# Code of Conduct

**Total Specific Solutions, TSS Europe and each of its direct and indirect subsidiaries (hereinafter "TSS") is committed to conduct its business with honesty and integrity, to follow laws and regulations and to make sure that each employee and business partner is treated respectfully. TSS is proud of its excellent reputation as a responsible and reliable partner. Notwithstanding local company specific values, business principles or other local codes already in place, this Code of Conduct contains the main business standards as rules of ethical behaviour all TSS group employees, directors and officers ("Representatives") must adhere to.**

**Our Code of Conduct conforms with both the OECD Guidelines for Multinational Enterprises and the UN Guiding Principles on Business and Human Rights.**

## Business Integrity

**1.1 Compliance with laws**

TSS must comply with all (local) laws and regulations applicable to its respective business activities. TSS trusts you to make yourself familiar with the applicable laws and regulations and ask your manager how to comply with them. Further guidance in respect of competition laws is provided in Annex 1 – Avoid Anti-competitive Conduct.

**1.2 Prevention of fraud**

Fraud is any dishonest activity that causes actual or potential financial loss to any person or entity. TSS takes a zero tolerance approach to fraud. TSS expects you to conduct your work in a reliable and honest way, not to steal or misuse any company property or property of your colleagues nor to mislead anyone or set up a scheme with the intention that you benefit in a way that was never intended by TSS. Further explanation and examples are set out in Annex 2 - Prevention of Fraud.

**1.3 No corruption or bribery**

TSS takes a zero tolerance approach to bribery and corruption in all jurisdictions where TSS is active in business. Bribery is offering, promising, providing or receiving something of value (such as cash, gifts, favours or benefits) as an inducement or reward in order to gain any commercial, contractual, or personal advantage. Do not in any way (try to) bribe another person, organisation or company. You shall not offer or accept anything of value from someone if such items are beyond what could reasonably be considered ethical and within accepted business practices. Should you reckon that declining or not offering will be against (local) business courtesies, please discuss with your manager. Further explanation and examples are set out in Annex 3 - No Corruption or Bribery.

**1.4 Avoid conflicts of interest**

Representatives must act in the best interest of TSS in all circumstances and are not permitted to engage in any activity that conflicts with the interests of TSS. A conflict of interest exists whenever a Representative's private interests interfere or appear to interfere, with the interests of TSS, and may arise whenever a Representative takes action or has an interest that prevents that person or appears to prevent that person from performing their duties for TSS openly, honestly, objectively and effectively. as explained in Annex 4 - Avoid Conflicts of Interest.

**1.5 Accurate accounting and reporting**

All books, records, accounts and financial statements, time and expense reports should be recorded consistently and accurately, reflecting the true view and conforming to all applicable legal requirements and internal control policies. This requirement applies regardless of whether such records would disclose disappointing results or a failure to meet anticipated profit levels. Any attempt to mask actual results by inaccurately reflecting costs or sales will not be tolerated.

**1.6 Protection of Personal Information**

You are expected to act in compliance with applicable privacy and data security laws, and should only acquire or retain personal information where it is required by law, requested by customers or required in connection with the operation of business activities of TSS. Access to any such personal information is to be restricted internally to those with a legitimate need to know and you must take appropriate measures to protect it and prevent unauthorized access (including using strong authentication practices and multi-factor authentication where applicable). You must not share credentials, disable or bypass security controls, or store personal information on unapproved systems, tools or storage locations. Representative communications transmitted through or by TSS' computer systems are not considered to be private and may be monitored or restricted by authorized TSS personnel. Further explanation and examples are set out in Annex 5 - GDPR.

**1.7 Insider trading**

The shares of TSS' shareholders, Topicus.com Inc. ("TOI") and Constellation Software Inc. ("CSU") and its affiliates Lumine Group Inc. ("LMN") and Sygnity S.A. ("SGN), are listed on the Toronto Stock Exchange and the Warsaw stock exchange respectively. Buying and selling stocks of TOI, CSU, LMN and SGN based on inside non public information is not legally permissible and therefore Representatives and related persons are not allowed to do so. Besides the general rule, there may be certain periods throughout the year in which certain selected Representatives of TSS will not be allowed to buy or sell any shares. Those periods are called black-out periods. Disclosure of commercially or financially sensitive information is generally prohibited as it may affect the price of publicly traded shares. Prior to full public disclosure of information, Representatives must not discuss or make public important business developments involving TSS or any other relevant affiliate, even in the most casual manner, with family, friends, outsiders or other Representatives who do not need to have such information. Giving a "tip" to someone else based on inside information is illegal. Both the discloser and the person given the "tip" may be subject to significant criminal and civil penalties if securities are traded based on a disclosure of inside information. Further guidance is provided in Annex 6 – Disclosure, Confidentiality and Insider Trading Policy.

**1.8 Sanctions, Export Controls, and Trade Compliance**

TSS is committed to complying with applicable international trade laws, including sanctions, export controls and customs laws, and you must comply with the TSS Trade Sanctions Policy. You must not engage in business with restricted or sanctioned individuals, entities or jurisdictions without proper authorization. If you are involved in cross-border transactions, transactions involving unfamiliar jurisdictions, or you notice potential red flags (such as unusual payment structures, unclear end users, or routing through third countries), seek guidance and escalate concerns to your manager and legal@tss-vms.com before proceeding.

## Disclosure of Information

In addition to the insider trading rules, any commercial or financially sensitive information regarding TSS may not be disclosed to the public nor communicated to the press without consulting TSS first. Furthermore, every Representative should refrain from disclosing information, by any means of communication, that may harm the image of TSS or any of its Representatives. You may not disclose any confidential information regarding TSS, its customers and suppliers. Always take appropriate measures to keep such information strictly confidential.

## Dealing with Suppliers

All companies part of TSS must select their suppliers on the basis of objective comparison criteria, including commercial conditions, reputation, sustainability and reliability. Suppliers should only be contracted if they adhere to similar standards as reflected in this Code of Conduct.

## Responsible Work Conduct

The IT and communication systems of TSS are built for business purposes. The capacity, software and security are not designed for private purposes and any use for private purposes should be limited as much as reasonably possible. Representatives must always use best efforts to protect the assets of TSS, including facilities, computer equipment, and any other physical property, from unauthorized use, loss, theft or misuse. All assets should be used for legitimate business purposes only and not for personal benefit. The use of any TSS funds or assets for any unlawful or improper purpose is strictly prohibited. Claims for travel and entertainment expenses must be fair and should only relate to TSS business. Further guidance is provided in Annex 7 - Responsible Work Conduct and Annex 7a – AI Policy.

## Responsible Work Environment

TSS continuously strives to improve working conditions and pays special care to the health, safety and inclusivity aspects within your work environment. Each Representative is responsible for creating and maintaining an inclusive workplace culture in which all colleagues are respected and that is free of harassment, bullying and discrimination. TSS will not tolerate any use of drugs and inappropriate use of alcohol during working hours or even outside working hours when such use has an influence on your performance during working hours. Representatives must not take unfair advantage of others through manipulation, concealment, abuse of privileged information, misrepresentation or any other intentionally unfair dealing. Further guidance is provided in Annex 8 - Responsible Work Environment.

## ESG / Corporate Responsibility

TSS is committed to taking its responsibility in the fields of ESG, energy, waste, purchasing, personnel, health and safety very seriously and all of its Representatives are expected to do the same.

## Proper Authorisations and Approvals

We expect you either to notify your manager or to obtain proper authorisations with respect to all business matters and where so required. We consider such behaviour essential business practice. It is not the intention to restrict the entrepreneurial spirit, but to mitigate the risk of inappropriate representation and binding of TSS. Further guidance is provided in Annex 9 - TSS Authorization Scheme.

**SPEAK UP!** - Each Representative has an obligation to be familiar with the terms of this Code of Conduct, and to ask questions, seek guidance and express concerns with respect to its terms. Any person who has knowledge of a potential, suspected, or known violation of this Code of Conduct has an obligation to report this information to their manager, or alternatively, to TSS by contacting TSS through one of the TSS Speak Up Channels. Further guidance is provided in Annex 10 - Speak Up!

TSS will not permit retaliation against any Representative who, in good faith, seeks advice or reports improper behaviour under this Code of Conduct. Any violation of this Code of Conduct, including a failure to report a violation may lead to disciplinary action being taken up to and including dismissal for cause. Although any Representative who discloses their own misconduct may be subject to disciplinary action, TSS may consider such voluntary self-disclosure as a mitigating factor.

# Code of Conduct

# Annex 1 – Avoid Anti-competitive Conduct

## Further explanation

Almost all countries in which TSS is active have competition laws (or antitrust or anti-cartel laws). In essence the core of these laws is always the same: companies are not allowed to share any form of confidential information with their competitors. Of course, cartel or price-fixing between competitors or agreeing (even informally) with competitors to respect each other's customer groups or focus is clearly prohibited. Please note that certain competition restrictions may also apply to several businesses within TSS that may be considered competitors in a given market segment.

The cartel prohibition even goes much further. Providing a representative of a competitor with information on our current (price) policy, our intended action or even recent decisions relating to the commercial policy is a violation of the competition laws.

It may occur in daily practice that you meet with competitors. Talking to competitors is always very risky and if you choose to do so, it is your responsibility that no sensitive information is exchanged. In any case, you have to make absolutely clear in a conversation that you refuse to disclose or receive sensitive information even though such an information exchange may appear tempting or even useful for business.

The fines for violations of the competition rules are very severe and they apply to both the companies concerned and the individuals infringing competition law. In Europe, fines imposed on companies may be up to 10% of last year's group revenue.

Naturally, there are areas of competition law which are more nuanced, like: can we co-operate with this competitor in R&D? Or can we buy products together? Or can we ask for or provide exclusivity to a supplier or a distributor/customer? These are all questions which require a delicate legal and economic analysis. Please do not make any decisions on such issues without prior consultation with your manager so that legal advice can be obtained in advance. Another aspect of competition law concerns control of companies having a strong position on a given market. If a company has a very strong position on a market (quasi-monopoly or dominance) the commercial freedom is significantly restricted by some of the competition laws. Market dominance is usually deemed to exist where we can set our terms and conditions without having great consideration to our competitors.

## Example

What should you do when a competitor (even a former colleague, friend or relative) provides you with commercial information about their company?

Tell them that you are not allowed to talk about customer/supplier requests, the state of negotiations with customers/suppliers and/or about our negotiation strategy. It is however permissible to talk about end customers satisfaction with the supplier. As a rule of thumb you should keep in mind for any contact with competitors that you are not allowed to exchange information which, as a result, may prompt us or any competitor to adapt our/his business strategy, prices, product portfolio, production process etc. or at least to consider doing so.

## Q&A

**Question 1:** I received confidential business information about a competitor. What should I do?

**Answer 1:** It is decisive where the information comes from. If, for instance, the customer voluntarily provides you with information about the terms and conditions of your competitor, such information is legitimate and you can also use it in your own price negotiations. If such information is however received from a competitor, the principles explained in the examples above apply. Generally, you are not allowed to use such information. Immediately speak to your manager about the situation.

**Question 2:** I am participating in a working group in which representatives of competitors also participate. I sometimes pick up relevant information at these events. What can I do with this information?

**Answer 2:** The principles explained in the examples above apply. In personal conversations you must reject such an information exchange. You are not allowed to use such information. Immediately speak to your manager about the situation.

**Question 3:** A (big) customer group requests higher discounts and in return they will make sure that all their (new) group members will use our software. May I grant such a discount?

**Answer 3:** Make sure you contact legal@tss-vms.com so that prior legal advice can be obtained before agreeing with this customer on a discount, even though it is the wish of the customer. In many countries in which we do business, dominant companies are not allowed under competition law to set discounts freely.

**Question 4:** An employee of a competitor asks me if the information they have about our commercial practice is correct. What should I do?

**Answer 4:** In this case you have to distance yourself from such discussion and make clear that you do not want to participate in such an information exchange. Even the "confirmation" that the information a competitor has about our commercial practice is correct, will constitute a serious violation of the competition rules around the world. This also applies to other sensitive information relating to customers, pricing, turnover, sales figures, capacities, investments, innovations and technologies. There are even cases in which the competition authority has ruled that sharing information about commercial practices of competitors via customers infringes competition law.

# Code of Conduct

# Annex 2 – Prevention of fraud

## Further explanation

Fraud is a deception that is deliberately practiced to secure unfair or unlawful gain and includes deceit, concealment, skimming, forgery or alteration of (electronic) documents. Fraud may be committed by one person or by two or more persons (collusion) and may involve internal and/or external parties such as suppliers or customers. TSS (including CSI) maintains a zero-tolerance approach for its companies, Representatives and business partners with regard to fraud; in general this will lead to instant dismissal. Participating in fraud for customers, suppliers or other stakeholders is also not permitted.

Managers are responsible for ensuring they have identified fraud risks, having appropriate controls in place, and tracking the effectiveness of controls on an ongoing basis. Managers must make themselves familiar with the types of improprieties that might occur within their area of responsibility, and must orient their personnel to be alert to any indications of potential fraud. Representatives who detect or suspect any (potential) fraud must immediately report the matter to TSS' confidential counselor (*vertrouwenspersoon*) at codeofconduct@tss-vms.com, or TSS' CFO at cfo@tss-vms.com or please refer to Annex – Speak Up! for all other ways of (anonymous) contact. In addition, TSS may initiate random checks on its companies to verify compliance with this Code of Conduct.

## Example

A Representative has selected a specific supplier as this supplier provides the Representative with certain benefits or a kick back fee to be paid in person. This is considered to be theft because the purchase price for TSS could apparently have been lower than the contracted price. Such behaviour seriously harms TSS and may result in the instant dismissal of the Representative concerned.

## Q&A

**Question 1:**
I suspect a colleague of fraud and want to know what I must do?

**Answer 1:**
Please report the situation directly to TSS' confidential counselor (*vertrouwenspersoon*) at codeofconduct@tss-vms.com, TSS' CFO at cfo@tss-vms.com or please refer to annex – Speak Up! for all other ways of (anonymous) contact. If you suspect fraud, do not discuss the matter with any of the individuals involved and do not attempt to investigate or determine facts on your own. The informed person will review the matter and take the appropriate steps.

**Question 2:**
I suspect my manager to be involved in a fraud scheme and want to know what action to take.

**Answer 2:**
Report the situation to TSS' confidential counselor (*vertrouwenspersoon*) at codeofconduct@tss-vms.com, TSS' CFO at cfo@tss-vms.com or please refer to annex – speak up! for all other ways of (anonymous) contact. The matter will then be reviewed without prejudice and investigated.

**Question 3:**
Will there be consequences for me if I misjudged the situation?

**Answer 3:**
TSS appreciates its Representatives being committed to the company's interests and willing to raise concerns regarding suspicious situations. The ability to investigate and remediate fraud successfully depends on prompt and confidential reporting. You will of course not be adversely affected for raising concerns about fraudulent conduct where in hindsight your judgement proved to be incorrect. It is never allowed to accuse someone intentionally without a justifiable reason.

**Question 4:**
A customer requests me to adjust an invoice not in conformity with the actual circumstances so that the customer can book the expenses more favorable. Is this allowed?

**Answer 4:**
This is never allowed. This is considered as helping a customer with committing fraud.

# Code of Conduct

# Annex 3 – No Corruption or Bribery

## Further explanation

TSS is doing business around the world and its Representatives are subject to anti-bribery laws of many countries. TSS, its Representatives and business partners should comply with all applicable antibribery laws, also when doing business abroad. It is TSS' policy that bribery of persons is always forbidden in all countries it does business, even if in a certain country exceptions are legally allowed.

**What conduct is considered bribery?**

Anti-bribery laws prohibit persons or companies from offering, promising or paying a bribe to public officials or persons in the private sector to influence such persons in their (official) acts or function. Likewise, it is prohibited to solicit or accept a bribe. A "bribe" may consist of any advantage or benefit that has a value. Small payments or benefits are therefore not per se excluded. The mere offering or promising of a bribe is prohibited. The bribe does not have to be actually paid or accepted. The person offering, promising or soliciting the bribe does also not necessarily have to be the recipient of the bribe (indirect payments are also prohibited). Antibribery laws in the various countries are quite broad and may apply not only to the actual briber and the person being bribed but also to anyone knowingly cooperating in, approving, directing or covering up the bribe. Most anti-bribery laws apply if a payment, offer or promise is made in exchange for some type of improper action or omission by the bribed person (or a contact of that person). An important factor is whether any influence is exerted to obtain or retain business or a business advantage such as (a) granting of a licence or permit or awarding an assignment in circumstances where it may not otherwise be granted, (b) taking the decision not to investigate or prosecute an alleged offence by a company, or (c) providing confidential information to a company. It is not required that the intended recipient of the bribe is directly involved in awarding or directing the business advantage. The use of influence to establish a certain result may be sufficient.

**Representatives (or someone on their behalf, or a family member thereof) must not:**

- give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given;
- give, promise to give, or offer, a payment, gift or hospitality to a government official, agent or representative to "facilitate" or expedite a routine procedure;
- accept payment from a third party that you know or suspect is offered with the expectation that it will create a business advantage for them;
- accept a gift or hospitality from a third party if you know or suspect that it is offered or provided with an expectation that a business advantage will be provided in return; or
- threaten or retaliate against another worker who has refused to commit a bribery offence or who has raised concerns under this Code of Conduct.

**Corporate hospitality and promotional expenses, gifts and entertainment**

Hospitality and promotional expenditure as well as offering and accepting gifts and entertainment are not considered bribery (a) if reasonable and proportionate as regards the value and timing, the impression conveyed to third parties and the type of gift or entertainment, and (b) if there is no intention to induce a person to improperly perform their function, or to secure a business advantage or not.

As a general rule, you should never offer or accept a gift or entertainment with **a value exceeding EUR 50** or the local currency equivalent. If a gift gives you an uncomfortable feeling and/or you would not feel comfortable if all your colleagues would know of it you should never accept such a gift without consulting with your manager. Bona fide hospitality and promotional or other business expenditure which seeks to improve the image of TSS, to present the TSS' products and services, or to establish cordial relations, is recognized as an established and important part of doing business. However, the recipient of any gift and/or hospitality should not be given the impression that they are under an obligation to confer any business as a result of the hospitality itself, or that their independence will be affected by receiving any such hospitality.

Representatives must consider whether in all the circumstances the gift or hospitality is reasonable, proportionate and appropriate, including the following considerations:

- what the intention of the gift or hospitality is;
- whether there is any secrecy involved;
- the value of the gift/hospitality (the higher the value, the less likely it is to be appropriate); and
- how the gift or hospitality would reflect on TSS if the details were made public.

Circumstances that are usually acceptable include:

- occasional lunches and dinners with existing and prospective customers and suppliers, unless to be considered disproportionate;
- occasional attendance at sports, theatre and other cultural events, unless to be considered disproportionate; and
- gifts with a value of maximum EUR 50 or other small promotional items.

Circumstances which would not be appropriate include:

- gifts of cash or a cash equivalent;
- gifts in your name, not in the TSS' name;
- secret gifts;
- any gifts given to or received from suppliers, government officials or representatives to obtain or retain an improper advantage; and
- accepting any gifts from employees reporting to you and that were purchased with company funds.

As a general rule lunch/dinner invitations may be accepted if (i) they are not disproportionate/decadent; (ii) the costs do not substantially exceed the cost you would be prepared to pay privately for a lunch/dinner; and (iii) this does not occur too frequently. Anything that does not meet these requirements must always be discussed with your manager.

If you receive a gift, hospitality and/or entertainment with a value exceeding EUR 50 you must consult with your manager before accepting it. In case you have any doubts about the appropriateness of hospitality, entertainment or a gift that you intend to offer or accept, you must always contact your manager first.

**Facilitation payments and lawful government payments**

TSS prohibits all facilitation payments. Facilitation payments are small payments that are not prescribed by the written regulations in a certain country and are made to secure or expedite the performance of a routine governmental action (e.g. customs clearance). Payments to public officials that are prescribed by written regulations of the official's country, such as fees and payments for various government services, are not prohibited. Payments on top of such legally required amounts are strictly forbidden.

**Liability for and prevention of bribery by associated persons**

TSS could be held liable for bribery by associated persons acting on its behalf. TSS therefore requires that business partners acting on its behalf, such as agents, distributors and representatives, comply with all applicable anti-bribery laws. Consequently, all existing and future business partners must be investigated and selected with bribery risks in mind and the appropriate contractual arrangements should be made with these parties to avoid bribery risks. This investigation as well as the results of it must be documented. Any issues should be immediately notified to your manager.

## Example

You have received a Christmas gift from a local contractor. Although the gift is not exceptionally disproportionate you sense that the contractor expects you to award it a contract in the future. You must inform your manager. You may consider the possibility to politely return the gift. If you keep the gift, you should not award the contractor a contract without prior approval of your manager.

## Q&A

**Question 1:** After a long integration process, the supplier offers our entire team to join his company on one of their company trips. May we accept this invitation?

**Answer 1:** No, you may not. Such a trip is disproportionate as it is of high value. You should also not accept any trips from customers under any circumstances.

**Question 2:** I received a bottle of wine of a supplier worth more than EUR 50. Is this allowed?

**Answer 2:** If you receive a bottle of wine worth more than EUR 50 you must inform your manager and consult with your manager what would be appropriate to do with the bottle (e.g. send/give back, raffle among all colleagues drink the bottle together with all colleagues after work).

**Question 3:** You are sending all your good/important business acquaintances/relations a bottle of wine from TSS funds. As other managers or superiors within TSS are also important to you, you also send them a bottle of wine. Is this allowed?

**Answer 3:** No this is not allowed.

**Question 4**: We invite a few directors of a valued client for drinks and dinner every year. Is this allowed?

**Answer 4:** Corporate hospitality aimed at maintaining a good relationship with clients is allowed. However, no undue influence may be exerted and any impression of bribery must always be avoided. For example, you should not treat the directors to a dinner with costs substantially exceeding the cost you would be prepared to pay privately for a diner.

# Code of Conduct

# Annex 4 – Avoid Conflicts of Interest

## Further explanation

**What is a conflict of interest?**

Representatives are expected to avoid any actual or suspected conflict between the interests of TSS and their own personal interests. TSS recognises that you are part of a family, have friends, act in volunteering jobs, and have specific personal responsibilities and interests. A conflict of interest can arise when you take actions or have personal interests that can interfere with your performance for TSS. You should always declare any direct relationship with someone who may be entering into a contract with TSS to your manager if you have a direct involvement or management responsibility in awarding such a contract.

**Some common examples of conflicts of interest are:**

• Having a financial interest in a company that competes with or does business with TSS;
• Holding a position as a director, officer, employee or consultant of an enterprise that competes with or does business with TSS;
• Taking personal advantage or having a related third party taking advantage of an opportunity in which TSS has an interest;
• Diverting a business opportunity from TSS for personal benefit or using your position within TSS to influence TSS to do business with or give preferential treatment to a friend or relative (or a company with which the friend or relative is associated in a significant role); and
• Using TSS funds, facilities, personnel or other assets for personal benefit or for the benefit of related third parties.
• Hiring or engaging family members, friends or close relatives whether as employee, external contractor or otherwise without the prior written approval of your manager.
• Combining personal travel arrangements with business travel arrangement without the prior written approval of your manager.
• Determining your own remuneration, benefits, or compensation package (direct or indirect).

**Full disclosure**

You are required to disclose to your manager each actual or suspected conflict of interest situation in which you are directly or indirectly involved. You need to make this disclosure as soon as you become aware of facts giving rise to the actual or apparent conflict of interest.

**Guidelines**

If you are unsure as to whether a given situation creates a conflict of interest, raise the issue with your manager. Whilst it is impossible to describe every circumstance where a conflict of interest may arise, the following guidelines will help you avoid conflicts of interest:
a. never allow your personal or financial interests to interfere with your work for TSS;
b. always be able to satisfactorily explain your decision to your manager and to your colleagues;
c. always involve a(nother) management member in any possible conflict of interest situations in order to ensure the four-eye principle;
d. never hire someone you personally know who will work under your authority, unless you have received prior written approval from TSS' CFO cfo@tss-vms.com; and
e. anticipate that for alleged conflicts of interest, appearances do matter!

## Examples

**Example 1:**

You or one of your family members owns a financial interest in an entity that wants to do business with TSS and you are involved in the decision taking. This is a clear issue that should be raised with your manager. Your manager will decide on any measures to ensure that you are not involved on behalf of TSS regarding the possible relationship with this entity.

**Example 2:**

You work in a research and development department of a TSS company. Your family member works at sales department of a competitor. Your family member

## Q&A

**Question 1:** A good friend of mine works for a company that could become an important customer for TSS. Your friend approaches you, as a sales manager, to see whether TSS would be interested in selling to their company. What should I do?

**Answer 1:** Report the situation and relationship to your manager and keep your manager fully informed of the deal and each step in the process. However, since it can result in an important customer for TSS there is no need to say no to the (potential) customer beforehand, unless the dealing would be on non-commercial terms.

**Question 2:** I am asked by a good friend to provide advice to their company that is in direct competition with TSS. Although your friend only seeks technical advice, which seems not to be commercially sensitive, I am not sure what to do.

**Answer 2:** When considering such request, always involve your manager. Your manager will ensure that your question is considered objectively. In addition, be aware that information sharing between competing businesses is in many cases forbidden due to competition laws. Reference is also made to the Annex 1 – avoid anti-competitive conduct.

**Question 3:** I would like my BU or supplier to sponsor a sports team, event, or organization. Is that allowed?

**Answer 3:** It depends. Only if there is a clear and demonstrable business rationale for sponsoring, it may be allowed. Any sponsoring of a sports team, event, or organization in which you, family members, friends or other close relatives have a personal interest is not allowed. Also, arranging for a supplier or a business partner to do so is not prohibited.

# Code of Conduct

# Annex 5 – GDPR

## Further explanation

**What is GDPR?**

The EU General Data Protection Regulation ("GDPR") is a data protection law that regulates the way businesses process and manage personal data. In summary, the GDPR applies to any business that processes personal data by automated or manual processing. "Processing" means any operation performed on personal data, such as collection, usage, storage, transfer, dissemination or erasure. Even if your business only processes data on behalf of other companies, you still need to abide by the GDPR.

**What is personal data i.e. customers and employees?**

Personal data refers to any information that relates to an identified or identifiable, living individual. This can include:

- name
- address and phone number
- location
- income and banking information
- … and more

Personal data that has been de-identified, or pseudonymized, but that can still be used to re-identify a person also falls under the scope of the GDPR. However, personal data that has been rendered irreversibly anonymous in such a way that the individual is no longer identifiable is not considered to be personal data and thus not governed by the GDPR.

**Possible penalties?**

When a company does not comply with GDPR the company risks a fine of up to 4% of the company's worldwide annual revenue from the preceding financial year (Topicus.com or Constellation Software Inc. ("CSI") could be included in this calculation) or EUR 20 million, whichever is greater.

**How do I comply with GDPR?**

As the protection of personal data becomes more important, it is key that everybody complies with GDPR, both when it comes to internal (e.g. employees) and external (e.g. (end-)customers) data.

In essence the core of complying with GDPR consists of:

- Always enter into a (sub)processor agreement with your customers and suppliers;
- Make sure that personal data is only processed for the purposes as agreed upon with the owner of the personal data;
- Make sure that personal data is only accessible by authorised people (i.e. protected);
- Make sure that personal data is not disclosed to unauthorised people and/or for purposes which are not agreed upon by the owner of the personal data;
- If you need to transfer/disclose personal data for the purposes as agreed upon with the owner of the personal data make sure that this is done in a safe and protected manner.

In addition every business unit has its own policy as to how data (internal and external) is to be used and protected in their specific case. Make sure you have seen this policy and know how you can comply with this policy.

It is necessary to prevent personal data from ever leaking, however if it does occur, it is important that the incident is reported to TSS as soon as possible. Please ensure that all information security incidents are reported to legal@tss-vms.com as soon as possible and in any event *within 72 hours* after any (suspected) incident by means of filling in and circulating the Incident Reporting Form (you can request such form by any managing director). For the avoidance of doubt if any manager gets informed about any (suspected) incident they are obligated to immediately report this as described above.

## Examples

**Example 1:**

You have sent an email with a wrong attachment which contains personal data to a colleague from finance. Although your colleague is used to working with confidential information this is a breach of the GDPR. You must inform the recipient of the email and request such person to delete your email and attachment. Also you must inform your manager.

**Example 2:**

You lost your USB stick which contains personal data of your customers. You did protect the USB-stick with a password. Nevertheless you should immediately report it to your manager, your IT contact person and to legal@tss-vms.com. Even though the USB stick is password protected this loss may still qualify as a data breach that needs to be reported.

## Q&A

**Question 1:** Our software generates certain data which includes personal data. A company offered us a monthly fee for delivering such data to them. May we sell this data?

**Answer 1:** No. Personal data may not be processed for purposes which are not agreed upon by the owner of the personal data. You may only sell this data if all the people whom this data relates to have agreed in writing to this specific purpose.

**Question 2:** My colleague asked me to forward a CV to them by email. May I do so?

**Answer 2:** You may only do so if it is necessary for this colleague to see such CV for the specific purpose for which you received such data. Plus you always need to make sure that these kind of confidential documents are deleted from all media (including all email folders and trash folders on your computer) when the purpose to have this data is no longer there.

**Question 3**: I forgot my laptop in the airport. What should I do?

**Answer 3:** You have to immediately report this to your manager and IT contact person.

**Question 4:** I forgot that I had printed documents which contain personal data of our employees. As a result these documents were present on the printer the whole day and I don't know if people have seen them. What should I do?

**Answer 4:** You have to report this to your manager as soon as possible. Even suspected incidents may need to be reported.

# Code of Conduct

# Annex 6 – Disclosure, Confidentiality and Insider Trading Policy

## Definitions

"**Corporation**" means each of Topicus.com Inc., Constellation Software Inc, Lumine Group Inc and Sygnity SA.

"**Executive Group**" means the Chief Executive Officer and the Chief Financial Officer of the Corporation.

"**Insider Trading**" refers to an employee, officer or director of the Corporation or any of its direct or indirect affiliates or subsidiaries, purchasing or selling or otherwise monetizing securities of the Corporation while in possession of undisclosed Material Information.

"**Material Information**" means a fact, change or event that would reasonably be expected to have a significant effect on the market price of the securities of the Corporation.

"**Operating Group**" means each of the following operating groups of the Corporation: TSS Blue, TSS Public, and Topicus.

"**Restricted Persons**" means the following persons:

a) the Executive Group, the directors of the Corporation, and the directors of Topicus.com Coöperatief U.A.;
b) the Chief Executive Officer and Chief Financial Officer of each Operating Group of the Corporation; and
c) any person having access to the consolidated financial results of the Corporation in advance of such results being made public.

"**Tipping**" refers to disclosure of undisclosed Material Information to third parties, other than (i) if required by applicable law, or (ii) if such disclosure is made in the necessary course of business and to a person who has a duty of confidentiality to the Corporation or its affiliates.

## How do I comply?

1. Anyone possessing Material Information which has not been generally disclosed to the public must maintain its confidentiality and refrain from Insider Trading or Tipping.

2. Only the Executive Officer is authorised to disclose Material Information to the media, analysts, shareholders or the general public.

3. Prospectuses, management information circulars, interim financial statements, annual financial statements, the related MD&A, and all related press releases must be reviewed and approved in advance by the Audit Committee and the Board of Directors of the Corporation.

4. If any Material Information is undisclosed, the Executive Group shall promptly disclose the Material Information to the public as required by applicable law.

5. Any employee who becomes aware of undisclosed Material Information should promptly disclose that information to the Executive Group.

6. The Restricted Persons shall not purchase or sell or otherwise monetize securities of the Corporation during the period that begins on the first day of each fiscal quarter and ends on the third business trading day after the financial results of the Corporation for the prior fiscal quarter have been publicly disclosed.

7. Any person who violates this Policy may face disciplinary action as may be appropriate under the circumstances.

## Examples

**Example 1:**
You read certain rumours on the internet in respect of the Corporation which you know are not true. You want to set things straight and respond with the right information. Do not discuss or post any information relating to the Corporation or any of its subsidiaries or trading in securities of the Corporation in Internet chat rooms, newsgroups, bulletin boards, web logs or other electronic media available to the public as you may possibly disclose information that is not publicly available yet.

**Example 2:**
You know M&A is working on a really large acquisition and think that once this acquisition will be completed the stock price of the Corporation may increase. In anticipation of this transaction, you are already buying additional shares in the Corporation which will hopefully increase in value once the transaction has been announced. This is obviously not allowed as you have the possession over material information that other shareholders do not have. Besides violating the insider trading policy, you may also violate security or stock market laws and regulations and may become subject to large fines or imprisonment.

## Q&A

**Question 1:** I want to buy or sell shares in the Corporation outside a Black Out Period, but am not fully sure whether I may have the possession of certain Material Information that may not be publicly known to the market yet. Am I allowed to trade?

**Answer 1:** No. If you have any doubts, please contact TSS' CFO (cfo@tss-vms.com) or General Counsel (legal@tss-vms.com) prior to trading.

**Question 2:** I receive a phone call from a financial analyst from a large financial institution/bank with some questions about my business. Am I allowed to answer or provide some general information that is already publicly known to the market?

**Answer 2:** No. You are not allowed to share any information with external parties as any information will have to be shared in a consistent manner and in accordance with applicable policies. Therefore, disclosures shall only be made by (a representatives of) the Executive Group.

# Code of Conduct

# Annex 7 – Responsible Work Conduct

## Further explanation

**Company assets and funds**

All property of TSS may only be used for the intended business purposes. This includes but is not limited to:
a. physical assets such as office equipment, tools, technical equipment and IT equipment; b. software, intellectual property rights and confidential information; and c. company funds, bank accounts and other company resources. You must use company property only for the intended business purposes and guard it against misuse, loss or theft. Company funds may only be used for TSS business purposes and may never be used for private purposes. It is not permitted to combine business expenses such as lunches and travel trips with personal holidays with family members or friends without prior written approval of your manager.

**Use of IT and communication**

TSS' IT systems, software and all means of electronic communication, including the internet, shall be primarily used for business purposes and in TSS' interest. The capacity for communications, antivirus software and licenses are implemented for business use and not for private use. Though some proportionate personal use of these systems may be inevitable, such use should be limited as much as possible and may never interfere with the intended business purposes. The IT systems may never be used in any way that can result in the storing or communicating of content that breaches applicable legislation, harassment of colleagues or third parties, or discrimination or other improper behaviour. Only if there are justifiable suspicions that you do not act in accordance with this Code of Conduct or applicable legislation, TSS preserves the right to monitor your use of the IT systems and electronic communications in accordance with applicable laws.

Responsible use of IT also involves IT security. Every Representative must always use all IT systems responsibly and protect the Company's systems, accounts and data from unauthorized access. This consists of for example:

- Never click on suspicious links in emails without consulting the person you received it from and/or your IT contact person;
- Always use sensible and strong passwords which are not easy to guess or crack;
- Do not share your passwords or other credentials, do not let others use your accounts, and never attempt to disable or bypass security controls; use multi-factor authentication where it is available or required;
- Always comply with internal authorisation schemes before transferring money;
- Always make sure before sending an email that any attached document is actually the document you wanted to send.
- Never use your company laptop to visit websites with inappropriate content and/or download files from websites which are to be considered of high risk.
- Be vigilant against phishing, social engineering and suspicious communications, and promptly report suspected security incidents, breaches, lost or stolen devices, or unusual system behaviour to your manager and your IT contact person.

**Intellectual property**

TSS has developed or purchased licences for valuable intellectual property, including inventions, product names, software, engineering drawings, and confidential information for its business operation. You must strictly comply with the applicable intellectual property laws and licence conditions. Unauthorised use or disclosure of company intellectual property is forbidden and the intellectual property right of third parties must be fully respected.

**Generative Artificial Intelligence**

TSS is committed to fostering a culture of innovation and collaboration. Generative AI (i.e. a category of artificial intelligence that generates output from data it has been trained on) has emerged as a game-changing technology that has great potential to benefit TSS and empower TSS Representatives to achieve new levels of success.

TSS is equally committed to managing the significant risks posed by the use of generative AI to TSS' ability to maintain adequate information security measures, protect intellectual property rights, and ensure accuracy and integrity of its work products. Powerful tools like generative AI must always be used responsibly in a manner designed to mitigate the risk of exposing TSS to unintended adverse consequences. The attached Generative AI-policy is intended to establish guidelines for the proper use of generative AI by all TSS Representatives.

## Examples

**Example 1:**
You are the coach of the soccer team of your child and urgently need to send a mailing to various sponsors for the next soccer tournament. It is not allowed to use the company e-mail service for this. Your company e-mail address contains the trade name of your company and interferes with the business purposes of this name. This can damage the image or reputation of TSS. These mailings should be done with your private e-mail address outside office hours.

**Example 2:**
A Representative provides its children with office supplies to do their homework. This is not allowed and is considered to be theft.

**Example 3:**
A Representative downloads illegal software that they prefer for enhancing their business presentation. This endangers the safety of TSS' IT- systems and breaches third-party intellectual property rights.

## Q&A

**Question 1:** You receive an e-mail, apparently from a colleague, containing all kinds of confidential information. The e-mail turned out not to be intended for you but for another person within the company. What should you do?

**Answer 1:** Please make sure to (permanently) remove this email to make sure that the confidential information cannot be misused by someone and notify your colleague immediately.

**Question 2:** I sometimes take my TSS' laptop or USB stick at home to be able to work during the evening. Of course, there might a possibility that my laptop could be stolen in case of a burglary?

**Answer 2:** Never leave the laptop or storage device unattended in your car or in public places. Ensure that the laptop or USB stick uses state-of-the-art encryption and passwords to protect company sensitive information. Always lock your computer when you are not working on it. Ask your IT department for assistance before you store data on such devices. If the laptop has been stolen, report this immediately to your manager and your IT contact person.

**Question 3:** I am planning to work some days from home. I always drink coffee at work but I know that I am out of coffee beans at home. Am I allowed to take some coffee beans from work?

**Answer 3:** No, you are not. This is considered to be theft.

**Question 4:** I have traveled to another country for a business meeting. After the meeting I get informed that the flight back is materially delayed and I will have to stay another day abroad. In addition I get informed that I will get a refund/compensation from the flight company because of the delay. Am I allowed to keep this refund/compensation?

**Answer 4:** No, you are not. Company funds paid for your flight and therefore the refund/compensation belongs to the company as well.

# Code of Conduct

# Annex 7a – AI Policy Last Updated: 23 April 2026

Topicus and each of its operating groups (i.e. Topicus OG, TSS Public and TSS Blue), business units and other operations globally (collectively, the "Company") is committed to fostering a culture of innovation and collaboration. Generative AI (i.e. a category of artificial intelligence that generates output from data it has been trained on) has emerged as a game-changing technology that has great potential to benefit the Company and empower Company Staff (as defined below) to achieve new levels of success.

The Company is equally committed to managing the significant risks posed by the use of generative AI to the Company's ability to maintain adequate information security measures, protect intellectual property rights, and ensure accuracy and integrity of its work products. Powerful tools like generative AI must always be used responsibly in a manner designed to mitigate the risk of exposing the Company to unintended adverse consequences.

This policy is intended to establish guidelines for the proper use of generative AI by all Company Staff (as defined below).

## Scope of Policy and Overview

**General.** This policy is designed to help Company Staff (as defined below) effectively and responsibly use generative AI tools while considering key ethical and legal considerations. By adhering to this policy, we can continue to innovate and grow while upholding the highest ethical and legal standards. **Failure to abide by this policy may result in disciplinary measures, up to and including dismissal and/or legal action.**

**Guidance on Policy.** For guidance on proper disclosure methods and any related questions, please consult with your supervisor or the legal department. Your commitment to transparency and responsible generative AI use is essential to our organization's success and our collective growth.

**Amendment of Policy.** Generative AI is a fluid and evolving technology space and access to, and use of, generative AI platforms may be restricted in the future. The Company reserves the right to amend this policy whenever it deems it to be appropriate or required.

**Application of Policy.** This policy applies to all employees, executives, consultants, agents, vendors, and other third parties ("**Company Staff**") who have access to Company Data (as defined below). This policy applies to use of generative AI tools (whether publicly available, embedded in third-party software, or Company-licensed) by Company Staff in their roles within the Company. Company Staff may utilize generative AI applications as a supplement to other tools they rely upon to deliver services to our customers only in accordance with this policy. Examples of publicly available generative AI tools include chatbots like ChatGPT, Gemini, and MS Copilot, and code generators like Claude Code and Cursor. The Company may also acquire enterprise solutions that use generative AI. If your work includes the use of Company-licensed generative AI tools, your supervisor will provide further guidance on any license restrictions applicable to your use of such tools. For the Generative AI Risk-Assessment (self assessment), see Appendix A.

**Company Data Defined.** The term "**Company Data**" should be interpreted broadly for purposes of this policy, and includes, but is not limited to, at least the following: all Company business information and all personal data (whether of employees, executives, contractors, consultants, customers, acquisition targets, users, or other persons) that is accessed, collected, used, processed, stored, shared, distributed, transferred, disclosed, destroyed, or disposed of by any of the Company systems; all proprietary information and intellectual property (including, but not limited to, source code, designs, schematics, product roadmaps, product plans, product specifications, market analyses, white papers, strategy documents, financial information, internal communications, customer lists, customer files, customer contact information, customer contracts, customer's or third-party proprietary-, inside- or confidential data, and any non-public Company information). Company Data includes information in written, electronic, audio, video, or any other form or medium.

## Company Policy for Using Generative AI; Do's and Don'ts

- **Accounts.** If your work for the Company involves the use of Company-licensed generative AI tools, you may **not** use your personal account with a generative AI tool for your Company role.

- **Confidential Information**. You may **not** include any personal, sensitive, proprietary or confidential information in your prompts to generative AI applications, such as ChatGPT, unless a thorough risk-assessment has been made as to the use of such information and the risk-assessment has been signed off by the Managing Director of your Company. (Note: This includes source code, client confidential information and documents, passwords and other credentials, protected health information, personnel material, names, addresses, likenesses, information from documents marked "Confidential", "Sensitive", or "Proprietary", or any other non-public Company information that might be of use to competitors or harmful to the Company if disclosed.)

- **Integration and Attribution.** You may **not** incorporate or integrate generative AI based tools or AI-generated outputs into Company commercial software products and offerings , unless a thorough risk-assessment has been made as to the use of such tools and the risk-assessment has been signed off by the Managing Director of your Company . All Company Staff must clearly and conspicuously identify and/or label all AI-generated content in internal documentation, including the source generative AI application. Exploration or pursuit of, development, or incorporation into Company products or services of any functionality that can in any way be considered to be generative AI, must be approved in advance by your Managing Director as per the procedures set out in this AI policy.

- **Disclosure.** Where so required by applicable laws and/or regulations, you **must** disclose the use of generative AI in materials produced within your organization where such materials are relied upon by others for decision-making, are distributed beyond your immediate team, or are intended for external use. Inform your supervisor (or project owner) when you have used generative AI to perform a task, no matter how small. When presenting or submitting work that includes AI-generated content, you must clearly indicate the specific sections or elements that have been created or influenced by generative AI technologies. Where AI-generated content is included in your textual or visual graphic external-facing work (such as verbiage and images used in publications and other marketing content), acknowledge the use of generative AI and clearly identify the AI-generated content. For example, "Content used in compiling this report was sourced from ChatGPT". You may not under any circumstances represent work generated by a generative AI tool as being your own original work. You remain responsible for reviewing, verifying, and approving any AI-assisted work product before it is shared or relied upon.

- **Viral Risks. Always** assume that <u>any</u> information or data that you feed to a generative AI tool may be retained, used for model improvement, accessed by the vendor or other third parties, or otherwise disclosed with you or the Company potentially identified as the source. Such inadvertent disclosures may have legal consequences, including breaching the Company's contractual obligations, or applicable laws. Therefore, remain cautious when using any information that, when combined with other context, could reveal non-public Company Data or sensitive business activities.

- **Use of Company Data.** Do not use Company Data in generative AI prompts or transmit Company Data to a generative AI application unless a thorough risk-assessment has been made as to the use of such Company Data and the risk-assessment has been signed off by the Managing Director of your Company. Use of generative AI technology as part of or in connection with any offering that our customers will access and input their prompts (such as a front end AI application facilitating query of the product knowledge base), must have prior approval from the relevant Managing Director, and the AI technology must be managed and controlled by the Company and reside behind Company firewall protection.

- **Inaccuracy Risks**. **Do not** trust the accuracy of the AI output. It is common for generative AI to make mistakes, "hallucinate" or to create or produce content that is bias, stale, false, misleading or counter-factual. Check any work product produced with the use of generative AI with reliable, human, independent sources. You are responsible for the accuracy and completeness of your work.

- **Human Judgment.** Generative AI use is **not** appropriate for use in all circumstances. Use good judgment and common sense about when to use it. You may only use generative AI applications for appropriate work-related purposes and in any case, you may not use generative AI applications in any manner that may violate Company policies. You **mus**t verify that any response from a generative tool that you use in any way is accurate, appropriate, not biased, not a violation of any other individual or entity's intellectual property or privacy, and consistent with Company policies and applicable laws.

- **Ethical Use of AI.** The Company is committed to the responsible and ethical use of generative AI in all its forms. Company Staff must ensure that AI tools are used in a manner that is fair, transparent, and respectful of human dignity. This includes being mindful of potential biases in AI-generated outputs, avoiding uses that could lead to discrimination or harm, and ensuring that human judgment and oversight remain central to any decision-making process that affects individuals or stakeholders. The Company does not condone the use of generative AI to deceive, manipulate, or misrepresent, whether internally or externally.

- **No Use in Employment Decisions.** Where AI is used in processes that impact people, such as for example hiring, performance evaluation, or customer interactions, Company Staff must ensure appropriate human review and accountability are maintained at all times. You may **not** use generative AI tools to make or help you make employment decisions about applicants or employees, including recruitment, hiring, retention, promotions, transfers, performance monitoring, discipline, demotion, or terminations. This does not prevent use for purely administrative tasks that do not evaluate or rank individuals.

- **Ask Questions.** If you are ever in doubt whether or how you may use generative AI in a particular circumstance, check with your supervisor, Managing Director, General Manager or General Counsel (or similar) before using it.

## Alignment with Company Core Principles and Policies

**Key Principles for Use of Generative AI**

This policy integrates with and supplements other related Company policies and core principles, including those related to **confidentiality and privacy, information security, responsible work conduct, employment laws,** and **workplace ethics**. We explain some of the important legal and ethical considerations and concerns underlying this policy below.

1. <u>Safeguarding Company Data; Company Data Security</u>
   Respecting and protecting privacy and confidentiality is of utmost importance to the Company and its stakeholders. You should assume that your use of generative AI platforms is not secure or confidential

unless the tool is Company-reviewed and approved and configured for secure enterprise use. You may not input any Company Data into a generative AI platform unless a thorough risk-assessment has been made as to the use of such information and the risk-assessment has been signed off by the Managing Director of your Company. Such action could violate applicable codes of conduct, privacy laws, non-disclosure agreements and other contractual arrangements. When using generative AI tools or applications on a Company-issued device or a bring your own device with access to Company Data, work with Company IT to ensure that you have updated any settings to enhance security of and help prevent unauthorized access to Company Data.

2. Intellectual Property Considerations
   Be especially mindful of intellectual property rights when using generative AI and consider potential conflicts that may arise from the use of AI-generated content, now or in the future. Content outputs from generative AI may be subject to copyright protection or other third-party intellectual property rights (including open source licensing constraints for code). Be mindful of what information you input into generative AI tools and how you incorporate outputs from generative AI tools. Your use of generative AI tools must not cause the Company to infringe on the intellectual property rights of others, or relinquish or transfer our own IP rights to others.

3. Bias and Ethical Concerns
   Be skeptical of generative AI outputs. These outputs can be incorrect, out-of-date, biased, or misleading. Generative AI outputs can sometimes exhibit biases and create other ethical concerns because they are only as unbiased as the data on which they are trained. Be aware of these limitations and critically evaluate the content outputs from generative AI based tools. You are responsible for your use of generative AI tools within the Company, including verification and accuracy of any outputs from generative AI you may receive and use to support your role at that Company. If you have questions about how to verify generative AI outputs, sources of bias, or ethical concerns with your intended use of generative AI please consult with your Managing Director, General Manager or General Counsel (or similar) for guidance.

4. Exercising Caution in Business-Critical Decision Making
   Generative AI can provide valuable insights and support, but it is essential that our people, never our tools, make business-critical decisions. Always corroborate AI-generated recommendations with independent research, expert opinions, and sound judgment to ensure that our decisions are well-informed and reflect the best interests of the Company and its stakeholders. Human beings must oversee the decision-making process and ultimately make all decisions.

5. Mandatory Internal Disclosure of Generative AI Usage in Produced Materials
   Be transparent with your use of generative AI tools and outputs. The reason we require all Company Staff to disclose the use of generative AI in any materials produced within the Company is to enable team members and management to understand the origins of the content and make informed decisions about its appropriateness and reliability. Additionally, it encourages open dialogue about generative AI's role in our work and promotes a culture of collaboration and continuous learning.

6. Support Resources and Feedback
   To ensure effective use of generative AI based tools, the Company encourages making use of relevant training and support resources from outside sources such as workshops, webinars, tutorials, and user guides to enhance your understanding of AI technologies and their appropriate use in your work. Also, stay informed about new developments in AI technologies, regulations, and industry best practices.

   Provide feedback to help us improve this policy. The Company is dedicated to fostering a culture of responsible use of generative AI. Share your experiences, challenges, and successes with your colleagues, and collaborate to develop best practices for utilizing generative AI based tools in your work.

7. Vendor Management
   When selecting generative AI vendors or entering into partnerships with external organizations, those external organizations must align with the Company's ethical guidelines, demonstrate transparency, and share the Company's commitment to responsible generative AI use and any vendor use of generative AI must also be in accordance with this policy. If you work with a generative AI vendor or external partner ensure that the vendor or partner understands the Company's commitments regarding generative AI and is honoring them. If you have questions or concerns about a vendor or partner, please report them.

8. Generative AI Impact Assessment and Documentation
   We encourage Company Staff to conduct a generative AI impact assessment before any use of generative AI tools. Your generative AI impact assessment should evaluate the potential ethical, legal, and security implications of using generative AI in the specific context of your project and ensure you have steps in place to abide by this policy in your use of generative AI. Documenting these assessments helps promote transparency, accountability, and a culture of continuous improvement within our organization.

9. Reporting Misuse and Concerns
   If you witness or suspect any misuse of generative AI, or encounter any ethical, legal, compliance or security concerns (including any suspected disclosure of Company Data to a generative AI tool), please report the issue to your supervisor or Managing Director and to the legal department at legal@tss-vms.com as soon as possible.

Appendix A contains the TSS Generative AI Risk-Assessment (self assessment). The completed risk-assessment must be signed off by the Managing Director of your Company. Any use of generative AI tools is always subject to your use in compliance with (i) the Company's policy on generative AI use and (ii) the usage guidelines of the applicable tool.

**Form of Appendix A: TSS Generative AI Risk-Assessment attached separately.**

Appendix A

# Code of Conduct

# Annex 8 – Responsible Work Environment

## Further explanation

**Diversity & Inclusion**

Diversity embraces individual differences and unique characteristics such as personality, beliefs, values, gender, nationality, race, ethnic origin, age, religion, disability, sexual orientation, marital status and political preference. Inclusion recognizes and values people's differences to enrich work environments and enable optimal performance. It involves investment in understanding and eliminating bias, creating a working culture that accepts and respects everyone. In an inclusive environment, everyone is encouraged to thrive and be the best they can be.

Diversity and inclusion are vital to realize positive results for our business. By implementing our diversity and inclusion culture, Total Specific Solutions aims to create a diverse and inclusive workforce recognising human rights and equal opportunities for our people.

TSS wishes to be a company mirroring the diversity of the society in which it operates in all its business units and aspires to create an organisation where people from diverse backgrounds feel welcome and safe, can be themselves and receive space and recognition to use their talents in development and customers' success.

TSS' Diversity and Inclusion approach is supporting our growth ambition. Our approach is based on visible and invisible differences impacting all within our group, internationally and locally and in all areas such as Leadership, Human Resources, Research & Development, Sales & Marketing and more.

**Health and safety**

TSS strives for an accident free, secure and healthy working environment for all its Representatives and expects you to do your utmost best to ensure the same. You may never put yourself or anyone else at risk of your health or safety, even if you think that such would make the work more efficient. Further, we will not tolerate any level of violence or the threat of violence in the workplace.

**No harassment and discrimination**

TSS does not tolerate harassment of any kind, including on the grounds of race, colour, religion, gender, sexual orientation, national origin, age, disability or any other type of behaviour that is hostile, disrespectful, abusive and/or humiliating. Harassment or discrimination can take many forms, such as verbal, visual or physical. Such conduct will not be tolerated. Employment with TSS is based solely upon individual merit and qualifications directly related to your job. If you or a colleague are being harassed or discriminated, you should immediately report the incident to your manager, TSS' confidential counselor (*vertrouwenspersoon*) at codeofconduct@tss-vms.com or please refer to annex – speak up! for all other ways of (anonymous) contact.

**No workplace bullying**

Workplace bullying is behavior from a person or group that is unwanted and makes someone feel uncomfortable. Workplace bullying can take place in many forms, such as verbal, visual, digital or physical. TSS does not tolerate any form of workplace bullying. If you or a colleague are being bullied, you should immediately report the incident to your manager, TSS' confidential counselor (*vertrouwenspersoon*) at codeofconduct@tss-vms.com or please refer to annex – speak up! for all other ways of (anonymous) contact.

**Equal opportunity**

To be a leader in our business, we must be flexible, innovative, and creative and have an ability to accommodate other people's points of view. TSS strives to provide equal opportunities for its Representatives, including the recruitment, promotion, compensation, training and development. We expect our managers to exercise leadership in this field by role modelling appropriate behaviour.

**No drugs or alcohol**

TSS will not tolerate any use of drugs and inappropriate use of alcohol during working hours or even outside working hours when such use has an influence on your performance during working hours.

## Examples

**Example 1:**

A Representative does not want to promote a female to Managing Director as the job requires leading a difficult management team and from the Representative's point of view, the successor lacks a dominant leadership style. However, this is not a justified reason to prevent this promotion since the assessment shows that leadership skills are developed and one should be selected based on those leadership capabilities, and not personally preferred leadership style(s).

**Example 2:**

An employee wants to take parental leave during the finishing stage of a customer project. Ideally, it would be the period for when the team puts in additional effort to deliver the project on time. Although it might have an impact on project planning, parental leave should be made possible. Within the local legal framework and when requested on time, parents should be able to spend parental leave with their family when desired.

**Example 3:**

A Representative displays a screen saver with a cartoon that contains a harsh statement about a religion. Such display will be seen as discriminatory and will not be tolerated. Be aware to act respectfully against any religion practised by your colleagues.

**Example 4:**

A Representative notices that the breath of a colleague regularly smells of alcohol. The Representative tries to discuss this with such colleague, but is unfortunately not successful. The Representative should go to its manager or TSS' confidential counselor (*vertrouwenspersoon*) at codeofconduct@tss-vms.com or please refer to annex – speak up! for all other ways of (anonymous) contact, since drinking could severely influence the functioning of this colleague and could, as a consequence, damage such person and other Representatives.

## Q&A

**Question 1:** You are hiring a new employee for the team. Are you allowed to make the selection based on culture fit by, for example, considering sexual orientation?

**Answer 1:** No, the hire selection criteria for cultural fit are related to Innovative, Dedicated and Entrepreneurial behaviours or capabilities per job profile.

**Question 2:** When organizing an annual business unit event for employees, should you consider the relevant religious days of these employees?

**Answer 2:** Yes, to make people feel welcome and included it is pleasant to take all religions within the company into consideration and not skip important religious holidays as Christmas, Diwali or Eid ul-Fitr.

**Question 3:** I suspect that our company does not comply with fire safety regulations, which could potentially be very dangerous. My manager does not want to make sure all fire safety regulations are complied with, because this might put our targets at risk. What should I do?

**Answer 3:** If your manager does not take the appropriate actions, report this immediately to TSS' confidential counselor (*vertrouwenspersoon*) at codeofconduct@tss-vms.com or please refer to annex – speak up! for all other ways of (anonymous) contact. Prevention of dangerous conditions will always prevail over meeting targets.

**Question 4:** My colleague regularly makes sexually oriented comments on my appearance. I feel highly uncomfortable working with this colleague. What should I do?

**Answer 4:** First, discuss this situation with your manager or TSS' confidential counselor (*vertrouwenspersoon*) at codeofconduct@tss-vms.com. If your manager refuses to help you, report this situation to TSS' confidential counselor (*vertrouwenspersoon*) at codeofconduct@tss-vms.com or please refer to annex – speak up! for all other ways of (anonymous) contact.

**Question 5:** After work, I attended a gathering with the rest of my team. One of my managers made several unwelcome advances towards me. What should I do?

**Answer 5:** Unwelcome advances are never acceptable. If you are comfortable doing so, professionally and respectfully address the situation with the manager, and know that going forward, you can always do so in the moment. You should also speak up and consult with the appropriate resources such as TSS' confidential counselor (*vertrouwenspersoon*) so that additional steps may be taken consistent with established procedures.

**Question 6:** Whenever I ask my manager a question, my manager publicly mocks me and questions my qualifications. What do I do?

**Answer 6:** This behaviour may be considered bullying, and at a minimum is disrespectful and inconsistent with our code. Speak up via one of our Speak Up Channels.

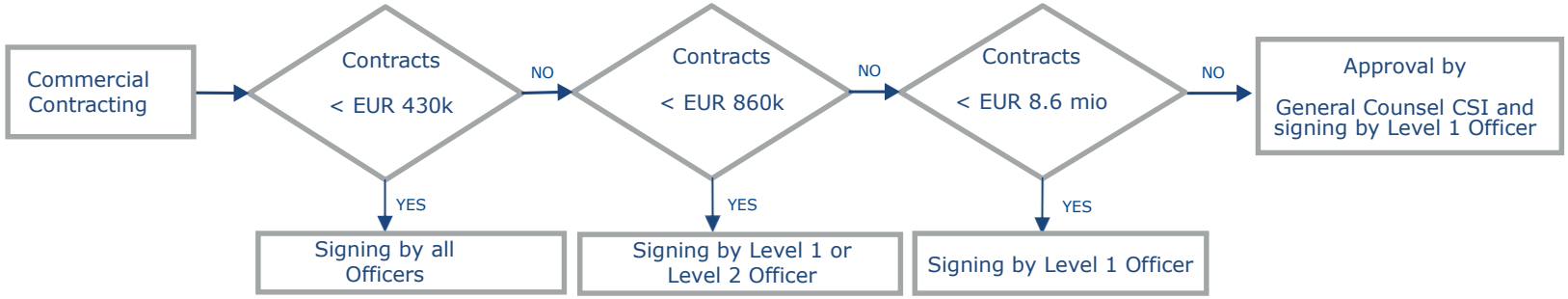
**Question 7:** I was in the lunch room with my colleagues, just having a casual conversation, and one of them made a comment about another colleague that I found offensive. How do I handle this situation?

**Answer 7:** If you are comfortable doing so, professionally address the situation with your colleague. If you do not feel comfortable addressing the situation yourself, need guidance or you are concerned that additional steps should be taken, then you should speak up via one of our Speak Up Channels.

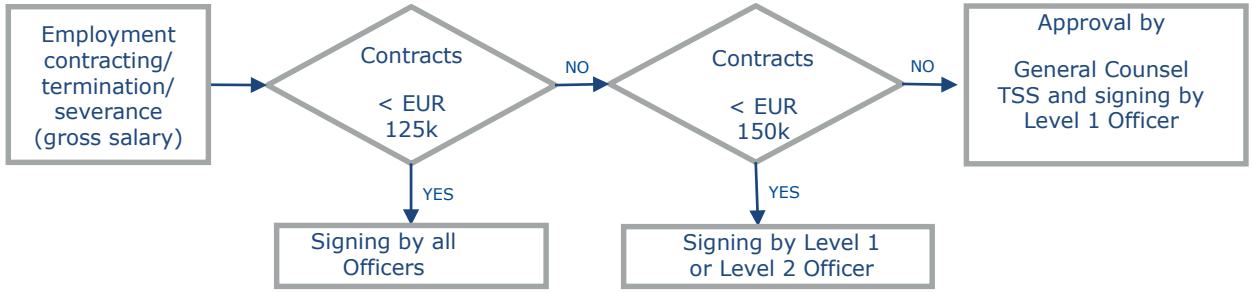
# Code of Conduct

## Annex 9 – Authorization Scheme TSS*

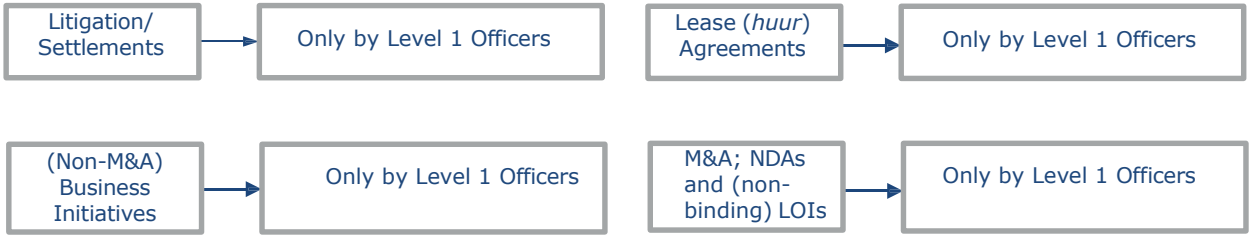
## Commercial Contracting – Sale and Purchase Contracts (in- en verkoop)




## Employment/ HR Contracting– Gross Salary (excl. bonus)




## Other




**TSS Officers**

Level 1: TSS Group CEOs

Level 2: General Managers

Level 3: Managing Directors

*** master version of the TSS Authorisation Scheme. Other versions may be applied within different subdivisions of TSS.**

# Code of Conduct

# Annex 10 – Speak Up!

## Further explanation

**What is the purpose of this annex?**
The purpose of this Annex is to explain how you can raise concerns about suspected misconduct in confidence and without fear of retaliation. As we are part of Topicus.com Inc, the Topicus Whistleblower Policy is also applicable to you. This Topicus Whistleblower Policy is also attached to this Annex. The Topicus Whistleblower Policy is an addition to our Code of Conduct.

**Your responsibilities**
We expect you to always act in accordance with the law and our Code of Conduct. Wherever laws, regulations or self-regulatory agreements are more restrictive, they prevail. We expect everyone to promote a culture of openness, in which we all feel comfortable raising questions, dilemmas and concerns regarding the interpretation of, or adherence to, this Code of Conduct.

Those in management positions have greater responsibilities: you have an essential role to play in sustaining our reputation and license to operate. You are expected to lead by example and create a transparent and open environment, in which concerns or suspicions can be raised without fear of retaliation. Managers are expected to take all concerns seriously, ensure they are properly escalated through the appropriate channels, actively prevent and respond to retaliation, and support compliance with company policies, controls and training requirements. Managers must not attempt to handle or investigate serious issues independently unless authorized

**What to do when in doubt?**
The Code of Conduct does not cover every situation that may occur, nor do they remove the need for using common sense and professional judgement. If you are in doubt about what to do, ask yourself the following question:

- Does it feel like it is the right thing to do?
- Is it legal and does it seem consistent with our values and our Code of Conduct?
- Does it reflect well on our company?
- Would I still accept full responsibility for this decision if I read about this in the media?

If the answer is “no” to any of these questions or if you are uncertain, stop and seek guidance. Discuss the matter.

**SPEAK UP**
Do you have a concern about a possible violation of our Code of Conduct or a (suspicion of) misconduct? Speak up! Remaining silent can only worsen the situation and undermine trust. When you honestly and truthfully raise a concern, you help to protect our company, your workplace, and ultimately your colleagues and yourself. So speak up. Raise any concern you have through one of the Speak Up Channels. All reporting is done confidentially and you can share your concerns anonymously or not. Whatever feels comfortable to you

**How to Speak up?**
Our Code of Conduct allows you to raise concerns about suspected misconduct through a variety of channels, either verbal or in writing. This policy does not replace any regular reporting lines or complaints procedures within your business unit. If you suspect misconduct, you are encouraged to address this directly with the person involved. If this would not be appropriate, please feel free to raise questions and concerns through any of our Speak UP Channels as set out on the next page or any other local external institutions that have been legally formalised in your country.

**Confidential Counsellor**
TSS has appointed two Confidential Counsellors (*vertrouwenspersoon*) (one female and one male) as a further point of contact for you to raise concerns about suspected misconduct. These Confidential Counsellors are available if you prefer not to raise a concern with your manager. They are there for you to discuss your concerns in confidence and advise on any next steps.

In addition to the above, there is no obligation to first report any possible misconduct internally. If you have a concern about possible misconduct, you can also directly report your concerns to any locally authorized external institutions depending on the nature of the misconduct.

**Topicus Ethicspoint**
If you suspect misconduct and genuinely believe that the matter cannot be dealt with through the available channels within your business unit or TSS, you can use our external Topicus Ethicspoint option to raise concerns confidentially. The Topicus Ethicspoint is run by an independent third party and is available 24/7, 365 days a year.

**Non-retaliation**
No one will suffer if we decline business to adhere to our Code of Conduct. Also, please feel confident that no one will be penalised for raising concerns in good faith about suspected misconduct via one of the Speak Up Channels. Any form of retaliation against you for speaking up will not be tolerated. Retaliation against reporters is treated as a violation of this Code of Conduct and consequently may lead to disciplinary measures.

**Disciplinary Measures**
A violation of the law and/or our Code of Conduct can have serious consequences for our company and the individuals involved, including you. The same goes for turning a blind eye to any such violation. As an individual you can be held liable and fined or sent to prison. In addition, our company can be held liable and fined, and its reputation can be severely damaged. A violation of the law and/or our Code of Conduct can also lead to disciplinary measures, which may include dismissal. Using a third party or other means to bypass this Code of Conduct is never allowed.

**What kind of information do you need to provide?**
When you file a report (in person, in writing, online or by phone), please provide as much detailed information as you can to enable our company to assess and investigate your concern, such as:

- The background, history and reason for the concern
- Names, dates, places and other relevant information
- Any documents that may support your report

**What should you do if you do not have all the facts?**
We encourage you to speak up as soon as possible, ideally before situations get out of hand or damage is done. It is always better to discuss upfront than to report afterwards. If you know about or suspect misconduct, speak up with the facts that you have. We do not expect you to have all the answers and you are certainly not expected to prove that your concern is well founded. Let our company look into the matter to determine if there is a reason for concern. Never investigate the matter yourself and do not seek evidence to build a strong case. We guarantee that no disciplinary measures or other steps will be taken against you if your genuine concern later turns out to be mistaken or misguided.

**Confidentiality**
All reporting is done confidentially. This means that information about your concern will only be shared with a limited number of people on a strict need-to-know basis. Information will only be disclosed outside this small group if we are required to do so by law or an important public interest is at stake. In principle, we are obliged to inform the implicated person that a complaint has been filed against such person, but your identity will not be disclosed. You yourself can help us protect confidentiality by being discreet and not discussing your report with your colleagues or anyone else.

You can share your concerns anonymously. We do however encourage you to reveal your identity as it is more difficult, and in some circumstances even impossible, for us to investigate reports that are made anonymously.

# SPEAK UP CHANNELS

**1** CONCERNED ABOUT (POSSIBLE) MISCONDUCT?

**2** WHO CAN I TALK TO?

IF POSSIBLE, TALK TO THE PERSON INVOLVED

or

TALK TO YOUR DIRECT MANAGER

or

TALK TO TSS' GENERAL COUNSEL (male) - legal@tss-vms.com

or

TALK TO TSS' CFO (female and male) - cfo@tss-vms.com

or

TALK TO TSS' CONFIDENTIAL COUNSELLORS (*vertrouwenspersonen*) -
codeofconduct@tss-vms.com (female and male)
codeofconductF@tss-vms.com (female)
codeofconductM@tss-vms.com (male)

or

TALK TO ONE OF THE LOCALLY AUTHORIZED EXTERNAL INSTITUTIONS

**3** YOU CAN ALSO USE ONE OF THE FOLLOWING TOPICUS ETHICSPOINT OPTIONS

1) Telephone
   - Australia 1800 571 077
   - Brazil 0800 000 0096
   - Croatia 0800 790 009
   - Denmark 80 83 0246
   - France 0800 99 06 83
   - Germany 0800 18 177 96
   - Italy 800 715 059
   - Netherlands 0800 0221236
   - Poland 800 005 082
   - Spain 900 999 457
   - Switzerland 0800 225 145
   - United Kingdom 0800 084 3471
   - Other jurisdictions will follow and communicated separately
2) Email - whistleblower@topicus.com; or
3) Online – http://topicus.ethicspoint.com

WE UNDERSTAND IT IS NOT ALWAYS EASY TO RAISE CONCERNS ABOUT POSSIBLE MISCONDUCT BUT WE DO ENCOURAGE YOU TO COME FORWARD WITH ANY CONCERNS AND SPEAK UP!

ANY CONCERN WILL BE DEALT WITH APPROPRIATELY AND CONFIDENTIAL.

# Code of Conduct

# Annex 11 – Whistleblower Policy

*This Whistleblower Policy ("Policy") applies to the operations of Topicus.com Inc. and each of its subsidiaries ("Topicus.com"). This Policy is designed to operate in conjunction with our Code of Conduct. This Policy has been established and approved by the Board of Directors of Topicus.com. Topicus.com actively monitors (management's) compliance with this Policy. To the extent there is any inconsistency between the Code of Conduct and this Policy, this Policy takes precedence.*

**1 Who does this Policy apply to?**
This Policy is designed to explain how possible misconduct can be reported, and how Topicus.com will protect people who raise such a concern. It applies to all current and former employees who are part of the Topicus.com group of companies, our contractors, and their respective family members and our freelancers, temporary workers, trainees and volunteers if they receive compensation for their work.

Topicus.com encourages employees, everyone who works with Topicus.com, and those affected by our businesses to raise concerns about any actions, decisions or situations that may be illegal or might be considered improper, such as a misconduct concern or a concern about an improper state of affairs or circumstances, any safety issues, or any suspected breach of our Code of Conduct.

Topicus.com's goal is to foster an open, transparent and safe working environment. We encourage people to speak up if they see possible misconduct or other improper situations. Doing so helps Topicus.com to identify and address issues promptly and improve how we do business.

**2 What concerns are covered by this Policy?**
A concern could be raised under this Policy if any person has reasonable grounds to suspect misconduct or an improper state of affairs or circumstances in relation to a Topicus.com company.

**3 What concerns are not covered by this Policy?**
This Policy is not designed to cover a personal work-related grievance. Examples of personal grievances include personal conflict between employees, decisions relating to transfer and promotion, issues about terms and conditions of employment, and decisions to suspend, discipline or terminate the employment of the reporting person.

**4 How should a concern be raised?**
There are a number of ways to report a misconduct concern: in person, by phone, by email or online.

- You can speak to your direct manager; or
- You can also raise your concern with your General Counsel; or
- You can also raise your concern with your Group CFO; or
- You can also raise your concern with the TSS' Confidential Counsellors; or
- You can also raise your concern with one of the locally authorised external organisations; or
- You can contact Ethicspoint, a confidential ethics hotline, to raise any concern or ask a question.

By phone at:

- Australia 1800 571 077
- Brazil 0800 000 0096
- Croatia 0800 790 009
- Denmark 80 83 02 46
- France 0 800 99 06 83
- Germany 0800 1817796
- Italy 800 715 059
- Netherlands 0800 0221236
- Poland 800 005 082
- Spain 900 999 457
- Switzerland 0800 225 145
- UK & Northern Ireland 0800 084 3471

*Phone numbers for other jurisdictions will follow and communicated separately*

By email at: whistleblower@topicus.com
Online: http://topicus.ethicspoint.com

AlertLine is operated by an outside vendor and is a resource for any Topicus.com employee to call or submit an online report. Employees can provide their names or remain anonymous, and all concerns will be followed up promptly with an appropriate response in accordance with this Policy.

When calling or submitting a concern or allegation to Ethicspoint, it is important to provide sufficient information to allow for the report to be appropriately investigated. It is helpful to include information such as: your involvement in the issue; if the matter is an ongoing or historical issue; the date of the most recent occurrence; any steps that have been taken to hide this issue; and if you have reported this issue to anyone within the organization.

**5 How am I protected if I report a concern?**
Topicus.com will not allow any form of (threatened or attempted) punishment, disciplinary or retaliatory action to be taken against anyone for reporting a concern in accordance with this Policy, or cooperating with a related investigation. Retaliatory action can take many different forms, including:

- threats;
- disciplinary action (e.g. termination of employment or reduction in pay or hours);
- any action that prevents or restricts someone from speaking out;
- damage to a person's property, reputation or business or financial position;
- demotion or denial of promotion; and
- intimidation, harassment, exclusion or humiliation.

It can also include more subtle behaviour, such as:

- withholding information that would assist an employee in their role;
- exclusion from social functions;
- not providing meaningful work; and
- the use of different voice or body language, or communicating differently compared with recent communications or communications with others.

Any person who feels that they are being retaliated against for reporting a concern or participating in an investigation, or believes that somebody else is a victim of retaliation (even if they are outside the organisation), should report it immediately to the persons or resources listed in Section 4.

You will not be disadvantaged for making reports on reasonable grounds even if the concern is ultimately unfounded. We consider all forms of retaliation to be misconduct. Retaliation is grounds for disciplinary action, up to and including termination of employment. You may also be entitled to additional legal protections in certain circumstances.

**6 Is a report of suspected misconduct under this Policy kept confidential?**
When you report a misconduct concern, the information you provide will be dealt with confidentially. This means that your identity will only be shared with your consent or where the concern is reported to an authority such as a law enforcement agency, as appropriate or as required by the law.
Where it is reasonably necessary for us to investigate a matter, we may need to disclose information which could lead to your identification for the purposes of investigating the matter. However, in all circumstances we will take all reasonable steps to reduce the risk that you will be identified in connection with an investigation.

**7 What process is followed when I report suspected misconduct under this Policy?**
Reports will be investigated where appropriate and Topicus.com will take the necessary steps to respond in a timely manner. Topicus.com will treat fairly all people involved in any investigation. In some cases, it may be possible to resolve your concern with direct advice, support and guidance. In other cases, it may be necessary to undertake an in- or external investigation. If an investigation is required, it will be performed by our Internal Auditor and/or external specialist. Matters that involve alleged or suspected fraud, violations of law or policy that are potentially significant will also be reported to Topicus.com its legal department, outside independent counsel, accountants and/or other specialists who may be retained as required.

Nothing in this Policy, the Code of Conduct or any other document or procedure at Topicus.com prevents you from, or requires approval for, reporting what you reasonably believe is a breach of the law to an appropriate government authority or from seeking legal advice in relation to your rights about disclosing information.

Topicus.com encourages all people who report a misconduct concern, where they are comfortable doing so, to provide their name and consent to this information being shared with the investigating Internal Auditor to help facilitate an effective investigation into the reported conduct. Investigations into anonymous complaints can be limited if further information is needed from the notifier.

**8 What are the possible outcomes for allegations of misconduct or breaches of the Code of Conduct?**
If allegations of misconduct are substantiated, this may result in disciplinary action up to and including termination of employment. If there has been illegal activity, civil penalties or criminal charges may also apply.

**9 What if I have questions about this Policy?**
If you have any questions about this Policy please contact your direct manager, Human Resources, the General Counsel, Internal Audit or Ethicspoint.

**10 Who is responsible for implementation and updates to this Policy?**
Internal Audit will monitor the implementation and review the suitability and effectiveness of the Policy on an ongoing basis.

Last approved by the Topicus.com Inc. board on January 27, 2021.