SK SECURITY
Services LTD

Data Protection & GDPR Policy

Data Protection

In order to operate effectively and fulfil its legal obligations SK SECURITY SERVICES LTD needs to collect, maintain and use certain personal information about current, past and prospective employees and other individuals with whom it has dealings. All such personal information, whether held on computer, paper or other media, will be obtained, handled, processed, transported and stored lawfully and correctly, in accordance with the safeguards contained in the Data Protection Act 2018 (DPA)- including GDPR.

Data Protection Principles

All personal data must be processed in accordance with the eight Data Protection Principles. The essence of these principles is set out below together with brief, non-exhaustive practical examples of when these principles may have relevance to you.

Personal data must: -

- Be processed fairly and lawfully;
- Be obtained only for one or more specified or lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- Be accurate and, where necessary, kept up-to-date;
- Staff must notify changes of name, address, telephone number, bank and marital status to the HR Department soon as possible. The HR Department will endeavour, periodically, to ask staff to confirm that such personal data held by the Company is accurate. Staff should advise the Company of any changes to their contact details or to any other details that may be of relevance.
- Not be kept for longer than is necessary
- Be processed in accordance with the rights of data subjects.
    - For example, employees have a right of access to the information that the Company holds about them. Upon receipt of a written or email subject access request the Company shall disclose all the information that it is required to do so by law.
    - If any member of staff receives any letter from a customer, business contact, other employee, or any other third party requesting any information about them then they must pass the letter to the Data Protection Officer.
    - Employees should, if they are making a subject access request of the Company, send their access request to the Director.
    - Access to personal data must be restricted to authorised individuals for approved purposes

SK SECURITY
Services LTD

Data Protection & GDPR Policy

- Be protected by appropriate technical and organisational measures against unauthorised or unlawful processing, against accidental loss or damage.
  - The Company may take steps to put in place technical methods (i.e. firewalls, encryption, password protection, etc.) or organisational methods (hierarchy of access to personnel files, locking cabinets etc.) of protecting personal data where the importance of the personal data makes this appropriate.
  - All employees who have access to personal data controlled by the Company whether or not on computer, and whether in the office or at home or elsewhere, must take adequate precautions to ensure confidentiality so that neither the Company, nor any individual employed by the Company, becomes exposed to criminal or civil liability as a result of the loss, destruction or disclosure of personal data. All individuals must fully comply with all Company procedures and requirements in this regard.
  - Staff should ensure the security of data at all times. Staff must not leave personal data on screen or on desk tops when they are not at their desks. Paper records should be stored securely unless under active consideration. A clear desk policy should be observed.
- Not be transferred to a country or territory outside the European Economic Area unless there is a clear legal basis in the Act for making the transfer.

Data Processing

Personal data provided by or about an individual to the Company will be processed in accordance with the Act. Data about an individual will only be processed for lawful and fair purposes. The Company is the legal person who determines the manner in which and the purposes for which personal data may be used. The Data Protection Officer who has the main responsibility internally for managing data protection issues and compliance in the Company is the Director. Personal data about an individual will be processed for various purposes which may include:

- to assess his/her application to become an employee;
- to administer the contractual sick pay system;
- to address any health and safety issues;
- to facilitate management decisions;
- to detect fraud;
- to administer any personal health insurance benefit or other similar benefit;
- to administer the employment relationship so that the Company may properly carry out its duties, rights and obligations to the employee. Such processing will principally be for HR, administrative, regulatory or payroll purposes.

Sensitive Personal Data

Certain personal data is given special status in data protection legislation. This personal data is called sensitive personal data. Sensitive personal data is personal data consisting of information as to:-

SK SECURITY
Services LTD

Data Protection & GDPR Policy

- racial or ethnic origin.
- political opinions.
- religious beliefs (or other beliefs of a similar nature).
- trade union membership
- physical or mental health
- sex life
- commission or the alleged commission of an offence.
- proceedings for any offence, the disposal of such proceedings or the sentence of any Court in such proceedings.

Subject to the exceptions set out below and elsewhere in this procedure, sensitive personal data shall generally only be processed after the employee has given express consent. The Company may in certain situations process the data without your consent if it is necessary for processing taking place for one of the following purposes: -

- ensuring health and safety of employees;
- ensuring a safe working environment;
- maintaining records of statutory sick pay or maternity pay;
- protecting the person and property of people entering on to the company premises or customer site;
- carrying out any other obligation or enforcing any right under employment law;
- Participating in legal proceedings or obtaining legal advice.
- For the administration of justice.
- For medical purposes by a health professional.

Sensitive personal data relating to racial or ethnic origin may be processed without express consent in order to SK SECURITY SERVICES LTD the effectiveness of the Company's Race Equality Policy and Procedure. The Company may also process such sensitive personal data about you without your explicit consent where it is otherwise entitled to do so by virtue of a condition under Schedule 3 to the Act.

Requests for Information

Employees about whom the Company holds personal data has the right to be:

- told whether their personal data is being processed by or on behalf of the Company and, if so, to be given a description of:

SK SECURITY
Services LTD

Data Protection & GDPR Policy

i. the personal data held;

ii. The purposes for which it is being processed and;

iii. The recipients of the personal data

- given a copy of the personal data in an intelligible format (unless to do so is disproportionate or the person has agreed to an alternative way of providing access)
- given any information available regarding the source of the personal data

For any subject access request. Written requests should be directed to the Director. If you are a member of staff and you receive a written request, then you should forward this to the Director immediately. The request for information will be dealt with promptly and in any event within 30 days from the Company receiving:

- the written request for the personal data;
- sufficient details to allow the Company to respond to it;
- sufficient details to confirm the identity of the person making the request; and

Where the provision of information would reveal the identity of a third party, the information may not be provided unless either the consent of that third party is obtained or it is reasonable to proceed without their consent. All requests for access to personal data must be made in writing (which includes e-mails). You should be aware that where access requests are made via e-mail and the Company need not respond until it is satisfied as to the identity of the individual making the request. Personal information relating to employees cannot normally be disclosed to an unauthorised third party. These include family members (see Para 25 below), friends, local authorities, government bodies and the police. There are only certain circumstances when personal information can be given to such third parties and these include:

- prevention or detection of a crime
- apprehension or prosecution of offenders
- prevention of serious harm to a third party
- protection of the vital interests of the data subject, e.g. release of medical data where failure could result in serious harm or death
- ensuring health and safety.

Employees have the right to expect documentary evidence to support such requests.

Management of Personal Data

Where we take any decision which significantly affects any member of staff exclusively upon the results of an analysis of his/her personal data carried out by automated means then we will provide that person with notice of this fact as soon as reasonably practicable thereafter. If the decision is

connected with a contract entered into between the Company and another person or is taken for the purposes of considering whether to enter into or with a view to entering into such a contract, the other person will be allowed to make representations on the outcome of that decision (perhaps as part of a formal grievance procedure).

In the event of a potential intended or actual transfer of a business, the Company will take all reasonable steps to limit disclosure of personal data about employees to any of the third parties concerned by for instance, the omission of names or other identifying particulars. However, staff should be aware that some personal data such as name, address, position, salary levels may be transferred to a prospective operator (or other similar party) of any part of Company operations as part of a due diligence process. Where this happens, the Company will place contractual obligations on the prospective operator to keep the staff's information safe. The transferee shall cease to be a third party on the date of the formal transfer, except in respect of the personal data concerning certain rights and obligations such as those relating to pensions – not required under the Transfer of Undertakings (Protection of Employment) Regulations 2003 as amended by the Trade Union Reform and Employment Rights Act 1996.

Responsibilities

We expect all employees to use computers, email and the Internet responsibly and in accordance with the data protection principles. You should make yourself aware of the provisions contained in the Company's IT Policy. Employees are expected to adhere to this procedure and to ensure that those for whom they are responsible both adhere to this policy and protect computer systems and personal data from security risks. Where necessary, managers should seek advice from the IT Department to assist in these goals.

Employees must become familiar with the aims of this procedure and follow the guidelines set out. In particular Employees should:

- Seek advice from the Director where they have an doubts as to whether or not the processing of personal data that they require to carry out in the course of their employment complies with the Act;
- Not use personal information that they hold in the course of their employment for any reason other than the performance of their employment duties. To procure personal information from the Company and use it without its consent is likely to constitute a criminal offence under the Act;
- Provide all assistance to the Director in the conduct of any audit or preparing a response to a subject access request;
- Keep information that you process for the Company safe and secure in accordance with any procedures issued by the Company. Where no procedures are set out explicitly, you should exercise a degree of care over the personal data that you process by considering the harm

SK SECURITY
Services LTD

Data Protection & GDPR Policy

that may result were the information to be disclosed unintentionally. Guidance on appropriate levels of security can be obtained from the Director.

- Not keep duplicate records relating to Employees or students for the purposes of our employment where a centralised filing option is available. Keeping your own records unnecessarily can complicate the process of responding to subject access requests.
- Notify the Director immediately should you detect any potential or actual breach of the Act.

Security

Any breaches of this Procedure in relation to personal data security will result in disciplinary action and, in serious cases, may result in the dismissal of an employee of the Company.

Employees will be authorised to gain access to certain computer systems, programs and data. No employee must attempt, alone or with others, to gain access to data or programs to which they have not been authorised to gain access. Employees must not disclose personal details of other Employees to unauthorised third parties where this information is personal data in respect of which the Company is the data controller.

Training

Employees will receive training on the importance of Data Protection during their induction training, and further reminders will be given during the monthly supervisor visits. This policy will be used to SK SECURITY SERVICES LTD the employee's awareness of the Data Protection Act, so further training needs can be identified.

SK SECURITY
Services LTD

Protection of the Public Policy

SK SECURITY SERVICES LTD recognises its responsibility to the wider community and the role it has to play in protecting the public.

All of our officers are empowered to report suspicious activity and behaviour to the police.

There is also an expectation that if in the course of their day to day duties our officers see evidence of criminal activity or anti-social behaviour, they will either report it directly to the local police or do so via their control centre. In the event that they do identify such incidents the officers are instructed they must not put themselves at risk of harm or injury. The officers have also received a similar instruction if they identify vulnerable people that may require protection to ensure their safety.

Members of the management team will encourage all employees to get awareness training in ACT. This is a NCTSO (The National Counter Terrorism Security Office) led initiative which asks businesses and other organisations to consider their preparedness for terrorist attack. It explores what is likely to happen in the event of a terrorist attack and identifies the measures that can assist in preventing, handling and recovering from such an incident.

Our Security Guards are trained to identify vulnerable people and know what steps to take to protect them. The aim is to enable Security staff to support police in taking an active role in ensuring the safety of the public.

Signed A Singre Position DIRECTOR Date 1/3/2018

SK SECURITY
Services LTD

Modern slavery Policy statement

This policy sets out the organisation's stance on modern slavery and explains how employees can identify any instances of this and where they can go for help. This statement is made pursuant to s.54 of the Modern Slavery Act 2015 and sets out the steps that SK SECURITY SERVICES LTD has taken and is continuing to take to ensure that modern slavery or human trafficking is not taking place within our business or supply chain. Modern slavery encompasses slavery, servitude, human trafficking and forced labour.

SK SECURITY SERVICES LTD has a zero-tolerance approach to any form of modern slavery. We are committed to acting ethically and with integrity and transparency in all business dealings and to putting effective systems and controls in place to safeguard against any form of modern slavery taking place within the business or our supply chain.

Our suppliers

SK SECURITY SERVICES LTD operates a supplier policy and maintains a preferred supplier list. We conduct due diligence on all suppliers before allowing them to become a preferred supplier. This due diligence includes an online search to ensure that particular organisation has never been convicted of offenses relating to modern slavery [and on-site audits which include a review of working conditions]. Our anti-slavery policy forms part of our contract with all suppliers and they are required to confirm that no part of their business operations contradicts this policy.

In addition to the above, as part of our contract with suppliers, we require that they confirm to us that:

1. They have taken steps to eradicate modern slavery within their business

SK SECURITY
Services LTD

2. They hold their own suppliers to account over modern slavery
3. (For UK based suppliers) They pay their employees at least the national minimum wage / national living wage (as appropriate)
4. (For international suppliers) They pay their employees any prevailing minimum wage applicable within their country of operations
5. We may terminate the contract at any time should any instances of modern slavery come to light
6. **Training**

We regularly conduct training for our procurement/buying teams so that they understand the signs of modern slavery and what to do if they suspect that it is taking place within our supply chain.

Our performance indicators

We will know the effectiveness of the steps that we are taking to ensure that slavery and/or human trafficking is not taking place within our business or supply chain.

Signed A Nagra Position DIRECTOR
Date 1/3/2018

SK SECURITY
Services LTD

Services LTD

Business Ethics Policy

SK SECURITY SERVICES LTD believes that it is important for SK SECURITY SERVICES LTD its employees to maintain high ethical standards in order to preserve its reputation in the marketplace. Good ethics are important to ensure that SK SECURITY SERVICES LTD meets not only its objectives in a fair and equitable manner but its wider social responsibilities externally. In addition, SK SECURITY SERVICES LTD is committed to ensuring high ethical standards within the workplace.

The procedure that follows provides general guidance on ethics and refers to other policies of SK SECURITY SERVICES LTD where necessary. The procedure will be closely monitored and will be developed as necessary to ensure that it meets the needs of the SK SECURITY SERVICES LTD, its employees and its stakeholders.

We will ensure that SK SECURITY SERVICES LTD is meeting its aims with regard to social impact and ethical behavior and that its stakeholders perceive SK SECURITY SERVICES LTD in a positive light.

Procedure

1. All employees will be provided with ethics training as part of the induction program. Ongoing ethics training, as the ethics policy and procedure develops, will be cascaded to employees via management.

2. All employees are required to adhere to the SK SECURITY SERVICES LTD policy and procedure on business ethics. Employees who breach SK SECURITY SERVICES LTD policy on business ethics will be subject to disciplinary action up to and including dismissal.

3. Employees who are faced with a potential breach of the business ethics code or have doubts about an ethical choice they are facing should, in the first instance, speak to their line manager.

4. SK SECURITY SERVICES LTD has a Code of Conduct which employees are expected to abide by. A copy of the Code of Conduct and other policies relevant to this procedure are available on in the Staff Handbook

5. The following areas are included in this procedure. However, this list is not exhaustive and will be developed as required.

    1. Data protection/Access to employee data.

2. Whistleblowing.
3. The giving and receiving of gifts.
4. Confidentiality.
5. Relationships with competitors, suppliers, advertisers, etc.
6. Equal opportunities, discrimination and harassment.
7. Moonlighting.
8. The environment.

6. SK SECURITY SERVICES LTD adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

- Process personal data **fairly, lawfully and in a transparent manner.**
- Obtain personal data only for one or more **specified** and **lawful purposes** and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
- Ensure that personal data is **adequate, relevant and not excessive** for the purpose or purposes for which it is held.
- Ensure that personal data is **accurate** and, where necessary, **kept up-to-date.**
- Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
- Ensure that personal data is kept secure.
- Ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

SK SECURITY SERVICES LTD employees should ensure that they understand how data protection impacts on their particular role, in particular with regard to external suppliers and customers. Employees who have any questions on the SK SECURITY SERVICES LTD Data Protection/Access to Employee Data policy should speak to their manager in the first instance.

7. SK SECURITY SERVICES LTD encourages a free and open culture in its dealings between its officers, employees and all people with whom it engages in business and legal relations. SK SECURITY SERVICES LTD recognizes that effective and honest communication is essential if malpractice is to be effectively dealt with and SK SECURITY SERVICES LTD success ensured.

8. SK SECURITY SERVICES LTD does not believe that the giving and receiving of gifts from suppliers and customers is appropriate. In certain

circumstances gifts may constitute a bribe. An employee who receives a gift from a customer or supplier, regardless of its value, must inform his or her manager who will decide whether the gift may be kept by the employee or whether it should be returned.

9. A confidentiality clause forms part of all employees' statement of particulars/contracts of employment. During the course of employment employees will have access to information of a confidential and sensitive nature. Employees must not disclose to a third party any SK SECURITY SERVICES LTD confidential information, either during their employment or after their employment has ended. Confidential information includes information on the SK SECURITY SERVICES LTD present or potential customers or suppliers and any information relating to the SK SECURITY SERVICES LTD business, including marketing, corporate or financial plans.

10. SK SECURITY SERVICES LTD recognizes that work may result in friendships and closer relationships developing. Relationships may develop not only with colleagues but suppliers and customers. It is natural for relationships to develop in a working environment. While SK SECURITY SERVICES LTD has every respect for the privacy of its employees, it asks that all employees consider the impact that personal relationships can have on the SK SECURITY SERVICES LTD.

11. SK SECURITY SERVICES LTD is committed to equality of opportunity and diversity in the workplace. It is the SK SECURITY SERVICES LTD policy to treat all job applicants and employees fairly and equally, regardless of their sex, trans-gender status, age, sexual orientation, religion or belief, marital status, civil partnership status, race, colour, nationality, national origins, ethnic origin or disability. Furthermore, SK SECURITY SERVICES LTD will monitor the composition of the workforce and introduce positive action if it appears that this policy is not fully effective. Employees are required to conduct themselves in a way that promotes equal opportunities at all times. Good practice will be promoted by senior management and employees will be provided with relevant training. Employees who feel they have been discriminated against or suffered harassment should speak to a member of management immediately.

12. Employees may seek to take up separate employment with another employer or pursue outside business interests while still remaining employed by the SK SECURITY SERVICES LTD. Although SK SECURITY SERVICES LTD has no desire to unreasonably restrict an employee's external activities, it must seek to protect its own interests and those of all its employees. Employees will not be permitted to undertake business activities or other work where SK SECURITY SERVICES LTD considers that this is incompatible with its interests and, in any event, unless employees have obtained prior written authorization from senior management.

13. SK SECURITY SERVICES LTD is committed to conserving the Earth's resources and to do what it can to reduce any negative effects it has on the environment. Employees are required to use the SK SECURITY SERVICES LTD equipment and materials wisely and reduce wastage where possible. Employees can play a positive role in helping the environment by recycling all non-confidential waste, using printers and photocopiers with care and switching off electrical equipment which is not in use.

Signed _____ Position DIRECTOR Date 1/3/2018

SK SECURITY
Services LTD

ANTI- CORRUPTION AND BRIBERY POLICY

1. Purpose

The purpose of this policy is to establish controls to ensure compliance with all applicable anti-bribery and corruption regulations, and to ensure that the Company's business is conducted in a socially responsible manner.

2. Policy statement

Bribery is the offering, promising, giving, accepting or soliciting of an advantage as an inducement for action which is illegal or a breach of trust. A bribe is an inducement or reward offered, promised or provided in order to gain any commercial, contractual, regulatory or personal advantage.

It is our policy to conduct all of our business in an honest and ethical manner. We take a zero- tolerance approach to bribery and corruption. We are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate and implementing and enforcing effective systems to counter bribery.

We will uphold all laws relevant to countering bribery and corruption in all the jurisdictions in which we operate. However, we remain bound by the laws of the UK, including the Bribery Act 2010, in respect of our conduct both at home and abroad.

Bribery and corruption are punishable for individuals by up to ten years' imprisonment and a fine. If we are found to have taken part in corruption, we could face an unlimited fine, be excluded from tendering for public contracts and face damage to our reputation. We therefore take our legal responsibilities very seriously.

3. Scope

3.1 Who is covered by the policy?

In this policy, **third party** means any individual or organisation you come into contact with during the course of your work for us, and includes actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies, including their advisors, representatives and officials, politicians and political parties.

This policy applies to all individuals working at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, home workers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with us, or any of our subsidiaries or their employees, wherever located (collectively referred to as **employees** in this policy).This policy covers:

Bribes;

Gifts and hospitality;
Facilitation payments;
Political contributions;
Charitable
contributions.

3.2 **Bribes**

Employees must not engage in any form of bribery, either directly or through any third party (such as an agent or distributor). Specifically, employees must not bribe a foreign public official anywhere in the world.

3.3 **Gifts and hospitality**

Employees must not offer or give any gift or hospitality:

which could be regarded as illegal or improper, or which violates the recipient's policies; or
to any public employee or government officials or representatives, or politicians or political parties.

Employees may not accept any gift or hospitality from our business partners if:

there is any suggestion that a return favour will be expected or implied.

Where a manager's approval is required above, if the manager is below Director level then approval must be sought from an appropriate Director.

If it is not appropriate to decline the offer of a gift, the gift may be accepted, provided it is then declared to the employee's manager and donated to charity.

We appreciate that the practice of giving business gifts varies between countries and regions and what may be normal and acceptable in one region may not be in another. The test to be applied is whether in all the circumstances the gift or hospitality is reasonable and justifiable. The intention behind the gift should always be considered.

Within these parameters, local management may define specific guidelines and policies to reflect local professional and industry standards. Where this policy requires written approval to be given, the Company Secretary shall put in place a process to maintain a register of all such approvals.

3.4 **Facilitation payments and kickbacks**

Facilitation payments are a form of bribery made for the purpose of expediting or facilitating the performance of a public official for a routine governmental action, and not to obtain or retain business or any improper business advantage. Facilitation payments tend to be demanded by low level officials to obtain a level of service which one would normally be entitled to.

Our strict policy is that facilitation payments must not be paid. We recognise, however, that our employees may be faced with situations where there is a risk to the personal security of an employee or his/her family and where a facilitation payment is unavoidable, in which case the following steps must be taken:

Keep any amount to the minimum;
Create a record concerning the payment; and
Report it to your line manager.

In order to achieve our aim of not making any facilitation payments, each business of the Company will keep a record of all payments made, which must be reported to the Company Secretary/Account department, in order to evaluate the business risk and to develop a strategy to minimise such payments in the future.

3.5 Political Contributions

We do not make donations, whether in cash or kind, in support of any political parties or candidates, as this can be perceived as an attempt to gain an improper business advantage.

3.6 Charitable contributions

Charitable support and donations are acceptable (and indeed are encouraged), whether of in- kind services, knowledge, time, or direct financial contributions. However, employees must be careful to ensure that charitable contributions are not used as a scheme to conceal bribery. We only make charitable donations that are legal and ethical under local laws and practices]. No donation must be offered or made without the prior approval of [the compliance manager.

All charitable contributions should be publicly disclosed.

4. Your responsibilities

You must ensure that you read, understand and comply with this

policy.

The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for us or under our control. All employees are required to avoid any activity that might lead to, or suggest, a breach of this policy.

You must notify your manager **OR** the Company Secretary or the confidential helpline as soon as possible if you believe or suspect that a conflict with or breach of this policy has occurred, or may occur in the future.

Any employee who breaches this policy will face disciplinary action, which could result in dismissal for gross misconduct. We reserve our right to terminate our contractual relationship with other workers if they breach this policy.

5. Record-keeping

We must keep financial records and have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

You must declare and keep a written record of all hospitality or gifts accepted or offered, which will be subject to managerial review.

You must ensure all expenses claims relating to hospitality, gifts or expenses incurred to third

parties are submitted in accordance with our expenses policy and specifically record the reason for the expenditure.

All accounts, invoices, memoranda and other documents and records relating to dealings with third parties, such as clients, suppliers and business contacts, should be prepared and maintained with strict accuracy and completeness. No accounts must be kept "off-book" to facilitate or conceal improper payments.

6. How to raise a concern

You are encouraged to raise concerns about any issue or suspicion of malpractice at the earliest possible stage. If you are unsure whether a particular act constitutes bribery or corruption, or if you have any other queries or concerns, these should be raised with your line manager **OR** the Company Secretary or through the confidential helpline.

7. What to do if you are a victim of bribery or corruption

It is important that you tell the Company Secretary/ Accounts Dept or the confidential helpline **on 01923 947264** as soon as possible if you are offered a bribe by a third party, are asked to make one, suspect that this may happen in the future, or believe that you are a victim of another form of unlawful activity.

8. Protection

Employees who refuse to accept or offer a bribe, or those who raise concerns or report another's wrong doing, are sometimes worried about possible repercussions. We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

We are committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential bribery or other corruption offence has taken place, or may take place in the future. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform [the compliance manager] immediately. If the matter is not remedied, and you are an employee, you should raise it formally using the company's Grievance Procedure.

9. Training and communication

Training on this policy forms part of the induction process for all new employees. All existing employees will receive regular, relevant training on how to implement and adhere to this policy. In addition, all employees will be asked to formally accept conformance to this policy on an annual basis.

Our zero-tolerance approach to bribery and corruption must be communicated to all suppliers, contractors and business partners at the outset of our business relationship with them and as appropriate thereafter.

10. Who is responsible for the policy?

The board of directors has overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it.

The Company Secretary has primary and day-to-day responsibility for implementing this

policy, and for monitoring its use and effectiveness and dealing with any queries on its interpretation. Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this policy and are given adequate and regular training on it.

11. Monitoring and review

The Company Secretary will monitor the effectiveness and review the implementation of this policy, regularly considering its suitability, adequacy and effectiveness. Any improvements identified will be made as soon as possible. Internal control systems and

procedures will be subject to regular audits to provide assurance that they are effective in countering bribery and corruption.

All employees are responsible for the success of this policy and should ensure they use it to disclose any suspected danger or wrongdoing.

Employees are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries should be addressed to the Company Secretary.

This policy does not form part of any employee's contract of employment and it may be amended at any time.

Signed _____ Position DIRECTOR Date 1/3/2018

SK SECURITY
Services LTD

Training and development policy

SK SECURITY SERVICES LTD promises to provide a training and development program for its staff that is structured and includes both vocational and occasional refresher training. The goal is to ensure success while enabling a high standard of service. This is also provided to comply with the **Private Security Industry Act of 2001**, the applicable legislation.

SK SECURITY SERVICES LTD will:

- Provide induction training for new staff and those transferring to new areas of our business

- Provide the required training for those seeking promotion so that they are appropriately prepared for achieving their new responsibilities

- Provide adequate training on health and safety for all employees

- Ensure that employees are aware of the availability of all training courses

- Develop a training plan for everyone, appropriate to each individual

- Review individual training plans during annual appraisals

We train staff members to be able to handle all tasks relevant to their specific assignments and to maintain or acquire the necessary specialist skills. Training is provided at continuation, refresher and contingency levels.

This policy has been reviewed and approved by the Directors of the firm and has the support of all management levels in SK SECURITY SERVICES LTD.

Signed A Nagra Position Director Date 1/3/2018

SK SECURITY
Services LTD

Recruitment and Selection Policy

We aim to provide equal opportunities in employment, and our recruitment and selection procedures reflect that. We correctly train our HR staff or other such members of staff who have recruitment and selection responsibilities, to ensure that they avoid unlawful discrimination, both of the conscious and the unconscious varieties.

Our policy is to hire, promote, and advance employees solely on the basis of merit. All decisions related to hiring, recruitment, promotion or advancement will be made on this basis.

From time to time, all job descriptions, if utilized, shall be reviewed and revised to make sure that they comply with our policy of equal opportunity.

When we place advertisements for job vacancies, we will take these issues into account, and they will be non-discriminatory in nature.

We are committed to providing fair treatment to each and every job applicant, and considering them only on the basis of their ability to carry out the essential functions of the job. All job interview questions must be of a nondiscriminatory nature, and only concern job requirements.

Signed _____ Position DIRECTOR Date 1/3/2018

SK SECURITY
Services LTD

Health and Safety statement of intent

1. Our company strives to take strict measures to monitor and control Health & Safety as an integral part of running our business operation. Amandeep Kaur Nagra is responsible for communicating this policy to all employees.

2. We will, so far as is possible:

   a. Make sure that all working practices and work equipment are safe and that they do not pose a risk or hazard to Safety and Health.
   b. Make sure that needed measures are carried out to safely use, store, and transport all substances and materials.
   c. Give all needed training, supervision, instruction and information to make sure that all employees have a working environment that does not endanger their Health or Safety.
   d. Control all workplaces, equipment and utilized transport in a condition that is safe and free from Health and Safety risks
   e. Make sure that employees have access to adequate facilities to safeguard their welfare
   f. Take measures to protect the Health and Safety of visitors, contractors and any members of the public who could be impacted by our operations
   g. Give employees all needed information concerning procedures to protect their Health and Safety and the Health and Safety of others, and, when needed, consult with them to improve how our company handles these issues.
   h. Make sure that all employees carry out their Health and Safety responsibilities and work with management to carry out this policy
   i. Monitor how this policy is carried out in the workplace.
   j. Make Sure sufficient funds are available to implement this statement.

SK SECURITY SERVICES LTD will also regularly review this policy to see if any changes are needed.

Signed Position Director Date 1/3/2018

SK SECURITY
Services LTD

Environmental Policy

SK SECURITY SERVICES LTD wishes to ensure their employees that we minimize any negative impact our operations could potentially have on the environment

Accordingly, our policy is to:

- Always strive to better our performance regarding environmental issues and use the best environmental management practices as part of our business operations.
- Try to minimize our use of resources and to attempt to efficiently use those resources that we must consume.
- Attempt to reduce our carbon footprint to comply with our targeted objectives.
- Responsibly apply the principles of waste reduction, waste reuse and waste recycling as per our waste management practices.
- Try to prevent pollution at our premises and work sites.
- Take environmental issues and energy performance into account in facility purchases, design, refurbishment and management.
- Take environmental issues, including climate change, into account when buying services and goods.
- Obey all applicable environmental laws and regulations.

The company monitors progress on these goals, seeks feedback from employees and customers on these issues, and informs employees about the importance of environmental issues. We work with our employees, service partners, landlords and their agents and customers to improve our performance on environmental issues. We take sustainability and other environmental issues into account when providing security services.

Signed _____ Position DIRECTOR Date 1/3/2018

SK SECURITY
Services LTD

Complaints Policy

We acknowledge that, no matter how hard we try to do our best, mistakes sometimes occur, and we may occasionally not give our Stakeholders, Employees or Clients the high quality of service that they properly expect from us.

We welcome, in those situations, being told that this has happened in the form of a Complaint.

When this occurs, which should be rarely, we will make every effort possible to quickly and efficiently remedy the problem, acknowledging directly our responsibility to correct errors, and doing so without compromising the rights and expectations of our Stakeholders, Employees, or Clients.

We incorporate everything we learn from addressing a Complaint to make our future quality of service better and to avoid similar problems from happening in the future.

We pledge to address Complaints:

Swiftly: A formal acknowledgement within 24 hours, If the complaint has not been resolved to send an interim response at the 3-day point, A full and final response at the 7-day point, A follow up 10 – 14 days after the final response to ensure the complainant is still happy with the resolution.

Efficiently: The Director of the business will personally take charge of the investigation of the complaint and directly communicate with the complainant to attempt to resolve the problem without delay.

Transparently: Documentation will be kept of the full results of the investigation and provided to the complaining party.

Honestly: If we have made an error or mistake, we will frankly acknowledge it. If our service was deficient in any way that was within our reasonable control, we will do our utmost to ensure that the complaining party does not suffer the consequences.
If you have a Complaint, please communicate with the SK SECURITY SERVICES LTD Team via Email, postal letter, fax, or telephone. Complaints can be addressed to any of our staff members.

Signed A Dogra Position DIRECTOR Date 1/3/2018

SK SECURITY
Services LTD

Child Protection Policy and Policy Statement

1.1 Introduction

Children, young people, and anyone who is particularly vulnerable are entitled to encounter a safe and enjoyable environment at social and educational organised events. Our company recognises its legal and moral duty to see to it that we provide these people with the best possible care when we are the security provider at such events.

We are dedicated to adopting and carrying out policies that mandate that all security personnel understand their strict obligation to protect children from abuse or other harm our personnel are required to follow our procedures adopted to protect children and to report any abuse of similar problems to the authorities.

At both indoor and outdoor functions and events, in the course of providing security services, we always strive to protect children, young people and others particularly vulnerable against abuse or harm. We endeavour to educate and train both employees and any volunteer security personnel to carry out this mission and be prepared to address specific child protection issues.

Each of our employees who perform security functions are fully licensed and trained by the Security Industry Authority, government initiated regulatory body for the security industry.

The Children's Act of 1989 defines a child/young person as anyone under the age of 18. Children's Act 1989).

1.2 Policy Statement

We believe that:

•Nothing is more important than the welfare of a child.

•Every child, regardless of gender, age, culture, ability, language, racial origin, sexual identity or religious belief and/or sexual identity is entitled to a safe and fun environment in which to pursue their religious, pleasure oriented or educational interests.

•It is our duty to protect children from degrading treatment, discrimination and other forms of harm through all possible measures. We endeavor to respect children's' feelings, wishes, and rights.

•We must take seriously and investigate thoroughly all allegations or suspicions of abuse of or poor practices aimed at children, and will promptly involve the authorities in any such incident.

•All our employees may, from time to time, with children while providing security services. Therefore, they are all screened and CRB checked as required by Security Industry Authority regulations. We provide all such employees with training and additional guidance concerning child protection measures to be taken. The CRB check and any screenings of employees are carried out by independent personnel not directed by the company.

•To be effective in protecting children, we must work in cooperation with event organisers, stakeholders, parents and children.

1.3 Monitoring and reviewing the policy and procedures

Child protection measures and procedures must be periodically reviewed and monitored. A regular report must be given to management concerning this by the Managing Director. The implementation of procedures should be regularly monitored and reviewed. The Managing Director should regularly report progress, challenges, difficulties, achievement gaps and areas where changes are required to the SK SECURITY SERVICES LTD management team.

This policy must be subject to overall review at least every three years or whenever the law or this organisation undergoes a major change.

Signed _____ Position DIRECTOR Date 1/3/2018