in good faith with our employees and their representatives within the appropriate legal framework.

Fair treatment and equal employment opportunity

Consortio Security is a company with approximately 650 employees operating in 3 continents. Our strength is the diversity of our people. Each employee is recognized as an important member of our worldwide team. We respect the rights and dignity of all employees.

Consortio Security aspires to create a work environment of mutual trust and respect, in which diversity and inclusion are valued, and where everyone who works for Consortio Security: -

- Knows what is expected of them in their job;
- Have open, constructive performance conversations;
- Is helped to develop their capabilities;
- Is recognized and competitively rewarded for their performance based on merit;
- Is listened to and is involved in improving team performance;
- Is fairly treated, with respect and dignity, without discrimination; and
- Feels supported in the management of their personal priorities.

Basic rules you must follow:

In support of these aspirations, as a Manager at Consortio Security you must:

Make sure your own decisions regarding recruitment, selection, development and advancement of employees are based on merit, qualifications, demonstrated skills and achievements. Do not allow factors such as race, colour, religion, gender, age, national origin, sexual orientation, gender identity, marital status or disability to influence your judgement.

Follow all applicable labour and employment laws wherever we operate. In some areas where we operate, legal requirements are stringent. Familiarize yourself with any applicable additional local requirements with which you must comply.

As an Consortio Security employee you must:

Report any breaches of which you become aware and seek advice if you have a concern in this area – whether it concerns yourself, direct reports or others.

Forced labour

Consortio Security is committed to the elimination of all forms of forced and compulsory labour. Each Consortio Security employee is expected to be aware of and be alert to any evidence of forced labour abuses in operations linked to our businesses and report them.

At Consortio Security, equal opportunity means just that, a fair chance for everyone.

Respectful, harassment-free workplace

At Consortio Security, we believe every employee is entitled to fair treatment, courtesy and respect. Consortio Security will not tolerate any form of abuse or harassment, in any company workplace, toward employees, contractors, suppliers, customers or others.

Basic rules you must follow:

Never

- Engage in behaviour that could be characterized as offensive, intimidating, malicious or insulting;
- Engage in sexual harassment i.e. unwelcome sexual advances, requests for sexual favours, physical contact or repeated sexual suggestions; and
- Engage in any form of harassment with the intent or effect of:

- Creating a hostile or intimidating work environment, including one in which employees may be driven to engage in inappropriate work practices in order to 'fit in';
- Unreasonably interfering with an individual's work performance;
- Affecting an individual's employment opportunity;
- Humiliate, denigrate or injure another person;
- Make racial, ethnic, religious, age-related, or sexual jokes or insults;
- Distribute or display offensive material, including inappropriate pictures or cartoons;
- Misuse personal information; and
- Spread malicious rumours or use voicemail, e-mail or other electronic devices to transmit derogatory or discriminatory information.

These are just examples. Whatever the form of abuse or harassment, Consortio Security takes it very seriously. It simply has no place in Consortio Security.

Privacy and employee confidentiality

Consortio Security is committed to respecting the confidentiality of our employees' personal information. It is Consortio Security's policy to acquire and retain only employee personal data that is required for the effective operation of Consortio Security, or that is required by law in the places where we operate.

Basic rules you must follow:

- Access to personal data is strictly limited to company personnel who have appropriate authorization and a clear business need for that information. If you do not have authorization or a valid business reason, do not seek access to this information;

- Those with access to personal employee data must only use it for the purpose for which it was collected and adhere to the highest standards of confidentiality in using it;
- Never provide personal employee data to anyone inside or outside of CE Security without proper authorization;
- Personal data must not be held longer than necessary to meet the legal or business reason for which authorization was given; and
- There may be legal restrictions on moving personal data outside the country of origin.

Personal data, information or electronic communications created or stored on company computers or other electronic media such as hand-held devices are not private. Records of your electronic communications may be made and used for a variety of reasons, and may be subject to monitoring or auditing at any time and without notice. Keep this in mind and exercise care when you use company electronic media. Consistent with its respect for employee privacy, Consortio Security does not normally take an interest in personal conduct outside of work unless such conduct impairs the employee's work performance or affects the reputation or legitimate business interests of Consortio Security.

Business partners

At Consortio Security we believe that business relationships founded on trust and mutual advantage, where both sides benefit are vital to our success. We will strive to create mutual advantage by understanding the needs of our customers, contractors, suppliers and conducting ourselves honestly, responsibly and fairly. Our continued success globally depends on competing aggressively, but we will do so fairly and in full compliance with the law.

RECEIVING AND GIVING GIFTS AND ENTERTAINMENT

The exchange of gifts and entertainment can build goodwill in business relationships, but some gifts and entertainment can create improper influence (or the appearance of improper influence). Some can even be seen as bribes that tarnish Consortio Security's reputation for fair dealing or break the law. 'Gifts and entertainment' means anything of value, e.g. discounts, loans, favourable terms on any product or service, services, prizes, transportation, use of another company's vehicles, use of vacation facilities, stocks or other securities, participation in stock offerings, home improvements, tickets, and gift certificates.

Gifts and entertainment between Consortio Security employees and others fall into three categories

- Those that are usually acceptable and that you may approve yourself;
- Those that is never acceptable; and
- Those that may be acceptable but require prior approval.

Usually acceptable self-approval test

Some gifts and entertainment are sufficiently modest that they do not require prior approval. Subject to your applying a 'self-approval test' (see below), the following are usually acceptable without prior approval:

- Meals: modest occasional meals with someone with whom we do business;
- Entertainment: occasional attendance at ordinary sports, theatre and other cultural events; and
- Gifts: gifts of nominal value, such as pens, calendars, or small promotional items.

Self-approval test

In addition to applying the principles above, ask the following questions to determine whether a gift or entertainment is appropriate:

- Intent – Is the intent only to build a business relationship or offer normal courtesy, or is it to influence the recipient's objectivity in making a business decision?
- Materiality and frequency – Is the gift or entertainment modest and infrequent or could it place you (or the other party) under an obligation?
- Legality – Are you sure that the gift or entertainment is legal both in your country and in the country of the third party?
- Compliance with the other person's rules – Is the receipt of gift or entertainment allowed by the recipient's organisation? Special care must be taken when dealing with government officials as many countries do not allow officials to accept gifts or entertainment.
- Transparency – Would you be embarrassed if your manager, colleagues or anyone outside Consortio Security became aware? If so, there is probably something wrong.
- Hypocrisy – Are you adopting double standards? We should only offer what we would be comfortable to accept (and vice versa).

Always unacceptable

Other types of gifts and entertainment are simply wrong. These are never permissible, and no one can approve them. These are:

- Any gift or entertainment that would be illegal (anything offered to a government official in breach of local or international bribery laws);
- Gifts or entertainment involving parties engaged in a tender or competitive bidding process;
- Any gift of cash or cash equivalent (such as gift certificates, loans, stock, stock options);
- Any gift or entertainment that is a 'quid pro quo' (offered for something in return);

- Any entertainment that is indecent, sexually oriented, does not comply with Consortio Security's commitment to mutual respect or that otherwise might adversely affect Consortio Security's reputation; and
- A gift or entertainment that you pay for personally to avoid having to report or seek approval for.

May be acceptable with prior approval

For anything that does not fit into the other categories, the gift or entertainment may or may not be permissible. You must get approval from your line manager or chief operating officer (COO) as appropriate for the following:

- Entertainment that exceeds the lower of

a) £150 or
b) The limit set by Consortio Security management.

- Gifts valued at more than £25
- Lavish meals that may cost more than £100.
- Special events – such as a World Cup game or major golf tournament (these usually have a value of more than £150).
- Travel or overnight accommodation, as this normally raises the personal benefit to material levels. Any entertainment valued at more than £500 (or gifts over £150) must be approved by the COO. In determining whether to approve something in this category, Consortio Security managers will apply criteria similar to those described in the 'self-approval test'.

In some departments and business units, more restrictive guidelines or rules on gifts and entertainment may apply. Employees must be careful not to accept any gift or entertainment that does not comply with such guidelines or rules.

Gifts and entertainment registers

All business meals, gifts and entertainment – whether accepted or declined by Consortio Security employees must be recorded in the gifts and entertainment register which you use. This does not apply to nominal value items such as promotional material, mementoes or working meals.

What to do if you receive an impermissible gift

It is acceptable to receive a gift that exceeds a designated monetary limit if it would be insulting to decline it, but the gift must be reported to line management who will decide whether it:

- May be retained by the recipient;
- Will be retained for the benefit of Consortio Security;
- Will be sold and the money donated to charity; or
- Will be returned to the donor.

You must immediately return any gift of cash or cash equivalent such as a bank cheque, money order, investment securities or negotiable instrument.

Rules for gifts and entertainment involving government officials

Governments in some parts of the world have substantially more stringent requirements regarding gifts and entertainment, and breaches of these rules can be serious offences. If you deal with a government, make sure you know the rules that apply to your circumstances. Seek legal advice, if in doubt.

It is acceptable to promote, demonstrate and explain the benefits of Consortio Security's services to state-employed decision makers or potential partners provided there is no attempt to bias a decision by offering personal benefits. It is unacceptable to pay for the travel, accommodation or daily expenses of a delegation without prior approval from legal.

If you have questions or concerns about gifts and entertainment policies, contact your line manager.

CONFLICTS OF INTEREST

Consortio Security respects its employees' privacy and therefore does not normally take an interest in personal conduct outside of work. However, when an employee's personal, social, financial or political activities interfere or have the potential of interfering with the employee's loyalty and objectivity toward the group, a 'conflict of interest' may exist that must be satisfactorily resolved. Actual conflicts must be avoided, but even the appearance of a conflict of interest can be harmful, too.

Conflicts of interest can arise in many ways. Here are examples of some of the more common ones.

Outside jobs and affiliations

Outside employment and affiliations can create conflicts of interest. Examples include:

- Having a second job.
- Performing services.
- Serving as a director or consultant.
- Holding a financial interest.

Any of the above relating to a third-party organisation that is a competitor, customer or supplier of services to Consortio Security, may raise a conflict of interest, or the appearance of a conflict of interest. (The same is true if the relationship is with an organisation that is seeking to become a competitor, customer or supplier.) Some arrangements of this kind are never permissible. For example, you must never work or provide services for anyone that you must deal with as part of your job for Consortio Security. For all other relationships with competitors, customers or suppliers that could possibly raise a conflict of interest, you must first disclose it and obtain written approval from your line manager.

Jobs and affiliations of close relatives

The activities of close relatives sometimes can create conflicts of interest, too. If you learn that a 'close relative' works or performs services for a competitor, customer or supplier, you

must promptly notify your line manager to determine if action is required. In general, a relative should not have any business dealings with you, with anyone working in your department, or with anyone who reports to you. In addition, you should never be in a situation where you have the ability to hire, supervise, affect terms and conditions of employment, or influence the management of any close relative, regardless of whether that person is an Consortio Security employee or employed by an Consortio Security contractor. Exceptions require specific approval by your line manager. 'Close relative' means a spouse, partner, parent, stepparent, child, step-child, sibling, step-sibling, nephew, niece, aunt, uncle, grandparent, grandchild and in-law.

Boards of directors

Occasionally, an employee may be asked to serve on the board of directors of another organisation and this can, in some cases, raise a conflict of interest or even a legal issue. Before accepting a position as a board member (including for not-for-profits), always get written approval.

Other relationships

You must also be careful to notify your line manager if you have any other relationships which could create, or appear to create, a conflict of interest.

Investments

Employees and their close relatives need to be careful that their investments do not create conflicts of interest, impairing the employee's ability to make objective decisions on behalf of Consortio Security. Conflicts can occur if investments are made in competitors, suppliers, or customers. Any 'substantial interest' in a competitor, supplier or customer requires the prior written approval of your line manager. A 'substantial interest' means any economic interest that might influence or appear to influence your judgement.

Some investments are always wrong

- Never invest in a supplier if you have any involvement in the selection or assessment of, or negotiations with, the supplier, or if you supervise anyone who has such responsibility.

- Never invest in a customer if you are responsible for dealings with that customer or supervise anyone with such responsibility. Usually, however, whether an investment creates a conflict of interest is a matter of good judgement. When deciding whether an investment might create a conflict, ask yourself these questions:

- Would the investment affect any decisions I will make for my company?
- How would the investment seem to others inside my company, such as my co-workers – would they think it might affect how I do my job for the company?
- How would it look to someone outside the company, such as a customer or shareholder, or even in a newspaper?

If you think you may have a conflict of interest, or that others could possibly believe an activity or relationship you are engaged in is a conflict of interest, you must promptly disclose this to your line manager. Many conflicts of interest can be resolved in a mutually acceptable way, but they must be dealt with. Failure to disclose a conflict may lead to disciplinary action.

COMPETITION AND ANTITRUST

Consortio Security adheres to what are called 'competition' laws in many countries and 'antitrust' laws in others. These are laws that promote or protect free and fair competition around the world. Competition laws prohibit anti-competitive behaviour, such as price-fixing conspiracies.

Facts about competition laws: Competition laws vary around the world

Many countries have laws prohibiting anti-competitive behaviour, so depending on where you work, the laws that apply to you may vary.

They can cover conduct outside the country

Some competition laws such as the US and EU antitrust laws can apply even when the conduct occurs outside the relevant country or countries' borders.

Penalties are severe

In the EU, fines for anti-competitive behaviour can be 10% of a company's global turnover. In the US and UK, individuals convicted of conduct such as price-fixing can receive prison sentences. Around the world countries are developing and enforcing laws on anti-competitive activity.

Careless conduct can break the law

A seemingly innocent business contact such as a lunch discussion with a competitor's sales representative or a business chat at an industry trade association can be viewed as an attempt to send an anti-competitive 'signal' to competitors. In short, even the appearance of compromising activity might be viewed as breaking the law.

Certain arrangements almost always break competition laws, never talk with or exchange information with competitors to:

- Fix prices – this can include setting minimum or maximum prices, or 'stabilizing' prices.
- Fix terms related to price, pricing formulas, credit terms, etc.

- Divide up markets, customers or territories. .
- Rig a competitive bidding process, including arrangements to submit sham bids.

Other activities may raise competition issues so always consult with legal before:

- Entering into joint ventures, mergers, acquisitions and marketing, purchasing or similar collaborative arrangements with competitors.
- Establishing exclusive dealings arrangements (e.g. contracts that require a company to buy or sell only from Consortio Security).
- Tying or bundling together different products or services (e.g. contracts that require a buyer who wants one product also to buy a second 'tied' product).
- Serving as a director or consultant in a company that competes with us.

Trade associations

Trade associations can perform useful and legitimate functions, such as the enhancement of safety within a particular industry. But because trade associations place us in close proximity with our competitors, their membership and activities require us to follow special cautionary guidelines. Employees must not engage in discussions or activities that would lead to the allegation or appearance of improper behaviour. Even passive participation in a meeting where a questionable discussion is taking place can put you and the company at serious risk. If you find yourself in this type of situation, you must make it clear that you believe the discussion is improper, break away from the discussion, and always promptly inform Consortio Security legal. You should consult legal if you are in any doubt about proper behaviour at trade association meetings.

Gathering competitor information

Competition laws can make obtaining competitor information difficult since direct or indirect contact with competitors can have serious legal consequences. However, in order to compete effectively in the global marketplace, it is necessary and, if done correctly, legal to gather competitor information. At Consortio Security we will conduct rigorous, lawful competitor intelligence gathering. We will use only available literature, industry and other publicly available sources to understand business, customer and supplier directions, technology trends, regulatory proposals and developments, and existing and expected courses of suppliers and competitors. Consortio Security will gather this information fairly and legally.

Some forms of information gathering are always wrong, examples include:

- Theft.
- Illegal entry.
- Bribery.
- Misrepresentation of who you are.
- Electronic eavesdropping.

At Consortio Security, we are committed to avoiding even the appearance of improper information gathering. If you even suspect that a piece of competitor information might be considered confidential by the competitor you must check with legal before using the information in any way.

If you have questions or concerns about your responsibilities under the competition laws or whether it is appropriate to accept or have certain competitor information, consult your line manager or legal.

MONEY LAUNDERING

Money laundering is the process by which individuals or entities try to conceal illicit funds, or otherwise make these funds look legitimate. Consortio Security will not condone, facilitate or support money laundering.

Few Consortio Security employees will ever personally be in the position to infringe 'money laundering' laws, but there are two areas which we all need to watch out for:

- Irregularities in the way payments are made.
- Customers who appear to lack integrity in their operations.

Payment irregularities

Consortio Security supports anti-money laundering policies by using procedures to avoid receipt of cash or cash equivalents that are the proceeds of crime. Be wary of:

- Payments made in currencies other than that specified in the invoice.
- Attempts to make payments in cash or cash equivalents.
- Payments made by someone not a party to the contract (unless approved).
- Payments to/from an account other than the normal business relationship account.
- Requests or attempts to make payments for each invoice or group of invoices by multiple cheques or drafts.
- Requests to make an overpayment.

Know your customer guidelines

To help make sure that we only do business with firms that, share our standards of integrity, always:

- Assess the integrity of potential customers and other business relationships.
- Communicate with customers about our compliance expectations of them.
- Continue to be aware of and monitor customers' business practices.
- Do not do business with any customer or other business partner suspected of wrongdoing relating to dealings with us unless those suspicions are investigated and resolved or otherwise approved by legal.

The above are guidelines only and are not a substitute for using good judgement and common sense when assessing the integrity and ethical business practices of customers and business partners. If anything doesn't seem quite right, seems too good to be true, or you feel uncomfortable with any customer or other business relationship, contact your line manager or legal for advice.

Suspicious transactions or activities by any customer must be reported promptly to Consortio Security, who will then be able to give prompt advice to ensure that the transaction is dealt with correctly.

WORKING WITH SUPPLIERS

Consortio Security's suppliers play a critically important role in our ability to operate and provide services to our customers. That is why we must choose suppliers carefully, based on merit, and with the expectation that our suppliers will act consistently with our compliance and ethics requirements.

If your job involves selecting or working with suppliers, keep the following rules in mind:

- Choose suppliers based on merit, avoiding conflicts of interest, inappropriate gifts and entertainment or any other kind of favouritism that might compromise selection.
- Seek to do business with suppliers who comply with legal requirements and who act in a manner that is consistent with Consortio Security's commitment to compliance and ethics as outlined in this code.
- Help our suppliers understand Consortio Security's compliance and ethics requirements.
- Be alert to and report to line management activity by suppliers that is inconsistent with those requirements.
- Be careful not to give one supplier's confidential business information (proposed rates, winning bid information, etc.) to another.

GOVERNMENTS AND COMMUNITIES

Places where we operate should properly benefit from our presence through the wealth and jobs created, the skills developed within the local population and the investment of our time and money in people. We will work towards improvements that are measurable and contribute to the real, independent growth of communities where we operate. We will not engage in bribery or corruption in any form and are committed to transparency in all our dealings. We will not participate in partisan political activity, make no political contributions in any country and seek to form a constructive and productive relationship with all branches of the media.
Bribery and corruption

Bribery means giving or receiving an undue reward to influence the behaviour of someone in government or business to obtain commercial advantage. A breach of law that prohibits corruption is a serious offence which can result in fines for companies and imprisonment for individuals. Even the appearance of a breach of anti-bribery or anti-corruption laws could do incalculable damage to Consortio Security's reputation. Anti-bribery and anti-corruption laws:

- Apply to Consortio Security employees.
- Forbid making, offering or promising to make a payment or transfer anything of value, including the provision of any service, gift or entertainment, to government personnel and other officials for the purpose of improperly obtaining or retaining business, or for any other improper purpose or business advantage.
- Forbid making improper payments through third parties, Consortio Security personnel must therefore be diligent in selecting and monitoring contractors, agents and partners.
- Require that companies keep accurate books and records so that payments are honestly described and company funds are not used for unlawful purposes.

Employees must never:

- Offer or make an unauthorized payment, or authorize an improper payment (cash or otherwise) to a local or foreign official, or any related person or entity;
- Attempt to induce a local or foreign official to do something illegal;
- 'Shrug off' or fail to report any indication of improper payments;
- Offer or receive money (or anything of value), gifts, kickbacks or commission, in relation to obtaining business or awarding contracts;
- Establish an unrecorded 'slush' fund for any purpose;
- Do anything to induce or facilitate someone else to break these rules; or
- Consortio Security does not permit 'facilitation' or 'grease' payments to be made to government officials, even if such payments are nominal in amount. ('Facilitation payments' are payments made to secure or speed up routine legal government actions).

Commercial bribery

Bribery of government officials is a serious matter, but bribery of those working in the private sector is also often illegal and always against our own standards of business conduct. You may have worked previously for, or have colleagues at, another company that allows facilitation payments to be made. Consortio Security does not.

Dealing with regulators

Being transparent in our communications about our performance (whether good or bad) increases trust in our activities, and makes others wish to do business with us. If during the course of your employment you are asked to provide information in connection with a regulatory agency enquiry or investigation, you must make sure that any information you provide is truthful and accurate, and that Consortio Security's legitimate interests are protected. Always seek advice from legal and your line manager before responding to a non-routine request for information from a regulatory agency.

Never

- Mislead any investigator or regulatory official.
- Attempt to obstruct in any manner the collection of information, data, testimony or records by properly authorized regulatory officials.
- Conceal, alter or destroy documents, information or records that are subject to an investigation or enquiry.
- Attempt to hinder another employee from providing accurate information.
- Retaliate against anyone who co-operates with regulatory agencies.

Always

- Co-operate courteously with officials conducting a regulatory agency enquiry or investigation. However, where the request is non-routine, notify and seek advice from legal and your line manager before responding.
- Make sure that records and information relevant to any regulatory agency enquiry or any litigation are preserved. Make sure that any automatic systems, including

electronic systems, for record disposal are stopped to avoid destruction of relevant records and information relating to such circumstances.

COMMUNITY ENGAGEMENT

At Consortio Security we seek to engage in open and transparent dialogue and consultation with communities and other representatives such as Non Government Organisations (NGOs).

Basic rules you must always follow:

- Comply with local laws and regulations in each community and country in which you work.
- Respect the cultures and varying business customs of those communities and countries (as long as they do not conflict with the principles in this code).
- Seek to recruit qualified local personnel, where practical.

- Notify contact with designated international NGOs to your line manager in advance of engaging in dialogue. We encourage employee participation in support of local community development initiatives and civic causes so long as there is no conflict of interest.

External communications

Investors, analysts and the media External communications with these audiences require careful consideration and a unique understanding of legal and media issues. Only those employees specifically authorized to do so may respond to enquiries from members of the community.

- Take advice before talking about company matters with a reporter or analyst, either on or off the record.
- Report enquiries promptly to Consortio Security and take advice before responding.

External speaking engagements

Statements of Consortio Security's existing financial position and forward-looking financial statements may be
made only by properly authorized officers of the company.

Political activity

Consortio Security's approach on corporate political participation is very simple and applies everywhere we do business, therefore:

- The company will not participate directly in party political activity.
- The company will make no political contributions, whether in cash or in kind, anywhere in the world.

In terms of personal political activity Consortio Security recognizes employees' rights to participate as individuals in the political process, in ways that are appropriate to each

country. However, you must be careful to make clear that you do not represent the company as you participate in the political process. Therefore:

- Do not use company time, property or equipment to carry out or support your personal political activities. In short, engage in the political process in your own time and with your own resources.
- Always make clear that your views and actions are your own and not Consortio Security's.
- If you plan to seek or accept a public office, notify your manager in advance. You should discuss whether your official duties might affect your work and work constructively with your manager to minimize any adverse impact on your job.

Lobbying/advocacy

Although Consortio Security will not directly participate in party politics, the company will continue to engage in policy debate on subjects of legitimate concern to the group, its staff and the communities in which it operates, if you are in doubt as to whether an activity is appropriate, or might be subject to misinterpretation contact your line manager.

COMPANY ASSETS AND FINANCIAL INTEGRITY

We have the responsibility as well as a legal duty to protect the physical, intellectual property and financial assets of Consortio Security. We will be forthright and transparent about our operations and performance, accurate in the recording and reporting of data and results, and exercise care in the use of our assets and resources.

Accurate and complete data, records, reporting and accounting

Honest, accurate and objective recording and reporting of information whether financial or non-financial is essential to:

- Consortio Security's credibility and reputation.
- Meeting Consortio Security's legal and regulatory obligations.
- Meeting Consortio Security's responsibility to its stakeholders.
- Informing and supporting our business decisions and actions.

All data that Consortio Security employees create whether financial or non-financial must accurately reflect transactions and events.

Financial data must conform to generally accepted accounting principles. Failure to keep accurate and complete records is not only contrary to Consortio Security policy but also may break the law. There is never a justification or an excuse for falsifying records or misrepresenting facts. Such conduct may constitute fraud and can result in civil and criminal liability for you and for Consortio Security.

Other data (e.g. HSSE performance, quality data, regulatory filings and other essential company information) must also be accurate and complete. This is true whether the data is in paper documents, computer-based or any other medium that contains information about Consortio Security or its business activities. Again, both our own company standards and, in many cases, legal standards, require it.

Therefore always:

- Ensure all transactions are properly authorized and accurately and completely recorded.
- Follow all laws, external requirements and company processes for reporting information, which apply in the jurisdiction(s) where your actions are recorded.
- Ensure that no undisclosed or unrecorded account, fund or asset is established or maintained.
- Co-operate fully with our internal and external auditors, provide them with accurate information and on request allow them unrestricted access to staff and documents (subject to legal constraints).
- Show financial integrity in submitting or approving expense claims.

Never:

- Deliberately make a false or misleading entry in a report, record or expense claim.
- Falsify any record, whether financial or non-financial (e.g. safety, environmental or quality results).
- Sell, transfer or dispose of company assets without proper documentation and authorization.
- Try to influence others to do anything that would compromise the integrity of Consortio Security's financial records or reports.
- Commit Consortio Security to contractual obligations which are beyond the scope of your delegated authority.

Falsifying or creating misleading information can constitute fraud and, simply put, fraud of any kind will not be tolerated.

Senior financial officers and others responsible for the accuracy of financial reporting have an additional responsibility to ensure that proper controls are in place to achieve truthful, accurate, complete, objective, consistent, timely and understandable financial and management reports. The applicable external and internal reporting standards as set out in the group reporting manual must be followed at all times.

Record retention

Documents and records must be retained in accordance with the law and our record retention guidelines.

Never:

- Conceal, alter, destroy or otherwise tamper with: company records or documents except as authorized in accordance with established standards and guidelines; Documents relating to actual, pending or threatened litigation and government/regulatory investigations, or in circumstances where there is reason to believe such litigation or investigation is reasonably likely to occur in the future.
- Remove or destroy records prior to the specified date without first obtaining permission.
- Destroy records you are uncertain about the validity of any entry or financial process.

If you believe you are being asked to create any false or misleading entry, data or report (whether financial or non-financial or for internal or external use). You must promptly report such concern or incident, or seek advice regarding the matter from:

- Your line manager or financial controller if you have doubts about how to record a transaction properly.
- The finance department if this does not resolve the concern.

If you are worried that a transaction is being, or has been, improperly recorded, you must promptly report this to the finance department. Your prompt reporting will enable early management intervention to take place.

Protecting Consortio Security's assets

All employees are responsible for using good judgement to ensure that Consortio Security's assets are not misused or wasted. These assets include property, time, proprietary information, corporate opportunities and company funds, as well as personal company equipment.

Company property

You are individually responsible for ensuring that Consortio Security property that you use or come into contact with as part of your work is not damaged, misused or wasted. You also have a duty of care to report the abuse of Consortio Security property by others. You must not use any company equipment or facilities for your personal activities except in the very limited circumstances.

Portable or home-working equipment that is issued to you (for example, laptops and mobile phones) remains the property of Consortio Security. You must take reasonable care of it as you would other Consortio Security

property: ensuring that it is not damaged, abused, wasted, lost or exposed to unnecessary risk of being stolen.

Company time

Whilst at the workplace you are expected to be fully engaged in your work and not undertaking personal activities. Devote the necessary time to your work in order to fulfil your job responsibilities. Those required to report their hours worked must do so truthfully and accurately.

'Intellectual property' and other protected information

At Consortio Security we regularly produce valuable, non-public ideas, strategies and other kinds of business information 'intellectual property' which we own and need to protect just as we do with other kinds of property. Because it is the product of Consortio Security's own hard work, various laws allow Consortio Security to protect this information from use by outsiders.

Intellectual property includes:

- Patents.
- Copyrights.
- Trademarks and service marks.
- Other kinds of confidential business information such as: Sales, marketing and other corporate databases.
- Marketing strategies and plans.
- Research and technical data.
- Business ideas, processes, proposals or strategies.
- Software bought or developed by the company.
- Information used in trading activities including pricing, marketing and customer strategies.

In addition, other confidential business information, such as personnel lists and customer data, must also be protected. Always protect and never disclose any confidential Consortio Security intellectual property or any other confidential information. This is to ensure that we reap the benefits of our own hard work and keep our commitments to others. These obligations apply throughout your employment and continue after your employment ends. Instructions for classification and protection of information are given in the Security of information standard. On occasion, we may need to share Consortio Security intellectual property with persons outside of Consortio Security for example, so that a third party can work effectively with us. However, even when there seems to be a legitimate reason to share proprietary information, you should never disclose such information without management's prior approval and then only under a written confidentiality agreement approved by legal.

Corporate opportunities

Employees owe a duty to Consortio Security to advance Consortio Security's legitimate business interests when the opportunity arises. Never use Consortio Security property, information, or position for personal gain.

Company funds

Always protect Consortio Security's funds as you would your own: guarding against misuse, loss, fraud or theft. This includes company monies advanced to you and any company travel and entertainment, procurement or credit cards you may hold. Make sure that all claims, vouchers, bills and invoices are accurate and submitted in a timely manner.

Intellectual property and copyright of others

Just as we protect our own business information, we are committed to respecting the intellectual and protected information of others. Basic rules you must follow:

- Do not bring to Consortio Security or use any confidential information, including computer records, from prior employers.
- Seek advice from legal when assigning work to a new employee if there is a risk that the employee might use protected information from a prior employer.
- Do not load any unlicensed software on any Consortio Security computer.

- Do not accept or use anyone else's confidential information except under an agreement approved by legal.
- Only copy documents and materials (including computer software) that are not copyrighted (for example, a government report) or when you have specific permission to do so.
- Do not use copyrighted materials or third-party trademarks (for example, portions of audio, video and off-the-internet or off-the-air recordings) in materials you are producing (including internet or intranet web sites) without specific permission from the copyright owner. Consult legal on whether 'fair use' may allow the use of brief excerpts.
- Do not knowingly infringe a valid patent of another party.
- You are; of course, free to gather competitor information from legitimate public sources.

DIGITAL SYSTEMS USE AND SECURITY

Digital systems and the information processed and stored on them, are critical to our company. Everyone who uses digital systems; employees, contractors, consultants and other people with temporary access must ensure that these resources are used appropriately and in line with relevant security policies. Effective security is a team effort requiring the participation and support of everyone who deals with Consortio Security's information or digital systems.

Computer hardware and software and all information on Consortio Security digital systems, as well as any Consortio Security information on your home or other non- Consortio Security digital systems, are company property. Therefore, use company digital systems responsibly and primarily for the business purposes for which they are intended. Do not load software onto an Consortio Security digital system unless you know this is approved.

Personal use must not:

- Displace any business activity.
- Consume more than a trivial amount of network or other Consortio Security resources (e.g. downloading large files or accessing streaming audio or video for personal use are considered digital systems misuse).
- Interfere with your productivity or the productivity of others doing Consortio Security work.
- Include soliciting other users or conducting any non- Consortio Security business enterprise.
- Damage the company's reputation.

Never use company electronic communications systems to transmit without authorisation:

- Confidential data about individuals.
- Confidential company information.
- Copyrighted or licensed materials.

Never deliberately access, store, send, post or publish: Pornographic, sexually explicit or sexually exploitative images or text or any materials promoting violence, hatred, terrorism or the intolerance of others.

Any material that is harassing, obscene, abusive or inconsistent with Consortio Security's non-harassment and equal opportunity policies is strictly forbidden.

In the event that you receive inappropriate unsolicited material – e.g. through e-mail spam – forward it to the IT department and delete it immediately. If the company identifies obscene material on company digital systems or premises, or other behaviour which is inconsistent with policy, not only will disciplinary action be taken, management may also notify civil and/or criminal authorities. Under Consortio Security's privacy and data protection policies and within the bounds of law, Consortio Security may access and monitor computer files and electronic communications stored on company servers, PCs and other devices for maintenance, business need or to meet a legal or policy requirement.

Digital resources are used for business purposes 24 hours a day, seven days a week. Personal use, especially in today's resource and content rich websites, does strain the system. You must run your 'home' business at home.