Securitas

POLICY TITLE AND NO:
22. Group Anti-Bribery and Anti-Corruption Policy
OWNER: SVP General Counsel
APPROVED BY: Board of Directors
APPROVED DATE: 240508
TARGET AUDIENCE: All employees, directors and officers of the Securitas Group

Group Anti-Bribery and Anti-Corruption Policy

1 Summary

The Securitas Group is committed to maintaining the highest standards of integrity and compliance with applicable laws, rules, regulations and any codes of conduct in the jurisdictions where it operates.

Securitas has **zero tolerance of any type of corruption,** including any type of bribes, facilitation payments or other improper benefits, and always aims to do what is right when it comes to our clients, our employees and society. Our clients are discovering the importance of working with a compliant company with strong values, and we aim to be their supplier of choice because of what we stand for.

The Board of Directors of Securitas AB (the "Board") expects that the Securitas Group employee is loyal, ethical, honest, and upholds a high degree of integrity and compliance with all applicable Anti-Bribery laws, including the US Foreign Corrupt Practices Act (the FCPA) and the UK Bribery Act (UKBA), , and the local laws in every country in which we do business (for example, federal, regional, provincial, and state laws) and our policies. Consequently, the Board has adopted this anti-bribery and anti-corruption policy (the "Policy"). This Policy is applicable to all Securitas legal entities, employees, directors and officers (jointly "Securitas Companies and Employees").

Strict compliance with this Policy is mandatory. Violations of applicable anti-corruption laws can result in substantial fines and criminal penalties for Securitas, possible imprisonment and fines for employees, and significant reputational damage generally.

Securitas expects all business partners to maintain the same high ethical standards. Accordingly, the content of this Policy shall be implemented, to the greatest extent possible, with all business partners and consultants, for example, through the inclusion of suitable contractual rights and obligations.

Summary of main changes since last revision:

No changes

2 Main Text of the Policy

This Policy sets forth the principles for appropriate and ethical conduct with regard to matters of anti-corruption, entertainment and gifts as well as conflicts of interest, and the compliance, review, and monitoring of third parties with which the Company conducts business. This Policy complements local legislation applicable to the Securitas business in all parts of the world.

Principles for corruption and bribes: zero tolerance

Securitas believes in a free market for the provision of our services, in a free and fair competitive environment. Consequently, within the Securitas business, there is zero tolerance for any type of bribes, facilitation payments or other improper benefits contrary to this Policy, the Values and Ethics Code, local laws and regulations, industry standards or ethical codes in the countries in which we

operate. The zero tolerance applies both when it comes to offering benefits or similar, but also in relation to accepting such benefits.

Non-compliance with this Policy and local laws and regulations may have very serious consequences for Securitas as a Group as well as for all Securitas Companies and Employees themselves.

Violations of this Policy are never in the interest of Securitas and reporting all such practices as well as offers or requests to provide any improper benefits will always serve the Securitas Group's best interest.

In order to avoid even the suggestions of unlawful or unethical behaviour, Securitas Companies and Employees shall, at all times, exercise good judgment and make every effort to avoid situations which may lead to an impression or even a suspicion of corrupt behaviour.

Anti-corruption legislation in certain countries has extra-territorial reach, meaning that it also applies to acts performed outside of the country that enacted the rules. Examples of such legislation are the US Foreign Corrupt Practices Act (the FCPA) and the UK Bribery Act (the UKBA). This Policy also seeks to ensure compliance with the principles of these Acts and to preserve the spirit and intent of these Acts in all countries.

For the purpose of this Policy, corruption is defined as any act or inaction which is intended to grant, offer or promise improper benefits or anything of value to induce the abuse of someone's entrusted power for illegitimate individual or group benefit or advantage. Corruption also includes accepting any such benefits.

> ***"Corruption is the abuse of entrusted power for private gain"***

Corruption includes a wide variety of behaviour including bribery, misuse of company assets but can also hide behind nepotism and conflicts of interest. The CEO of Securitas has issued *22.2. Instructions on Conflict of Interests*.

"Conflicts of Interests exist when your personal interest conflicts with, or appears to conflict with, the interests of Securitas"

Bribery is generally defined as promising, offering or giving, receiving or soliciting an undue advantage through the provision of anything of value to a person or entity, either directly or through an intermediary, to get the person or entity to perform, or refrain from performing, an act in breach of their business, public or lawful duties. Generally speaking, anti-corruption laws define "anything of value" to include as a bribe most anything that has value to the recipient, whether direct or to a family member or associate.

> ***"Bribe is the act of giving someone something of value, often illegally, to persuade that person to do something you want"***

The concept of a bribe or a corrupt behaviour is extremely broad and includes the provision or receipt of, as well as the facilitation of, for example:

- cash or other forms of payment or benefits to ensure or influence being awarded a contract or obtaining a permit or license
- inappropriate donations (either political or charitable) seeking to lead to specific benefits
- certain benefits without a direct financial value, such as memberships in clubs, prestigious awards or similar
- gifts, entertainment, lodging, or travel intended to influence the recipient to act in a specific way
- offers of employment or internships made to relatives of customers, business partners, or others, for an improper purpose
- so-called facilitation payments1 to obtain a decision or facilitate a process, even if such procedures are accepted or commonly practiced locally

It is not necessary that the benefit is given or offered directly to the person exercising the power. It may also be given or offered to an intermediary or a family member. Although corruption can occur in any business dealings (including with private companies and individuals) the risk of corruption is particularly acute when dealing with government officials[2]. In the context of government officials, an offence will be committed if a bribe is offered to a government official to gain a business advantage even if the official does not act improperly. Therefore, particular care should be taken when dealing with government or public entity officials.

The definition of corruptive practices or bribery varies from country to country. This Policy is not in any way meant to allow procedures that are not legal and/or not in line with business ethics in a country in which Securitas operates but may supplement and strengthen the requirements for a specific country with less developed anti-corruption legislation.

2.1 Gifts and Entertainment

A bribe can represent "anything of value." An area in which this can often be an issue is in the giving and receipt of gifts, hospitalities, meals, entertainment, travel, lodging, and similar benefits. When given or received for an improper purpose, such gifts and entertainments can constitute bribery.

All business-related gifts, meals, entertainment, hospitality, travel, and other benefits must be approved and may only be given or received in accordance with a Gift Policy. See *22.1 Instructions regarding Gift Policy*.

Securitas requires particular care to be exercised over gifts and entertainment involving government officials. It does not permit gifts or hospitality to be offered or provided to government officials which might influence them in the exercise of their public duties or appear to do so. Gifts or entertainment, if offered or provided to government officials at all, should be very modest in value and verified to be legal within the relevant jurisdiction.

---

[1] Facilitation payments are payments made to governmental officials to speed up or secure routine governmental action, most commonly when the payer is already entitled to such action. An example is a payment to a government official to speed up licenses renewals.

[2] Government officials are officials who hold positions in any central, regional, or local government departments, ministries, judiciary, or in partly/ fully state-owned or funded agencies/organizations and public institutions. Examples of government officials are politicians, ministers, staff of United States Department of Homeland Security or any country's Interior/ Home ministry staff, customs officials, and employees of tax authorities etc. Employees in state owned (partly or fully) organizations are also considered to be Government officials.

Certain forms of business-related gifts and entertainment may be appropriate and acceptable under local customs, if they are within the limits of this Policy and local laws and regulations and made in good faith. The standards for what is appropriate will vary from country to country, but will always need to be in compliance with local law as well as this Policy and the counterparty's anti-corruption policies.

Normally, acceptable benefits are benefits that can be given and received openly, where the benefit is limited and not such that it would normally be considered possible to influence the decision-making process.

The following factors can influence the assessment of whether a benefit given to or received by someone in connection with the Securitas business could be considered corruption or bribery or not:

- The value of the benefit - great care should be taken with any benefits that have more than an insignificant value.
- The position of the recipient - any type of gifts to government officials should be avoided.
- The nature of the benefit - benefits with little or no connection to the Securitas business are normally not appropriate.
- The timing of the benefit – benefits are normally not appropriate when given close to a tender period (before-during–after) or a negotiation period.
- The group of recipients and how the benefit is offered - any benefits that are not offered openly are normally not appropriate and benefits to selected individuals should be considered with more care than benefits offered to a whole group or category of people. Repeated invitations to or from the same person(s) within a short period of time should be avoided.
- Use common sense. If a gift could be perceived or interpreted as excessive, it is probably inappropriate.

Based on the framework provided by this Group Anti- Bribery and Anti-Corruption policy, every Country President must ensure that a local policy on gifts and entertainment is in place, defining approval protocols, monetary thresholds, reporting requirements and process to ensure that gifts and entertainment given and received are appropriately escalated for approval and recorded in a "Gifts and Entertainment register" maintained locally in accordance with local monetary thresholds and policy requirements.

2.2 Risk Assessment and Mitigation

It is the responsibility of each Divisional president, Divisional General Counsel and Country president together with their respective persons responsible for BE Compliance to continuously assess the risk for any Securitas Companies and Employees becoming involved in any type of corrupt behaviour, to flag such risks immediately and to adopt appropriate measures and controls to ensure that risks are adequately mitigated.

When entering new jurisdictions, committing to different types of cooperative relationships or being involved in mergers or acquisitions of entities, all Securitas Companies and Entities must ensure that a full assessment of the risks for corruption, bribes and other improper benefits in the country or in the relationship in question has been conducted.

Due diligence procedures shall include appropriate investigations of past and present anti-corruptive measures and the overall risk exposure with regard to corruption and bribes for each acquisition target or prospective partner. It shall be the responsibility of each project manager to ensure that

such processes are carried out routinely when commencing new relationships and continuously throughout the relationship when warranted. For more information see *12. Group Acquisitions and Divestments Policy*.

3 Applicability to Securitas and Third Parties

This Policy is applicable to all Securitas Companies, employees, directors and officers and shall be communicated and implemented, to the greatest extent possible, with all business partners and consultants, including such acting on behalf of Securitas. It is the responsibility of each Divisional President, Divisional General Counsel and each Country President together with the respective person responsible for BE Compliance, to ensure that the Policy is fully understood and implemented in their areas or countries of responsibility.

Strict compliance with this Policy is mandatory.

Securitas can be held responsible for the conduct of business partners which act on its behalf. Securitas has a responsibility to ensure that all those with which it conducts business understand that Securitas has zero tolerance for corruption. Securitas expects all those with which it conducts business to adhere to the same high ethical standards that govern Securitas. A business partner must never be engaged by the Company to do something that is prohibited by this Policy. See *21. Securitas Business Partner Code of Conduct*.

Securitas requires that all agreements with business partners be on reasonable market terms and that a reasonable due diligence be conducted before retaining business partners and monitoring their activities going forward. The amount of due diligence and monitoring must be proportionate to the risk of corrupt activities occurring in the region, industry, or specific project in question. Detailed instructions pertaining to suppliers can be found in *15.6 Global Purchasing Instructions and Instructions for the Approval and Monitoring of Suppliers*.

Securitas Companies and Employees shall make all reasonable efforts to include the *21. Securitas Business Partner Code of Conduct* and the principles of this Policy in agreements with all types of partnerships and other business relationship. Special care should be taken in the selection and management of external agents and representatives. Note also the section in this Policy on the risk assessment of third party relationships.

As business partners can sometimes be used to create 'slush funds' from which bribes may be paid, care must be taken to ensure that business partners are paid only commercially reasonable fees for legitimate goods or services that are provided to the Company. Payments must be made only upon a showing of sufficient support that the goods or services have been rendered. All payments to business partners must be accurately recorded in Securitas' accounts indicating the nature of the goods or services provided to Securitas and the amount paid to the business partner. Furthermore, adequate segregation of duties should be in place to ensure that no one employee has responsibility for more than one step in a transaction from completion to review. For example, an individual in a purchasing functions should not also be responsible for paying the supplier.

When any type of bribe or other improper benefit is requested, offered or given by a third party, the Securitas Company or Employee should always bring this to the attention of his/her manager or other appropriate functions within the local company, such as the local responsible for BE Compliance, local legal or Risk Manager. As soon as reasonably possible, it should be made clear to the third party that Securitas Companies and Employees can never accept or give any type of bribe or improper

benefit. Thereafter, the Country President of the country in question shall ensure that an evaluation of the possibility to continue the relationship is carried out. If the decision taken is not to abandon the relationship, it shall be the responsibility of the Country President together with the Divisional President and the divisional responsible for BE Compliance to ensure that such a decision is only taken after a proper risk assessment and appropriate safe-guards are put in place to avoid future incidents contrary to this Policy.

4 Implementation and Responsibility

It is the responsibility of the Business Ethics Compliance function to provide a framework which the Divisions and Countries must follow to ensure they adequately manage business ethics risks in their business. The Business Ethics Compliance function together with the Divisional President and the Divisional General Counsel will work with the countries' leadership teams to assess business ethics risks and support the countries in setting up plans to implement adequate measures and controls to mitigate such risks. The Business Ethics Compliance function shall monitor risk mitigation measures to ensure that adequate procedures are in place.

Each country shall appoint a local person responsible for Business Ethics compliance ("BE responsible person"). The Business Ethics Compliance Officer for the division shall be consulted on the appointment.

It is the responsibility of each Divisional President, Divisional General Counsel and each Country President, together with their respective BE responsible person and Head of Legal/General Counsel, to implement adequate measures and controls to mitigate risks and to adopt proper procedures to ensure that all Securitas employees are aware of, understand and comply with local laws, rules and regulations and this Policy. Each country shall also have appropriate internal procedures for staying up to date with legal developments within this area within the country or countries of operation and appoint a person responsible for providing guidance on this Policy.

All Securitas companies shall

(1) if deemed necessary, issue a local version of the Policy adapted, as the case may be, to local laws and regulations; otherwise it is a minimum requirement to translate this Policy into local language and

(2) issue specific local guidelines and rules for allowed gifts and entertainment and setting out procedures to be followed by any employees who have received gifts, intend to give gifts or are travelling to sponsored conferences (Gift and Entertainment Policy), in keeping with this Policy and local laws. These rules should be clearly published and known by all directors and employees to whom the Policy applies. The local Gift and Entertainment Policy must be reviewed and updated as necessary to reflect any changes in local or international laws, as well as any changes to this Policy.

A copy of any issued local policies and gift guidelines shall be provided to Group Legal.

5 Training

Who: The following employees – as a minimum - shall undergo training to ensure proper understanding of the principles of this Policy and local rules and regulations on anti-corruption:

- all Securitas support staff (including, legal, HR and finance/controller functions),
- all operative staff above and including branch manager level,
- all employees in contact with decision makers at customers or competitors,
- all employees engaging with government and government officials at any level including those responsible for managing license applications and payments,
- all sales personnel and
- employees responsible for purchasing and procurement.

Such training shall be appropriate for the position of the individual in question and their responsibilities within Securitas as well as the local situation and risk assessment. A general e-learning on anti-bribery and anti-corruption, financial misconduct and conflicts of interest will be available in LMS.

When: All relevant new employees shall undergo training within 3 months after start date and thereafter all employees shall undergo training every 18 months.

How: All relevant employees shall undertake the global web-based training and in complement a separate training on the *22.1 Instructions regarding Gift Policy* shall be held.

It is the responsibility of the Divisional Presidents, Divisional General Counsel and Country Presidents together with their respective responsible for BE Compliance to ensure that relevant training is provided to all employees on a regular basis and training records maintained, in order to ensure compliance with these principles. The Business Ethics Compliance function shall monitor training activity to ensure that suitable training is deployed.

6 Reporting, Investigations and Consequences of Breach

All Securitas Companies and Employees are required to report any suspicions of improper behaviour contrary to this Policy to their immediate managers, or, where this is not possible, a more senior manager, the local responsible for BE Compliance, the country risk manager, local ombudsman or legal counsel, as appropriate in each jurisdiction. Any instruction or requirement to act in violation of this Policy, must be reported as soon as possible. It shall be clearly communicated to all employees that no employee will suffer negative consequences for refusing to pay or accept bribes or engage in corruptive practices, even if such a refusal may result in the company losing business. Nor will any employee be the subject of retaliation for making good faith reports of potential misconduct.

All reported events or suspicions will be investigated and followed-up appropriately.

If a reporting person does not wish, or is unable, to report a suspicion to his or her immediate manager or another official in his/her organization, all such issues should be reported through the Securitas Integrity Line at https://securitas.integrityline.com/, via e-mail at integrity@securitas.com or to the Securitas Chief Business Ethics Compliance Officer. Up to date contact information can be found on the Securitas website, www.securitas.com.

Any violations of this Policy or local laws and regulations on anti-corruption and bribery will result in disciplinary action appropriate to the violation, including, but not limited to, termination of the employment. It may also result in fines or penalties for which the individual employee may be held responsible.

7 Review and Follow-up

Compliance with this Policy by all Securitas Companies and Employees will be monitored as part of the Business Ethics compliance program as well as by internal and external audits and routine follow-up of all reported matters that require resolution.

8 Reference to Instructions and Guidelines

- 22.1 Instruction regarding Gift Policy
- 22.2. Instructions on Conflict of Interests
- 22.3 Anti-fraud guidelines
- 15.6 Instruction for Supplier Risk Management

INSTRUCTION TITLE AND NO:
22.1 Instruction regarding Gift Policy
OWNER: SVP General Counsel
APPROVED BY: Group CEO
APPROVED DATE: 240508
TARGET AUDIENCE: Legal Function (Group, Division, Business Unit and Country), Employees responsible for Business Ethics Compliance (Group, Division, Business Unit and Country)

Gift Policy – Template

NOTE TO DRAFTER: This is a template gift policy stipulating the minimum requirements in the Securitas Group. When used please note that meal and gift limits should be adapted to comply with local customs and local laws. If a stricter approach is required by local law (e.g. in relation to public officials), countries may adopt specific sections to meet these needs.

Background and Purpose

The purpose of these local guidelines for allowed gifts and entertainment is to set out a procedure to be followed by all employees and directors of [COMPANY] ("**Securitas**") before offering or accepting any benefits, such as travel, accommodation, meals, gifts, hospitality, entertainment and events, all in relation to external companies or people not employed within the Securitas Group, in order to ensure compliance with Securitas' anti-corruption policy. The guidelines have been drafted on the basis of transparency, meaning that benefits given or received should be transparent towards the company and the immediate superior.

All examples below relate both to offering and accepting benefits if nothing else is stated. When approval from your immediate supervisor is required, such approval shall, if possible be received before accepting or offering the benefit. If it is not possible to receive such approval prior to accepting or offering a benefit, the approval shall be requested at the earliest convenience following such event. If the supervisor would not accept an already offered or accepted benefit, the local legal department should be contacted to discuss how to handle the matter.

1 Forbidden Benefits

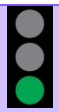
The following benefits are always forbidden: 	
a)	monetary gifts, gift cards or vouchers and any benefits that could be considered as cash equivalents;
b)	access to vehicles, boats, holiday homes or similar for private use;
c)	wholly or partially paid entertainment trips or holiday trips;
d)	benefits which are private and not connected to the work (including if such benefits are offered to or received by family members, partners or friends);
e)	offers that are perceived as generally unethical, e.g. strip club visits and similar activities
f)	offering benefits to public officials (public officials include e.g. (i) any employee of a government, state or municipality-owned or controlled enterprise or public international organization; (ii) members of political parties; (iii) any person acting in an official capacity;

	and (iv) any person that exercises public authority or carries out public procurements even if such person works on behalf of a private company). A coffee or a simple lunch may be acceptable in certain countries if it is not offered frequently, not offered to an important decision-maker, and not offered in connection with a negotiation. Always check with legal and local management before offering anything.

2 Benefits that require Preclearance

If you are uncertain whether a benefit is allowed or not, it should always be approved by your immediate supervisor. The following benefits must always be approved by your immediate supervisor: 	
a)	benefits of high value or regularly repeated (see examples and amount thresholds below);
b)	benefits (if not otherwise allowed as per this gift policy) directed at a selected individual (as opposed to a group of people, e.g. an entire department) or that invites a private companion;
c)	benefits of such nature or that are given in a way that cannot openly be discussed; and
d)	benefits that are given while business negotiations with the counterparty take place.

3 Allowed Benefits

A benefit may only be accepted or offered if it meets all the requirements below: 	
a)	It is in accordance with Securitas' anti-corruption policy and not knowingly in breach of the counterparty's anti-corruption policy
b)	It is of limited value and cannot be seen as extravagant (see examples and amount thresholds below);
c)	It can openly be discussed both within Securitas' organization and the counterparty's organization; and
d)	It does not create an appearance of a conflict of interest or a reputation risk for Securitas and is consistent with local customs and practices.

4 Examples

4.1 Travel or accommodation

a)	Attending a conference with a clear and lawful business purpose for one or two days is normally allowed but should be approved by your immediate supervisor before being accepted or offered.	
b)	However, do not accept that a business partner pays for your cost of travel or accommodation – this cost should be paid by Securitas.	
c)	Correspondingly to the above – it is not allowed to pay for travel or accommodation for a business partner (including clients).	
d)	Accepting or offering a free weekend at a hotel is never allowed.	

4.2 Meals

a)	Accepting or offering a *restaurant business lunch* is allowed if the lunch has a limited value (lower than SEK [AMOUNT] per person), has a clear business purpose and is not repeated regularly (e.g. not more than **four** times a year). If of a higher value and/or repeated more regularly or the business purpose is not clear, it should be approved by your immediate supervisor.	
b)	Attending or hosting a *dinner* with a business partner to e.g. network and discuss branch specific topics is acceptable if the value is limited (lower than SEK [AMOUNT] per person), is not repeated regularly (e.g. not more than twice a year) and the business purpose is clear. If of a higher value, repeated more regularly or the business purpose is not clear, it should be approved by your immediate supervisor.	
c)	Invitations to private companions (e.g partner, child, close relative or friend) are never allowed unless the companions pay for their own meals.	
d)	Accepting or offering meals which coincides in time with business negotiations is normally not acceptable, unless offered for practical or time saving reasons and the meals are of limited value (lower than SEK [AMOUNT]) but should always be approved by your immediate supervisor.	

4.3 Gifts

a)	Accepting or offering low value tokens which are produced for the purpose of being given away is allowed. Examples are marketing materials such as pens, candy, mugs, USB sticks.	

b)	Certain gifts of limited value (lower than SEK [AMOUNT]) designated at an *entire department*, e.g. flowers or a box of chocolate, on certain regular occasions, e.g. Christmas, or in connection with office moves, are allowed.	
c)	Certain gifts of limited value (lower than SEK [AMOUNT]) designated at an *individual* in connection with certain occasions which are not regular, e.g. a decade birthday, a wedding or a new job appointment, are normally allowed but should be approved by your immediate supervisor.	
d)	Gifts which have no connection with certain occasions are never allowed.	
e)	If you are offered an expensive gift during a business meeting and, because of cultural traditions, it would offend the provider if it is not accepted, you should report the gift immediately to your immediate supervisor. The gift may be returned or, with the provider's permission, donated to charity.	

4.4 Hospitality, entertainment and events

a)	Hospitality, entertainment and events should always be approved by your immediate supervisor before being accepted or offered. Attendance is only allowed if (i) employees from the counterparty are also attending, (ii) the counterparty does not pay for your accommodation or travel and (iii) the entertainment or event has a clear business purpose.	
b)	An invitation to a conference for e.g. the presentation of new products and services which is followed by an event that includes dinner and drinks is normally allowed, but should be approved by your immediate supervisor before being accepted or offered. Attendance is only allowed if (i) the total value of the event is not extravagant (less than SEK [AMOUNT] per person), (ii) the event is aimed at a large group of people, and (iii) includes a company presentation or similar.	
c)	Invitations to private companions (e.g. partner, child, close relative or friend) are never allowed unless the companions pay for their own costs of attendance.	
d)	A ticket to a local sports event or a similar event should always be approved by your immediate supervisor before being accepted or offered. It is only allowed if the value is limited (lower that SEK [AMOUNT] per person) and the game is held in connection with a sales event or similar with a clear business purpose.	
e)	If the ticket can be used at one's own convenience there is no valid business purpose, and the gift is accordingly not allowed.	

Instructions on Conflicts of Interest

1 Summary

DISCLOSE	You have an obligation to disclose any actual, potential, or perceived conflicts of interests to your manager
AVOID	You must avoid all conflicts of interests. Certain practices - such as nepotism and self-dealings (personal gain) - are prohibited
DOCUMENT	The resolution of any disclosed conflicts of interests shall be documented

These instructions are applicable and mandatory for all directors, officers, employees, agents and other representatives of Securitas.

2 Introduction and Objective

Business decisions must always be based on objective reasons and criteria and be taken in the best interest of Securitas. Business decisions may never be influenced by an employee's personal relationships, activities outside Securitas or financial interests. Conflicts of interest can impact the decisions we make, harm our brand and reputation, and create mistrust within and outside the company.

Pursuant to *20. Securitas' Values and Ethics Code*

- employees and business partners must avoid all conflicts of interest or perceived conflicts of interest between their personal activities and their part in the conduct of Securitas' business.
- business transactions between Securitas and parties related to an employee, such as family members1, relatives, friends, suppliers or clients with whom a Securitas' employee has a personal common interest ("**Related Parties**"), are only permitted under exceptional circumstances and after "grandparent approval", that is, approval by the employee's manager's manager.
- Grandparent approval is also required when members of the same family are employed or where there are close personal relationships between employees.

These instructions aim to provide further guidance for all Securitas employees on what a conflict of interest situation is, how employees should act and which situations to avoid. They also include an obligation on the individual to disclose any conflicts of interest, whether actual, potential or perceived.

These instructions are mandatory for all directors, officers, employees, agents and other representatives of Securitas.

Summary of main changes since last revision:

[1] Family members include but are not limited to the individual's spouse or partner or someone it has a romantical relationship with, children, parents, siblings, in-laws, grandparents, grandchildren, nephews, nieces, aunts, uncles, or people living in the individual's same household. It also includes persons with whom such people have a romantic relationship.

— Update on the new digital disclosure workflow.

3 What is a Conflict of Interest?

A conflict of interest (a CoI) exists when a person's interests (family, friendships, financial, or other) can influence that person's loyalties, judgment, and actions. For example, a person has a duty of loyalty to its employer but may also have a loyalty to a family business. Each of these businesses expects the person to have its best interest first and when that is not possible there is a conflict between the interests.

Conflicts of interest can occur on all levels and in all areas within Securitas.

There are 3 types of conflicting interests:

1. ACTUAL	**you are currently being influenced by a conflicting interest**
For example – You (on behalf of Securitas) sign an agreement with a supplier that is owned by your brother	
2. POTENTIAL	you **could be** influenced by a conflicting interest
For example – You are a board member of or have a financial interest in a company that considers tendering for Securitas business	
3. PERCEIVED	you **could appear** to be influenced by a conflicting interest
For example – You consider signing an agreement (on behalf of Securitas) with a supplier that is the employer of your sister. This does not influence your decision as the supplier is the best, but you understand that someone may think that you are choosing or influencing the decision to choose this supplier to benefit your sister. Note that perceived conflicts of interest are more likely to occur if the Securitas employee concerned is a high-ranking manager.	

4 Expected Conduct

All employees must avoid all conflicts of interest or perceived conflicts of interest between their personal activities and their role at Securitas.

Your expected conduct can be summarized in three key takeaways:

— Make a strict separation between business decisions and personal interests
— Do not give preferential treatment to personal contacts such as friends or family
— If a situation would arise that could lead to a conflict of interest (actual or perceived), you must immediately inform your manager

Make a habit of regularly asking yourself: (1) Do I have any conflict of interest to disclose? (2) Can my personal relationships influence my business decisions? (3) Does my role include (or could it be perceived to include) any decision-making authority over business with entities involving family members or close friends?

All employees must report all actual, potential or perceived conflicts of interests as soon as the employee identifies that there may be a conflict of interest and, whenever possible, before the employee engages in any conduct in which the conflict may influence (or appear to influence) the

employee's decision making. Failure to report conflicts of interest may result in disciplinary action appropriate to the violation, including, but not limited to, termination of employment.

Do

- take all reasonable steps to avoid conflicts of interest
- disclose actual, potential, or perceived conflicts of interest to your manager, local Business Ethics representative or Business Ethics Compliance Officer when they first arise
- keep a professional relationship with suppliers and business partners, avoiding over-familiarity
- avoid situations that might create suspicion of preferential treatment
- obtain grandparent approval before becoming a board member, employee or consultant of an external business, non-profit or similar organization
- tell your manager and obtain grandparent (that is, manager's manager) approval if you take part in social or professional activities outside your job that create an actual, potential, or perceived, conflict of interest
- make sure that an appropriate due diligence is performed when involving agents and representatives to facilitate business for Securitas to ensure that potential conflicts of interest involving agents and representatives are identified and appropriate measures are taken to avoid, manage and mitigate them
- seek advice and recommendations from your Legal Department or the Business Ethics function if you have doubts or questions about these topics

For practical examples of different situations and expected conduct, see Exhibit 1.

5 Prohibited Conduct

Prohibited conduct are:

NEPOTISM	you give favours to personal contacts such as family members or friends
For example – you make the decision to hire or promote, or you directly or indirectly supervise a family member, close friend or somebody you are in a relationship with or grant them special benefits because of your personal relationship with them	
SELF-DEALINGS (PERSONAL GAIN)	you act in your own interest rather than the interest of Securitas
For example – You take business opportunities that Securitas is entitled to for yourself or use Securitas' assets for your private benefit	
CONTRADICTORY INTERESTS	you have an interest that is contradictory to Securitas interest
For example – You serve on the board of a business that competes with Securitas or otherwise work/consult for or represent or help a business that competes with Securitas	

Prohibited conduct can only be permitted to continue as is (i.e. without being mitigated) under exceptional circumstances and only after obtaining both (1) written grandparent approval (that is,

approval by the employee's manager's manager) AND (2) approval by the General Counsel and President of the relevant Division or Group.

More examples of prohibited conduct can be found in Exhibit 2.

6 Disclosure Obligations

6.1 All Employees

All new employees must disclose any actual, potential or perceived conflicts of interest in relation to employment with Securitas, to their immediate manager, HR Department, Business Ethics representative or Legal Department when they become an employee and thereafter immediately if they become aware of any actual, potential or perceived conflict of interest situation.

All conflicts of interest disclosures submitted at the time of employee on-boarding must be documented using the form in Exhibit 3 – Declaration of Conflicts of Interest and filed in the individual employee file

6.2 Management and Senior Executives

The following employees must annually complete the COI disclosure form using Exhibit 3 – Declaration of Conflicts of Interest and send it to their manager:

- All members of Group, Divisional and Country Management,
- Employees reporting to a President (Group, Division or Country President) and employees reporting to a person reporting to the President and
- Employees holding particular sensitive positions/at-risk employees (such as members of the purchasing, sales and business development department etc.).

All disclosure forms must be filed with the person responsible for BE Compliance for a period of 5 years or as set out in local legislation.

As of 1st of June 2024 a digital disclosure workflow will be available through the ServiceNow module (Risk & Compliance -> Declare COI).

6.3 What situations should be disclosed?

The following list includes illustrative examples of situations that should always be disclosed:

A. **Outside employment or service.**
   - Taking on a second job or consulting or volunteer assignment that could conflict with your work at Securitas
   - Acting as a corporate director, board member, or consultant for another business or organisation that could conflict with your work at Securitas

B. **Outside financial and other commercial interests**
   - Having a financial[2] or other interest that allows influence over the operations in companies or organisations that are Securitas' suppliers, contractors, intermediaries, customers, other business partners or competitors.

C. **Familial and other close personal relationships (Related Parties) and contacts within Securitas**
   - If a family member[3] applies for a job with Securitas where that position will involve reporting lines to the employee (directly or indirectly) or where the employee is involved in the hiring decision-making process or has influence over the terms and conditions of employment for the job applicant
   - If you have a romantic relationship with someone in the same reporting line, i.e. someone that directly or indirectly supervises you or whom you supervise.

D. **Familial and other close personal relationships (Related Parties) outside of Securitas**
   - If you have a family member[4] or other Related Party[5] that is employed in a decision making role (with respect to procurement or execution processes with Securitas) or have a direct or indirect interest (financial[6] or non-financial interest) or other relationship in a vendor, supplier, partner, contractor, subcontractor, client, agent, or competitor of Securitas.
   - Signing a contract on behalf of Securitas with a business that is managed or owned by a closely related party, such as a family member or close personal friend

E. **Family members or Related Parties being a Government Official (GO)**
   - Holding a public office, or having a relationship with a public official, that could lead to an actual, potential, or perceived conflict of interest.

F. **Other[7] potential conflicts of interest**
   - Offering, soliciting or accepting gifts and entertainment, illegal payments, remuneration, donations, or comparable benefits from competitors, clients and suppliers or potential suppliers that may influence your judgement. All such transactions should be consistent with the Instruction regarding Gift Policy in Policy 22 "Group Anti-bribery and Anti-corruption policy".
   - Taking business opportunities that Securitas is entitled to for yourself or using Securitas' assets for your private benefit.

---

[2] Shareholdings in suppliers, agents, contractors, or clients publicly listed on a stock-exchange are excluded from the disclosure obligation.

[3] Family members include but are not limited to the individual's spouse or partner or someone it has a romantical relationship with, children, parents, siblings, in-laws, grandparents, grandchildren, nephews, nieces, aunts, uncles, or people living in the individual's same household. It also includes persons with whom such people have a romantic relationship.

[4] Family members include but are not limited to the individual's spouse or partner or someone it has a romantical relationship with, children, parents, siblings, in-laws, grandparents, grandchildren, nephews, nieces, aunts, uncles, or people living in the individual's same household.

[5] Related Party includes immediate and/ or extended family members and close personal friends where the party is in a position to influence decisions/ bias of the employee.

[6] Shareholdings in suppliers, agents, contractors, or clients publicly listed on a stock-exchange are excluded from the disclosure obligation.

[7] You may have been involved in activities, which are not covered by the disclosure categories above, that you think might be (or might be perceived as) a conflict of interest with respect to our organization.

7 Evaluation and Decision

Any disclosed conflicts of interests shall be evaluated fairly by the “grandparent”, based on the employee’s immediate manager’s recommendations, taking into account business and reputational risk for Securitas, as well as the perception of the conflict of interest by others within and outside Securitas. The decision taken by the grandparent shall be documented in writing and shall resolve the conflict of interest whilst minimizing the risks for Securitas, protecting the reputation of the company, and protecting the private interests of the individual to the extent possible.

For guidance on how to resolve conflicts of interests, see Exhibit 4.

The decision, along with its reasoning, shall be communicated to the employee by the immediate manager and it is the immediate manager’s responsibility to make sure that the employee understands and complies with the decision.

For annual COI disclosure activity specified under 6.2, a copy of the decision shall be filed with the person responsible for BE Compliance for a period of 5 years or as set out in local legislation.

8 Applicability

These instructions are mandatory and apply to all companies, employees, directors and officers of companies within the Securitas Group, that is, companies where Securitas AB (publ) directly or indirectly, owns or has a controlling interest.

9 Implementation and Responsibility

A person responsible for Business Ethics Compliance shall be appointed in each country (“BE Compliance representative”).

It is the responsibility of the respective President and the person responsible for BE Compliance for the area or country to ensure that these Instructions are fully understood and implemented in their areas or countries of responsibility. They must also ensure that effective administrative and organizational processes and controls are implemented and maintained with a view of taking all reasonable steps to prevent conflicts of interests, and managing and mitigating them when avoidance is not possible.

These instructions should be clearly published and known by all employees, officers and directors. It should be clearly stated to whom an employee can turn for guidance in the relevant area or country.

10 Training

It is the responsibility of the respective President and the person responsible for BE Compliance for the area or country to ensure that relevant training is provided to employees on a regular basis (at least every 18 months), in order to ensure compliance with these principles.

Such training shall be appropriate for the position of the individual in question and their responsibilities within Securitas, as well as the local situation and risk assessment.

11 Reporting, Investigations and Consequences of Breach

All Securitas entities and employees are required to report any suspicions of improper behaviour contrary to this Policy to their immediate managers or, where this is not possible, to a more senior manager, country risk manager, local ombudsman, legal counsel or Business Ethics representative, as appropriate in each jurisdiction. No employee will suffer negative consequences for complying with this Policy, even if such compliance results in the loss of business, or for reporting non-compliance. All reported events or suspicions will be investigated independently and followed up.

If a reporting person does not wish, or is unable, to report a suspicion to his or her immediate manager or another official within the organization, all such issues should be reported through the Securitas Integrity Line at securitas.integrityline.com, via e-mail at integrity@securitas.com or to the Securitas Chief Business Ethics Compliance Officer. Up to date contact information can be found on the Securitas website, www.securitas.com.

Any violations of this Policy or of the applicable local laws will result in disciplinary action, up to and including termination of employment.

12 Review and Follow-up

Compliance with these instructions by all Securitas entities and employees will be monitored as part of the Business Ethics Compliance program as well as by internal and external audits, and routine follow-ups of all reported matters that require resolution.

Exhibit 1

Practical Examples

A. My neighbour is a supplier to Securitas and has invited me to stay at her summerhouse for the weekend. Can I go?

It depends. A personal relationship does not have to be negatively affected due to a business relationship. However, the personal relationship must never affect or influence the business relationship. Always ask your manager if you are unsure. If you are in a decision-making position with regards to the supplier the presumption is that you have a conflict of interest and should not accept the invitation.

B. My niece recently graduated and is looking for a job. We have relevant open positions and she has asked me to help her secure one. What should I do?

Direct your niece to the website where she can apply or direct her to the contact person that manages applications. Inform the person responsible for hiring that the applicant is your relative and remind the person responsible for hiring that grandparent approval is required to hire relatives.

C. The CEO of one of our largest clients is a close friend of mine. Is this a concern or a problem?

Inform your manager and if you are a member of Group, Divisional and Country Management or have a sensitive position, fill out the Declaration of Conflicts of Interest form. You cannot take part in any business-related decisions regarding that client.

D. My husband is working for a company that is being considered as a supplier to Securitas. Is this appropriate?

It depends. It may be OK with grandparent approval. However, you need to remove yourself from this conflict of interest situation by declaring the relationship to your manager and not participating in the procurement or execution processes. Do not disclose information to the Related Party that might give them an advantage over other potential suppliers participating in a bidding process.

Exhibit 2

Prohibited Conduct

It is, for example, prohibited to:

I. In general

- participate in decision-making that creates a conflict of interest
- have close personal relationships that influence the decisions for example in a bidding process
- influence a business decision of a third party to the benefit of Securitas, with the help of a Related Party

II. Nepotism

- give preferential treatment to personal contacts such as family members or friends
- hire or directly or indirectly supervise a family member, close friend or personal business partner; this also includes approving employment terms (including salary, benefits and education) and not-insignificant changes of job descriptions for such person
- have a romantic relationship with someone who directly or indirectly reports to you
- have business transactions between Securitas and a company directly or indirectly controlled by Related Parties to the employee or in which the Related Parties otherwise have a financial interest

III. Self-dealings

- have business transactions between Securitas and a company directly or indirectly controlled by the employee or its family members or in which the employee otherwise has a financial interest
- own or control a supplier of Securitas either directly or through a Related Party
- use Securitas' assets for your private benefit unless such use is explicitly allowed pursuant to the employment agreement or company policies
- take business opportunities for yourself that Securitas is entitled to

IV. Contradictory interest

- compete with Securitas by for example serving on the board of a competitor of Securitas or otherwise work/consult for or represent such competitor

Exhibit 3

Declaration of Conflicts of Interest

Name:	Date:
Employer company:	Employee ID number:
Line manager:	Manager's manager:

□ I would like to disclose the following existing or potential conflict of interest situations arising from my duties as a representative of the entity stated above or the Securitas Group:

*Persons/companies with whom/which I have official dealings or other business contacts and private interests with and a description of the nature and all relevant facts regarding my duties in relation to this person/s and/or company/ies (as described in **Securitas Instruction on Conflict of Interests**).*

1.
2.
3.
4.

I propose that the disclosed conflict of interest is resolved in the following way:

□ I declare that to the best of my knowledge and belief, I do not have any interests which might conflict – or be perceived to conflict – with my duties to the entity stated above and/or the Securitas Group. If my situation would change, I will update my declaration accordingly.

I confirm that there are no other actual or potential conflicts of interests that I am aware of than the ones described above.

Employee Signature

DECISION ON CONFLICT IDENTIFIED

Approvers name:	Date:
1.	
2.	
3.	
4.	
Signature	

Exhibit 4

Guidance on how disclosed conflicts of interest can be resolved

Conflict type (Actual, Potential, Perceived)	**Personal interests** (Family, Friends, Romantic relationship, Personal finances, Investments, Industry standing, Consulting work, Board memberships, Charitable work)	**Conflict of interest disclosed by employee**	**Prohibited Conduct?**	**Guidance on how the conflict of interest could be resolved** Resolving the conflict of interest means to remove the conflict, in other words implement changes to ensure the conflict no longer exists (for actual conflicts) or risks materializing (for potential or perceived conflicts).
Actual	Family	Employee directly or indirectly supervises family member	Yes	The family member or the employee is reassigned to another department
Potential	Family	Employee works in same company as family member	Maybe	Ensure that the employee is not involved in any employment, performance, or compensation questions
Potential	Family/friends	Family member or close friend has applied for a job in same company as employee	Maybe	- Ensure that employee is not involved in the recruiting process or decision - Ensure that employee will not (directly or indirectly) supervise the applicant - applicant should ideally not work in same department as employee.
Actual	Family/friends	Family member or close friend directly or indirectly controls a supplier to Securitas	Yes	Ensure that employee is not involved in decisions related to the supplier.
Actual	Romantic relationship	Employee directly or indirectly supervises a person with whom he/she has a romantic relationship	Yes	The person or the employee should be reassigned to another department
Potential	Romantic relationship	Employee has a romantic relationship with a colleague but does not directly or indirectly supervise that person	Maybe	Ensure that the employee is not involved in any employment, performance or compensation questions related to the person
Potential	Family	Family member or close friend works for a customer and is involved with Securitas (who is the supplier to the customer)	Maybe	Ensure that the employee is not involved in decisions related to the customer
Actual	Board membership	Board member in a company that is a competitor to Securitas	Yes	Employee should be required to resign as a Board member of the competitor
Actual/Potential	Investment	Employee owns shares in a company that competes with Securitas	Maybe	Case-by-case assessment. Impact depends, for example, on size of shareholding by the employee and the employee's position within Securitas including her/his decision making possibilities. If shareholding could influence the employee's decision making this needs to be resolved, for example, by requiring that the shares are divested or by reassigning the employee.

Anti-fraud guidelines

1 Summary

Every year, huge sums are lost by business of all sizes and in all industries due to fraud. It is often the result of a high number of small frauds and not necessarily the big specular cases that are reported on in the media. Fraud committed by organized criminals is increasing. Examples include false or stolen identities, for example so called fake president fraud, and other forms of e-fraud.

Some facts:

- fraud losses are not restricted to a particular sector or country
- only a small percentage of losses from fraud are recovered by organizations
- a large part of frauds are committed by persons in a senior position in the company
- greed is one of the main motivators for committing fraud
- fraud is increasing in developing markets

The threat of fraud can be internal or external, but the likelihood that a fraud will be committed decreases substantially if the potential fraudster believes that the rewards will be small, that they will be found out, or that the potential punishment will be unacceptably high.

The law relating to fraud varies from country to country, but in most countries it is a criminal offence. Please make sure that you are familiar with the laws and regulations in your country.

These guidelines will define fraud and give examples on what you can do to prevent, or in worst case, detect fraud that has already been committed.

Summary of main changes since last revision:

- No changes

2 Definition of fraud

Securitas is governed based on a zero-tolerance approach to any kind of fraud and aims at developing an anti-fraud culture that permeates all aspects of Securitas Values and Ethics code. The approach to anti-fraud efforts shall be based on five founding principles: Transparency, Accountability, Responsibility, Independence, and Reasonability

Fraud is when someone intentionally tries to mislead another person or entity or abuses his/her position to achieve a gain or an advantage for the employee or someone else – for example to unjustly receive money, services, or assets.

Human errors1 are not included in the definition of fraud. Fraud could include activities such as theft, corruption, conspiracy, embezzlement and extortion.

Examples of fraud:

- corporate identity fraud, money laundering
- phishing, spamming, copyright crimes, hacking, social engineering frauds
- misrepresentation of the quality of services or goods
- financial statement fraud
- payroll fraud, falsifying records or expense claims for improper advantage, thefts of cash, assets or intellectual property, false accounting
- unauthorized and/or illegal use of organizational resources, information, or services for personal purposes
- fraudulent insurance claims, misappropriation of funds
- signature forgery, information forgery on documents
- acts of bribery and embezzlement
- grant fraud, social security benefit claim frauds, tax evasion

Refer **Appendix-1** for examples of common types of internal fraud.

These guidelines focus on fraud/ unethical conduct against the company that is mainly carried out by internal people. It will cover two main categories of fraud that affect the organization.

1. Asset misappropriations, that is, the theft or misuse of an organization's assets. Examples include theft of inventory or cash, false invoicing, accounts receivable and payable fraud and payroll fraud.
2. Fraudulent statements, usually in the form of falsification of financial statements in order to obtain some form of improper benefit. It also includes falsifying documents such as employee credentials.

Why
There might be many reasons for fraud, but often it is a combination of pressure/motivation, opportunity, and rationalization. Pressure or motivation is often based on greed or need. Many people might have the opportunity to commit fraud, but only a few of the needy and greedy actually do it.

When it comes to opportunity, fraud is more likely in a company where there is weak internal control systems, little risk of detection or an unclear stand regarding acceptable behaviour.

Most people comply with laws, policies or rules because they believe it is the right thing to do, or because they are afraid of being shamed if they are caught. Others might rationalize fraudulent actions as necessary (doing it for the business), harmless (it will not have any major impact on the victim) or justified (the victim deserved it).

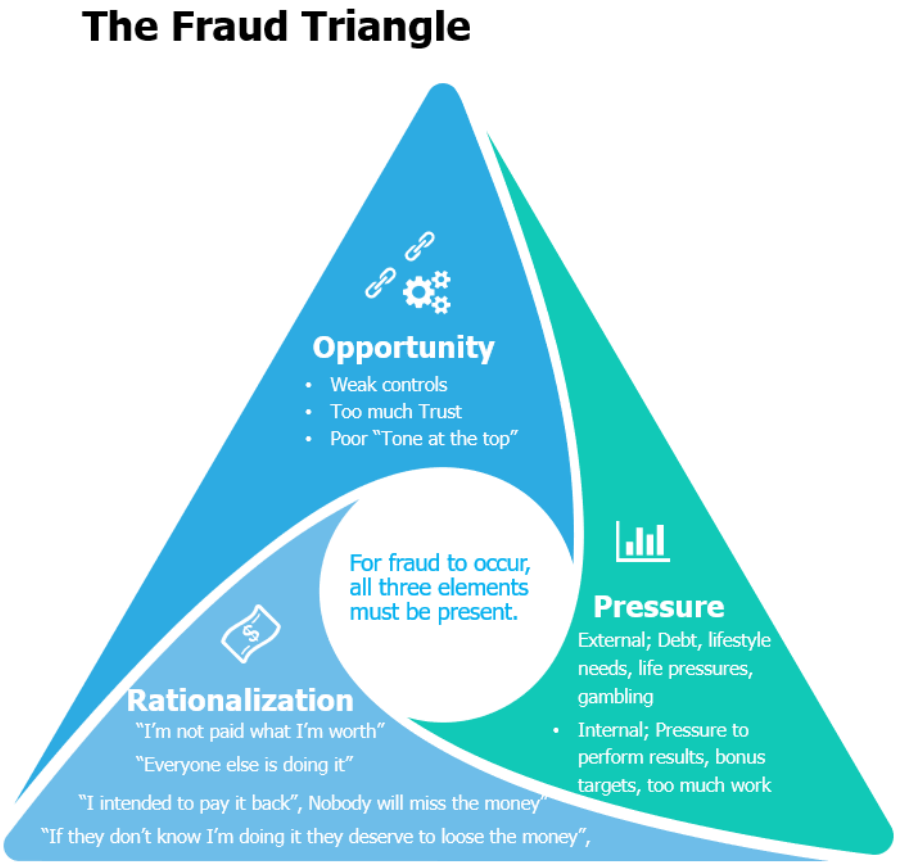
Who
There are three main types of fraudsters

- Those who intend to commit fraud from the start

[1] Human errors are un-intention mistakes during the performance of one's responsibilities without any malfeasance or wrongful intent to cause loss to any person or organization.

— Those who start off honest but then commit fraud when something happens, such as feeling mistreated at work or negative changes in the personal life
— Those who carry on to cover losses or debts caused by fraud

This can also be illustrated by the so called “Cressey’s fraud triangle”:



Cressey’s fraud triangle

3 Managing the risk of fraud

Managing the risk of fraud is the same in principle as managing any other business risk. First, the potential consequences of fraud on the organization need to be understood. The risks should then be reduced by developing and implementing an anti-fraud strategy. This is best approached systematically, by having policies together with controls and procedures.

3.1 Analyzing fraud risks

Fraud risk is included in two different risk categories in Securitas' risk register, depending on the type of risk: the financial risk category (management fraud risk) and the operational risk category (fraud and error risk). These guidelines will focus on the fraud and error risk, that is, the risk for fraudulent activities carried out by employees, clients, suppliers or others, against Securitas or our clients.

To be able to analyze the risk for fraud, a fraud risk review is recommended. The review should take into account whether errors or events could be the result of a deliberate act designed to benefit the perpetrator. The team conducting the review should ideally include people with in-depth knowledge of the business and market and people with knowledge and experience of fraud.

To avoid having a scope that is too narrow, the risks should be classified by reference to the possible type of offence and the potential perpetrator(s). Fraud risks need to be assessed for a number of different areas and processes, for example, cash payments, cash receipts, sales, purchasing, expenses, inventory, payroll, fixed assets and loans.

Refer **Appendix-2** for example on fraud risks analysis

3.2 Risk strategy

Once the risks have been identified and assessed, strategies to deal with each identified risk can be developed. Strategies for responding to risk generally fall into one of the following categories:

- risk retention - for example choosing to accept small risks
- risk avoidance - for example stopping sale of certain services to avoid the risk of occurring
- risk reduction - for example through implementing controls and procedures
- risk transfer - for example contractual transfer of risk; transferring risks to insurers

The chosen strategies should be allocated and communicated to those responsible for implementation. For the plan to be effective it is important that responsibility for each specific action is assigned to the appropriate operational manager, including clear targets for each action. It is also important that the management of the fraud risk is continually reviewed and developed.

3.3 Anti-fraud strategy

An effective anti-fraud strategy in fact has four main components:

- prevention
- detection
- deterrence
- response

Fraud detection acts as a deterrent by sending a message to likely fraudsters that the organization is actively fighting fraud and that procedures are in place to identify any illegal activity that has occurred. The possibility of being caught will often persuade a potential perpetrator not to commit a fraud. A consistent and comprehensive response /to suspected and detected incidents of fraud is also important. This sends a message that fraud is taken seriously, and that action will be taken against perpetrators.

3.3.1 Fraud prevention and detection

A strong ethical culture and an effective system of internal control form the base of the anti-fraud strategy. However, a sound system of internal control cannot provide complete protection against all fraudulent behavior. Even if it is close to impossible to remove all opportunities for perpetrating fraud, it is important to have additional fraud prevention and fraud detection measures.

In the case of deliberate acts of fraud, the aim of preventative controls is to reduce opportunity and remove temptation from potential offenders. Prevention measures include having appropriate policies, procedures and controls, and activities such as training and fraud awareness to stop fraud from occurring.

Key elements of a comprehensive fraud detection system include analysis and other procedures to highlight anomalies, for example through exception reporting, data mining, trend analysis and ongoing risk assessment.

3.3.2 Indicators and warnings

Paying attention to some of the most common fraud indicators can provide early warning that something is not quite right and increase the likelihood that the fraudster will be discovered.

Fraud indicators fall into two categories:

- warning signs
- fraud alerts

3.3.2.1 Warning signs

Warning signs can be described as organizational indicators of fraud risk. Below are some examples.

- Business risk, which can be split into:
    - cultural issues, for example lack of a strong company culture, adequate policies, and internal controls
    - management issues, for example lack of clear management control of responsibility, authorities, delegation, etc., lack of finance expertise, strained relationship with auditors
    - employee issues, for example inadequate recruitment processes, insufficient controls of conflicts of interest, dissatisfied employees, employees with personal problems such as indebtedness, poor implementation of internal controls and training
    - process issues, for example lack of job segregation and independent checking of key transactions, poor management accountability and reporting systems, Poor access controls to physical assets and IT security systems
    - transaction issues, for example poor documentation of transactions, large cash transactions, assets exposed to misappropriation

- Financial risk
    - Complex transactions
    - Management compensation highly dependent on meeting aggressive performance targets
    - Rapid changes in profitability

- Environmental risk
    - The introduction of new accounting or other regulatory requirements that could significantly change reported results
    - Highly competitive market conditions and decreasing profitability levels within the organization
    - Rapid technological changes that may change the market
    - Significant changes in client demand

- IT and data risk
    - Users not adopting good computer security practices, for example sharing or displaying passwords
    - Unauthorized access to systems by employees or external attackers
    - Sensitive data being stolen, leaked, or lost
    - Rapid changes in information technology
    - Unauthorized electronic transfer of funds or other assets
    - Manipulation of programs or computer records to disguise the details of a transaction

3.3.2.2 Fraud alerts

Fraud alerts can be described as specific events or red flags, which may indicate fraud. A list with examples of possible fraud alerts is provided below.

- Anonymous e-mails/letters/telephone calls
- E-mails sent at unusual times, with unnecessary attachments, or to unusual destinations
- Employees with discrepancy between earnings and lifestyle
- Unusual, irrational, or inconsistent behaviour
- Alteration of documents and records
- Photocopies of documents in place of originals
- Stamp signatures instead of original signatures
- Signature or handwriting discrepancies
- Missing approvals or authorization signatures
- Transactions initiated without the appropriate authority
- Ledgers that do not reconcile with control accounts
- Extensive use of ‘suspense’ accounts
- Inappropriate or unusual journal entries
- Confirmation letters not returned
- Supplies purchased more than need, or not delivered
- Higher than average number of failed login attempts
- Systems being accessed outside of normal work hours or from outside the normal work area
- Controls or audit logs being switched off

Refer **Appendix-3** for examples of fraud indicators, risks, and controls

3.4 Fraud response plan

The fraud response plan should specify the activities in place for dealing with detected or suspected cases of fraud. The intention is to provide procedures so that evidence gathering and collation will

facilitate informed decision-making, and also ensure that evidence gathered will be admissible in the event of any civil or criminal action. A published fraud plan can also work as a deterrent.

Steps for responding to detected or suspected instances of fraud include:

- Clear reporting mechanisms: it should be clear to all employees how fraud should be reported (for e.g. through Securitas Integrity Line or at Group Integrity mailbox (integrity@securitas.com)
- A independent, thorough investigation
- Disciplining of the individuals responsible (internal, civil and/or criminal)
- Recovery of stolen funds or property
- Modification of the anti-fraud strategy to prevent similar behavior in the future

Refer **Appendix-4** for examples of identifying anomalies

4 Managing fraud complaints

All board members, general management, divisional and country leadership teams, managers, and co-workers have a clear responsibility to react as soon as fraud, or unethical conduct or non-compliance to Securitas Values and Ethics code is reasonably suspected. A suspicious course of events is reason enough to react. This means if one believes, in good faith, that uncovered or observed evidence indicates a case of fraud or corruption.

Managers or co-workers who are aware of fraudulent or corrupt conduct, or who suspect fraudulent or corrupt conduct has taken place, are responsible to report the incident to either:

- Supervisor
- Local HR/ Divisional HR
- Country/ Divisional Business Ethics responsible
- Securitas Integrity Line

Depending on the magnitude and the complexity of the allegations/ concerns raised, investigations will be carried out either in-house by Business Ethics function, Legal or People function or by external parties such as independent accountants with specialized forensic accounting expertise and/ or lawyers with access to criminal law expertise, or where deemed appropriate, by the police. The decision whether to use internal or external investigation services, or a combination of both, will be made by the Group Business Ethics and Compliance Officer on the advice of the Divisional or Group General Counsel, with the assistance of local legal counsel as necessary.

Subject to provisions under law, the concerned employees and investigators shall ensure that the identity of those filing grievances filed related to suspected fraud/ unethical conduct or violation of Securitas Values and Ethics code shall be kept confidential until the investigation is completed and it is ascertained that wrongdoing has been committed.

Key tasks in managing fraud complaints are briefly highlighted below:

4.1 Investigation log

An investigations log is typically a log of all reported suspicions, including those dismissed as minor or otherwise not investigated. The log will contain details of actions taken and conclusions reached. It is an important tool for managing, reporting, and evaluating lessons learned.

4.2 Investigation

An investigation team should be put together with the appropriate roles represented.

- The objectives of the investigation should be clearly identified
- Identify the resources required, the scope of the investigation, and the timescale
- Prepare an action plan and delegated roles and responsibilities in accordance with the skills and experience of the individuals involved
- Reporting procedures and procedures for handling and recording evidence should be clearly understood by all concerned

4.3 Evidence

A main objective in an investigation must always be to secure or preserve sufficient evidence, to be able to prove a case of wrongdoing. Local laws and regulations must of course be followed when it comes to how evidence can be treated. Seek legal advice to know if it is possible to secure access to or to allow seizure of the evidence.

It is important that control is taken of any physical or electronic evidence so it cannot be removed or destroyed by the suspect(s). This might have to be done early in the investigation before any witness statements is collected or interviews of suspects are conducted.

It is important that proper records are kept from the start, including accurate notes of when, where and from whom the evidence was obtained and by whom including complete details of all interviews and statements obtained as part of investigation procedures. The Business Ethics team, or legal counsels, can advise on how this should be done.

4.4 Course of action

The course of action to take with regard to a case of fraud can differ. The actions may include one or a combination of actions.

- Internal disciplinary action according to local HR and disciplinary guidelines
- Action through civil courts to recover losses
- Action against the individual(s) concerned in a police managed enquiry
- A combined response: civil action to recover misappropriated assets is taken in combination with a police investigation

4.5 Lessons learned

It is important to learn from experience after an identified incident of fraud. Lessons learned could be collected by examining the circumstances and conditions which allowed the fraud to occur, including identifying potential system failures or areas of weakness and suggesting improvements to systems, processes and procedures. The appropriate remedial actions should be taken to avoid more fraud incidents.

For further details on our Group Whistleblower policy and Investigation procedures, please refer Policy 26 Group Whistleblowing Policy.

5 Roles and responsibilities in Fraud Response and Control

Below are some roles that will probably have responsibility for fraud risk management. It is up to each organization to decide what roles should have what responsibility.

- Managers: generally, managers are able to take responsibility for detecting fraud in their area
- Financial controller/finance manager: it is common that the financial controller/finance manager has the overall responsibility for the organization's response to fraud
- HR: The HR department will usually have responsibility for any internal disciplinary procedures and to give advice on issues relating to employment law, or equal opportunities
- Legal advisers (internal or external): Legal advice should be sought as soon as a fraud is reported, for example regarding civil, internal, and criminal responses, and recovery of assets
- IS/IT: IS and IT staff can provide technical advice on IT security, capability and access. They can also give advice if computers have been used to commit the fraud, or if they are required for evidential purposes
- Business Ethics (BE): The Divisional and/or Country BE Responsible will usually have responsibility for investigating concerns around BE matters, BE team may work with legal, HR and ICFR colleagues or any external consultants to investigate concerns brought to attention.
- Communications: The communications department should prepare Q&A documents, statements to the press, etc., if news about the fraud becomes public
- External consultants: External expertise in investigation, etc., might have to be brought in.
- Insurers: The Group Insurance department should be informed

6 Applicability

All entities within Securitas Group are recommended to follow these guidelines.

7 Implementation and responsibility

All entities have a responsibility to implement a fraud risk analysis and a fraud strategy. The main responsibility lies with the appropriate managers, including the finance manager/financial controller.

8 Reporting, investigations and consequences of breach

If you have concerns or wish to report a case of fraud you can report to any manager or another official or via email at integrity@securitas.com. You can also raise concerns through Securitas Integrity Line available at securitas.integrityline.com.

9 Review and follow-up

The existence of a fraud risk assessment and fraud strategy will be reviewed and followed up, as part of the Enterprise Risk Management process.

Appendix 1

Examples of common types of internal fraud

SNO.	Primary Risks	Risks Classification	Risks Description
1	Asset Misappropriation	Cash	Stealing from petty cash
			Skimming of cash before recording revenues or receivables (understating sales or receivables)
			Stealing incoming cash through an account set up to look like a bona fide payee
		False payment requests	Employee creating false payment instruction with forged signatures and submitting it for processing
			False email payment request together with hard-copy printout with forged approval signature
			Taking advantage of the lack of time which typically occurs during book closing to get false invoices approved and paid
		Billing schemes	Over-billing clients
			Recording of false credits, rebates, or refunds to clients
			Pay and return schemes (where an employee creates an overpayment to a supplier and pockets the subsequent refund)
			Using fictitious suppliers or shell companies for false billing
		Misuse of accounts	Wire transfer fraud (fraudulent transfers into bank accounts)
			Unrecorded sales or receivables
			Employee account fraud (where an employee is also a customer, and the employee makes unauthorized adjustments to their accounts)
			Writing false credit note to clients with details of an employee's personal bank account or of an account of a company controlled by the employee
			Stealing passwords to payment systems and inputting series of payments to own account
		Non-cash-Inventory and fixed assets	Theft of inventory
			False write-offs and other debits to inventory
			False sales of inventory
			Theft of fixed assets, including computers and other IT-related assets
			Theft or abuse of proprietary or confidential information (client information, intellectual

SNO.	Primary Risks	Risks Classification	Risks Description
			property, pricing schedules, business plans, etc.)
			Receiving free or below market value goods and services from suppliers
			Unauthorized private use of company property
			Employees trading for their own account
		Procurement	Altering legitimate purchase orders
			Falsifying documents to obtain authorization for payment
			Forging signatures on payment authorizations
			Submitting for payment false invoices from fictitious or actual suppliers
			Improper changes to supplier payment terms or other supplier details
			Intercepting payments to suppliers
			Sending fictitious or duplicate invoices to suppliers
			Improper use of company credit cards
			Marked up invoices from contracts awarded to supplier associated with an employee
			Sale of critical bid information, contract details or other sensitive information
		Payroll	Fictitious (or ghost) employees on the payroll
			Falsifying work hours to achieve fraudulent overtime payments
			Abuse of commission schemes
			Improper changes in salary levels
			Abuse of holiday leave or time off entitlements
			Submitting inflated or false expense claims
			Adding private expenses to legitimate expense claims
			Applying for multiple reimbursements of the same expenses
			False workers' compensation claims
			Theft of employee contributions to benefit plans
2.	Fraudulent statements	Financial	Improper revenue recognition
			Holding the books open after the end of the accounting period
			Inflation of sales figures which are credited out after the year end
			Backdating agreements
			Recording fictitious sales and shipping
			Improper classification of revenues
			Inappropriate estimates for returns, price adjustments and other concessions

SNO.	Primary Risks	Risks Classification	Risks Description
			Manipulation of rebates
			Recognizing revenue on disputed claims against clients
			Recognizing income on products shipped for trial or evaluation purposes
			Improper recording of consignment or contingency sales
			Over/under estimating percentage of work completed on long-term contracts
			Incorrect inclusion of related party receivables
			Side letter agreements (agreements made outside of formal contracts)
			Early delivery of product/services (e.g., partial shipments, soft sales, contracts with multiple deliverables, up-front fees)
			Channel stuffing or trade loading (where a company inflates its sales figures by forcing more products or services through a distribution channel than the channel is capable of selling)
		Misstatement of assets, liabilities and/or expenses	Fictitious fixed assets
			Overstating assets acquired through merger and acquisitions
			Improper capitalization of expenses as fixed assets (software development, research and development, start-up costs, interest costs, advertising costs)
			Manipulation of fixed asset valuations
			Schemes involving inappropriate depreciation or amortization
			Incorrect values attached to goodwill or other intangibles
		Fictitious investments	Improper investment valuation (misclassification of investments, recording unrealized investments, declines in fair market value/overvaluation)
			Fictitious bank accounts
			Inflating inventory quantity through inclusion of fictitious inventory
			Inflating inventory quantity through inclusion of fictitious inventory
			Fraudulent or improper capitalization of inventory
			Manipulation of inventory counts

SNO.	Primary Risks	Risks Classification	Risks Description
			Accounts receivable schemes (e.g., creating fictitious receivables or artificially inflating the value of receivables)
			Misstatement of prepayments and accruals
			Understating loans and payables
			Fraudulent management estimates for provisions, reserves, foreign currency translation, impairment, etc.
			Off balance sheet items
			Delaying the recording of expenses to the next accounting period
		Other accounting misstatements	Improper treatment of inter-company accounts
			Non clearance or improper clearance of suspense accounts
			Misrepresentation of suspense accounts for fraudulent activity
			Improper accounting for mergers, acquisitions, disposals, and joint ventures
			Manipulation of assumptions used for determining fair value of share based payments
			Improper or inadequate disclosures
			Fictitious general ledger accounts
			Journal entry fraud (using accounting journal entries to fraudulently adjust financial statements)
			Concealment of losses
		Non-financial	Falsified employment credentials e.g., qualifications and references
			Other fraudulent internal or external documents
3.	Corruption	Conflicts of interest	Collusion with clients and/or suppliers
			Favoring a supplier in which the employee has a financial interest
			Employee setting up and using own consultancy for personal gain (conflicts with the company's interests)
			Employee hiring someone close to them over another more qualified applicant
			Transfer of knowledge to a competitor by an employee who intends to join the competitor's Company
			Misrepresentation by insiders about a corporate merger, acquisition, or investment
			Insider trading (using business information not released to the public to gain profits from trading in the financial markets)

SNO.	Primary Risks	Risks Classification	Risks Description
4.	Bribery and extortion	Bribery	Payment of agency/facilitation fees (or bribes) to secure a contract
			Authorizing orders to a particular supplier in return for bribes
			Giving and accepting payments to favor or not favor other commercial transactions or Relationships
			Payments to government officials to obtain a benefit (e.g. customs officials, tax inspectors)
			Anti-trust activities such as price-fixing or bid rigging
			Illegal political contributions
		Kickbacks	Kickbacks to employees by a supplier in return for the supplier receiving favorable treatment
			Kickbacks to senior management in relation to the acquisition of a new business or disposal of part of the business
			Employee sells company-owned property at less than market value to receive a kickback or to sell the property back to the company at a higher price in the future
			Purchase of property at higher than market value in exchange for a kickback
			Preferential treatment of customers in return for a kickback
		Extortion	Extortion (offering to keep someone from harm in exchange for money or other consideration)
			Blackmail (offering to keep information confidential in return for money or other consideration)

Appendix 2

Example of risk analysis

Column 1: Identified risks
Column 2: Dates of the risk assessment
Column 3: Probability/likelihood: assessment of the likelihood of this risk occurring (high, medium, or low)
Column 4: Impact: assessment of the impact of a fraud in this area (high, medium or low)
Column 5: Assessment of the controls in this area (high, medium or low)
Column 6: Net likely impact: assessment of the likelihood of a fraud not being detected by the controls (high, medium or low)

Example:
The major suppliers have remained the same for a long time without any proper renewal procurement process. This could imply a risk for fraud, especially as the controls appears to be weak.

Identified risk	Assessment. date	Probability/ likelihood	Impact	Controls impact	Net likely	Action
Unchanged major suppliers	Feb 202X	High	High	Low	High	Priority- immediate action
Personal relationships between employees and suppliers	Mar 202X	Medium	High	Low	High	Priority – action within 3 months

Appendix 3

Examples of fraud indicators, risks, and controls

Example 1: Procurement fraud

Fraud in the purchasing or procurement function is a particular risk. The following may be indicators of fraud in the tendering and contract award process.

Before contract award
- Disqualification of suitable tenderers
- 'Short' invitation to tender list
- Unchanging list of preferred suppliers
- Consistent use of single source contracts
- Contracts specifications that do not make commercial sense
- Contracts that include special, but unnecessary specifications, that only one supplier can meet
- Personal relationships between staff and suppliers

During the contract award process
- Withdrawal of a lower bidder without apparent reason and their subsequent sub-contracting to a higher bidder
- Flexible evaluation criteria
- Acceptance of late bids
- Changes in the specification after bids have been opened
- Consistently accurate estimates of tender costs
- Poor documentation of the contract award process
- Consistent favoring of one firm over others

After the award of contract
- Unexplained changes in the contract after its award
- Contract awarded to a supplier with a poor performance record
- Split contracts to circumvent controls or contract conditions
- Suppliers who are awarded contracts disproportionate to their size
- Frequent increases in the limits of liability
- Frequent increases in contract specifications

Example 2: Fraud in the selling process

Fraud risks also exist in the selling process. Those involved can include any combination of the clients' staff and the company's own employees, with or without any collusion.

The following are indicators of fraud in the selling process:
- Overcharging from an approved list or standard profit mark-up
- Short-changing by not delivering the contracted quantity or quality
- Diversion of orders to a competitor or associate
- Bribery of a client by one of the company's own sales representatives
- Bribery of a client by a competitor – no proper explanation of why the contract went elsewhere

- Insider information by knowing competitor's prices
- False warranty claims that are made or paid
- Over-selling of goods or services that are not necessary
- Giving of free issues/samples when not necessary
- Links with cartels or 'rings'
- Bribery to obtain contracts which would not otherwise be awarded
- Issuing invoices or credit notes which do not reflect reality and of which the ultimate payer is unaware
- Issuing credit notes to hide additional discounts or rebates
- The use of sales intermediaries (fixers)
- Sales commission gates, which can often cause misreporting of orders

Appendix 4

Examples of Identifying anomalies

Here are some tools that can be used to identify anomalies.

- Keep up to date with fraud trends and issues
- Based on the fraud risk assessment, design specific tests to detect the significant potential frauds
- Act on irregularities which raise a concern
- Benchmark by for example comparing financial periods, the performance of one cost center
- Examine the systems in place and identify any weaknesses that could be opportunities for the fraudster
- Perform analyses to identify any abnormal trends or patterns, for example in expenditures
- Use specialist software, such as audit tools for data matching analysis, real time transaction assessment, targeted post-transactional review, or strategic analysis of management accounts
- Set up automatic reports for results that fall outside of predetermined threshold values (exceptions) to quickly detect results deviating from the norm
- Set up alerts to be sent directly to a manager when exceptions are identified