CIC Hospitality Policies 2023

Table of Contents

Code of Conduct Policy

Applicability of Code of Conduct and ethical guidelines

This Code of Conduct and Ethical Guidelines applies to all employees (including hired personnel) and directors of the Company. It also applies to the Company's subsidiaries and majority owned joint ventures, as well as to sales representatives, agents and others who act on the Company's behalf.

The Company is committed to act with integrity and in compliance with all applicable laws, policies, regulations, and not to cause harm to its stakeholders or the image of the industry it operates within.

Integrity is a fundamental building block of trust in business relationships. The Company seeks competitive and commercial success through the application of superior individual and collective skills and not through the use of manipulative, deceptive or illegal practices.

What does this mean for you?

- You must at all times comply with all applicable laws and regulations, as well as applicable internal policies/procedures adopted by the Company.
- Conduct business in a responsible manner and display loyalty to the Company in your day-to-day work and actively seek to conduct all business activities with integrity and honesty.
- Conducting the business activity of the Company in an ethical manner implies keeping legitimate promises regardless of whether or not there is a legal obligation to do so. Hence, you shall only make promises you are capable of fulfilling, and you shall act in a reasonable and just manner based on facts and circumstances.

Depending on the circumstances, the Company may be subject to antitrust laws and regulations of Norway, the EU/EEA, the US, or elsewhere. Act in fairness

The Company supports fair and open competition and is committed to act in compliance with applicable antitrust laws and regulations. Any violation within our organization may expose both the Company and individuals to fines, criminal liability and other severe legal consequences, and would also represent a risk to our reputation.

The Company's expectations and standards for antitrust compliance are set out in the Company's *Antitrust Policy*.

What does this mean for you?

- You must never engage in, or contribute to, activities that violate antitrust laws and regulations, such as price-fixing, market-sharing or bid-rigging, and shall work against the Company becoming involved in such practices.
- You must familiarize yourself with, and act in accordance with, the Company's Antitrust Policy. Never engage in corruption, trading in influence or money-laundering and terrorist financing

Corruption, trading in influence, money laundering and terrorist financing

Corruption means offering, promising or giving any person (directly or indirectly), or requesting, receiving, accepting or soliciting for oneself or others, an undue advantage (including money, gifts, loans, favor, reward, facilitation payments or other benefits) in connection with the person's performance of a position, office or assignment.

Trading in influence means giving or offering any person, or requesting, accepting or receiving for oneself or others, an undue advantage in return for influencing the conduct of another person's position, office or performance of an assignment.

Money laundering means i) safeguarding or disguising, or being part of an arrangement to assist another party in safeguarding or disguising the proceeds of crime in order to hide its illegal origins, or ii) receiving or obtaining proceeds of crime.
Terrorist Financing means any dealings with funds or other assets for the purpose of financing terrorism.

The Company shall work against corruption, trading in influence, money-laundering and terrorist financing, fraud and other economic crimes in all its forms. Such practices represent unacceptable business conduct, constitutes a threat to fair competition and undermines legitimate business activities. Any violation within our organization may subject both the Company and individuals to criminal liability and other severe legal consequences, and would represent a risk to our reputation.

The Company's standards and expectations with respect to anti-corruption, anti-money laundering and countering terrorist financing are set out in the Company's *Anti-Corruption Policy*. The policy covers i.a. matters such as gifts and hospitality, facilitation payments, events that might increase the risk of corruption, and examples of practical scenarios that could constitute a corrupt act.

What does this mean for you?

- You must never engage in, or contribute to, corruption, trading in influence or money laundering and shall work against the Company becoming involved in such practices.
- You must familiarize yourself with, and act in accordance with, the Company's Anti-Corruption policy.

Conflicts of interest

A conflict of interest occurs when an individual's personal relationships or interests could influence, or could be perceived to influence, the individual's decision making when acting for the Company.

Conflict of interest situations may occur and should be dealt with in an open and transparent manner. The Company aims to minimize decisions being made by employees or directors in conflict of interest situations, as this may result in the Company's interests not being properly safeguarded, and could also represent a risk to our reputation. Perceived conflict of interest should also be considered and managed/avoided, as such situations might harm the Company's reputation in line with situations of actual conflict of interest. Conflicts of interest

The Company's standards and expectations with respect to conflict of interests, as well as practical examples of relevant situations, are set out in the Company's *Anti-Corruption Policy.*

What does this mean for you?

- You shall take necessary actions to minimize the risk of conflicts of interest arising, for instance avoid being involved in decision making where you could be perceived to have a personal interest. Further, you shall act in accordance with the legitimate interest of the Company, and not make decisions based on what will benefit you or your family or close friends personally.

- You shall not use the Company's name, business contacts or otherwise exploit your position in the Company in connection with actions that are not specific to the Company's business activities.

- You should raise any questions regarding potential conflict of interest with your immediate superior.

- You must familiarize yourself with, and act in accordance with, the Company's Anti-Corruption policy.

Violating economic sanctions or trade controls

Never engage in transactions violating economic sanctions or trade controls. Economic sanctions impose restrictions on dealings involving certain countries and parties. They can be comprehensive and prohibit virtually all activities and transactions relating to a country/region. Or they can be selective and targeted, restricting activities in certain industry sectors or with named entities, individuals, groups or vessels.

Trade controls involve restrictions with respect to import or export/provision of certain controlled equipment/products, technology or services to/from a country.

The Company is committed to comply with applicable economic sanctions and trade controls laws and regulations. Violation of such laws and regulations may subject both the Company and individuals to criminal liability, and would represent a risk to our reputation.

What does this mean for you?

- You must identify whether a potential project or business partner is subject to economic sanctions and trade controls. You should raise any questions regarding such potential risks with your immediate superior.

- You must never engage in, or contribute to, violation of sanctions and export controls laws and regulations, and shall work against the Company becoming involved in such violations. Protect the company's real estate, assets, property and intellectual property

Protecting the Company

The Company's real estate, assets and property (including intellectual property) shall be safeguarded, and only be used for legitimate business purposes. Further, information of confidential nature relating to the Company, its employees or to its business partners shall be respected and protected.

Cybercrime poses an increased risk to our business. The Company is committed to working to minimize risks posed by malicious cyber actors to our Company and our business partners.

What does this mean for you?

- Protect and avoid harm being made to the Company's real estate, assets and property from theft and loss and comply with the Company's security standards, including familiarizing yourself with the Company's routines for mitigating risks related to cybercrime.

- You have a duty of confidentiality. You must ensure that all business information and other sensitive information, both of the Company and of our counterparties and business partners, are kept confidential.

Environmentally sustainable business activity[1]

The Company is committed and works to ensure that its business activity is environmentally responsible and energy efficient, and that the environmental impacts are reduced wherever possible. The Company is continuously focusing on environmentally friendly improvements.

What does this mean for you?

- Strive to support the Company's commitment to contribute to an environmental sustainable business activity.

- Inform your immediate superior if you become aware of business activities that could constitute a risk of accidents and environmental damage.

Social and working environment

The Company shall ensure proper labor and working conditions, safeguard the health and safety of its employees and promote the development of the communities in which it operates.

The Company strives to ensure that no harassment, discrimination or bullying occurs. We believe in equal opportunities, and the Company shall be a stimulating workplace with an inclusive working environment. The Company believes that it is only then that the employees will perform at their full potential and receive the proper recognition and reward for their performance.

The Company is committed to protect and respect the fundamental human rights of anyone affected by our operations. The Company expects its employees, directors, business partners and other parties directly linked to its operations, products or services to be equally committed to respect internationally recognised human rights.[2]

Purchase or in any other way make use of any sexual services is forbidden by Norwegian law and may contribute to human trafficking and other human rights violations.

What does this mean for you?

- You must familiarize yourself with, and act in accordance with, the Company's HSE/safety requirements.

- Treat everyone with courtesy and respect, regardless of race, gender, national or social origin, disability, sexual orientation, religious belief etc.

[1] Cf. also the Company's ESG policy
[2] Cf. also the Company's Procedure for ESG in relation to third parties and the Company's Anti-corruption policy

- You must never engage in, or contribute to, human rights violations, and shall work against the Company becoming involved in such practices.

- Do not purchase or in any other way make use of any sexual services in relation to business trips, either domestically not abroad.

Whistleblowing

The Company encourages reporting of suspected breach of laws and regulations, this Code of Conduct and Ethical Guidelines or any of its underlying policies, as well as other misconduct. Reporting allows the Company to rectify problems and prevent the problems from growing.

Details and guidelines with respect to reporting concerns are set out in the Company's *Whistleblowing Policy*.

What does this mean for you?

- If you have suspicions concerning breach of: legislation, this Code of Conduct and Ethical Guidelines and its underlying policies, or other misconduct, you should immediately report this to your supervisor or through the Company's whistleblowing channel.

Further information and consequences of breach

Any breach of this Code of Conduct and Ethical Guidelines may put the Company at severe risk and the Company may take retaliatory actions that could have adverse consequences for employee's employment or business partner's relationship with the Company. With respect to employees, breaches could for example result in written admonition, dismissal and/or reporting to government authorities.

Any questions you may have regarding this Code of Conduct and Ethical Guidelines may be taken with the CEO of the Company.

Environmental, Social and Governance policy

Introduction and purpose

CIC Hospitality is fully committed to promote sound environmental, social and governance (ESG) principles to all shareholders and the society we operate in. Our ESG policy reflects this commitment and its purpose is to maintain proper ESG management and decision-making processes.

The Company believes that high ESG standards make good business sense and that it has the potential to protect and enhance returns as well as promote the development of the communities in which it operates.

The Company is compliant with internationally recognized standards for responsible business operations including the UN Global Compact, UN's Universal Declaration of Human Rights and guidelines outlined in the Organization for Economic Co-Operation and Development (OECD) (if applicable: The UN Sustainable Ocean Principles. We also

All employees (hereunder directors, executives etc.) of the Company are required to familiarize themself and comply with the ESG policy as well as with the CIC Sustainability report 2022

CIC Sustainability Report 2022.pdf

Environmental

CIC Hospitality seeks to maximize sound stewardship on environmental themes, encourage environmental consciousness and facilitate the sustainability transition. We promote sustainable business propositions, along with products and services that actively reduce the potential impact on the environment. Specifically, we measure and monitor the carbon emission of our operations as defined by the Greenhouse Gas Protocol and specific targets for reduction of climate gas emissions are set annually.

The Company supports the goals set out by the 2015 Paris Agreement. We measure and monitor the carbon emissions in our company as defined by the GreenHouse Gas protocol. Specific targets for reduction of climate gas emission are set and measured on an annual basis.

Social

The Company shall respect internationally recognised human rights and provide proper working conditions for its employees. Assessments should be made to identify health and safety risks relating to or arising from working activities and appropriate measures shall be taken.

Equal opportunities should be granted regardless of gender, sexual orientation, age, race, color, ethnic origin, religion, trade union affiliation or disability. The Company does not directly or indirectly impose any restrictions in relation to the employees' freedom to establish or join trade unions or legal strikes. The Company must ensure that it does not directly or indirectly use forced labour, illegal child labour or take unjust advantage of migrant workers.

Governance

CIC Hospitality understands the importance of good corporate governance and business integrity within a business.

The Company shall ensure proper recording, reporting and review of financial and tax information but also that relevant ESG related policies are in place. The Company has implemented an anti-corruption policy, whistleblowing policy, anti-trust policy, code of conduct, sanctions policy and a social media policy to which all employees must adhere to.

We adhere to local and international agreements and legislation, and through a high level of transparency throughout our operations we seek to ensure high standards of business ethics.

CIC Hospitality and its employees must at all times exhibit honesty, integrity, fairness and respect in its business dealings. Further, information obtained through the Company's business must be used in the best interest of the Company and not for personal gain by any of its employees.

Implementation of the ESG policy

The Company shall conduct its activities and affairs in compliance with this ESG policy. Any deviations, concerns etc. shall be addressed and explained in a proper manner. If it becomes clear that the Company is in material breach of the adopted ESG policy, reasonably necessary actions must be made to rectify any such breach. The Company acknowledges that ESG issues are important; hence the ESG policy shall be reviewed by the board of directors of the Company at least on a yearly basis.

Cyber Security Policy & Plan

Overview

The purpose of the plan is to establish the goals and the steps for the cyber security incident response process and coordinate response in times of crisis (security vulnerability identified or exploited). This document will clearly define to whom it applies and under what circumstances, and it will include the definition of a cyber incident, staff roles and responsibilities as well as reporting, remediation, and feedback mechanisms. The plan shall be communicated and made easily available to all CIC Hospitality's personnel.

To minimize the risk of a cyber attack it is important to follow guidelines that evolve around this matter. Below is a list of actions that can be taken to minimize the risk of a security breach.

- Changing passwords on a regular basis
- Having a strong and long password.
- Having different passwords to access different platforms, tools etc.
- Keeping software up-to-date
- Check links before you click
- Use of anti-virus or anti-malware software
- Double check for HTTPS on websites
- Back up important files
- Make sure that you are communicating with the right person
- Double authentication

It is always recommended to keep yourself updated on any updates that increase your security knowledge and take actions if seeing breaches.

Background and roles

A cyber security incident is any event that threatens the confidentiality, integrity or availability of the information resources CIC Hospitality utilizes internally, especially sensitive information whose theft or loss may be harmful to CIC Hospitality, CIC Hospitality Funds and/or other stakeholders.

This plan mandates that any CIC Hospitality's employee who suspects or is faced with a cyber security incident on CIC Hospitality property (including but not limited to desktop, laptop, smartphone, tablets etc) must immediately inform and provide a description of what occurred via e-mail to Matthias Tanski, who will take further action regarding contacting relevant security company.

CIC Hospitality's ICT users should be informed that they must:

- Report immediately all suspected cyber security breaches as described above (e.g. information failures; loss of services; detection of malicious code; denial of service attacks; errors from incomplete or inaccurate business data)
- Note all important details (e.g. type of breach, messages on screen, details of unusual occurrences)
- Restrain from attempting to take remedial actions themselves

Cyber security incident response steps

Step 1- Identify cyber security incident

It is important to detect and assess accurately possible cyber security incidents by determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.

The Cyber Security Incident Response Team shall liaise timely with a security team to assess whether the suspected incident occurred and to which extent CIC Hospitality's information and communication technology environment including CIC Hospitality's data have been compromised.

In this context Cyber Security Incident Response Team can seek external expert analysis and support to ascertain the occurrence of cyber security breach. To this end, Cyber Security Incident Response Team shall:

- Ensure identification of a suspected cyber security incident (e.g. monitoring evidence of unusual occurrences and assessing one or more trigger points)
- Perform analysis of all available information related to the potential cyber security incident
- Determine what has actually happened (e.g. a DDOS[3], malware attack, system hack, session hijack or data corruption)
- Confirm that an actual cyber security attack or a cyber-related breach occurred.

The Cyber Security Incident Response Team shall notify the board of directors of the affected entity(ies) without undue delay of the incident and planned or proposed steps.

Step 2 - Define objectives and investigate situation

Once a cyber security incident has been identified, the next stage is to define what the objectives are for the response activities – and to investigate the situation in an appropriate manner. Cyber Security Incident Response Team shall engage forensic work to determine how the breach or exposure occurred, the types of data involved, the number of internal/external individuals and/or organizations impacted and analyze the breach or exposure to determine the root cause. To this end the investigation shall seek to provide answers to the below questions:

- What is the scope and extent of the attack (including targeted user(s) and damage assessment)?
- When did the attack occur?
- What did the threat agent take from us?
- Why did they do it?
- Who is the threat agent?

As early as possible the incident shall be classified in terms of severity (e.g. critical, significant, normal or negligible impact) and prioritization shall be made accordingly to address the incident and to the extent needed engage timely with external advisors, investigators, or cyber security experts.

Step 3 - Take appropriate action

i. Containing the cyber security incident

One of the first key actions to be taken after the initial investigation (and often as part of that investigation step described above) is to contain the damage being done by the cyber security

[3] Distributed denial-of-service

incident, for example by stopping it from spreading to other networks and devices both within CIC Hospitality's organization and beyond.

Containment typically comprises a number of concurrent actions aimed at reducing the immediate impact of the cyber security incident, primarily by removing the attacker's access to CIC Hospitality's systems. The objective of containment is not always to return (directly) to business as usual, but to make best efforts to return to functionality as normal, while continuing to analyze the incident and plan longer term remediation.

ii. *Eradicating the cause of the incident*

After an incident has been contained, eradication is often required to eliminate key components of the incident (e.g. removing the attack from the network, deleting malware and disabling breached user accounts), as well as identifying and mitigating vulnerabilities that were exploited.

Considering CIC Hospitality's ICT framework actions shall be decided by CIC Hospitality's Cyber Security Incident Response Team with the input and advice of external adviser and cyber security expert.

Step 4 - Recovery of systems, data and connectivity

The final step in responding to a cyber security incident is to restore systems to normal operation, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar incidents occurring.

Once systems have been recovered and controls have been tested, internal stakeholders should then be provided with a brief summary of what took place. The Cyber Security Incident Response Team should report that eradication was completed successfully and note any exceptions and other significant findings.

The conclusion of the investigation work on the incident shall be documented in a written report and where applicable propose remediation action(s) to avoid or mitigate the reoccurrence of similar incidents.

Communication

Once a cyber security incident has been successfully handled, formal reporting may be required to both internal and external stakeholders such as but not limited to Fund boards, Fund administrator and Investors.

Key questions to consider include:

- What are our reporting requirements?
- Who shall receive which information?
- What is the appropriate reporting format?
- What is the overall objective of reporting and an appropriate communication plan?

The actual reporting itself should include:

- A full description of the nature of the incident, it's history, and what actions were taken to recover

- A realistic estimate of the financial cost of the incident, as well as other impacts on the business, such as in terms of damage to reputation, loss of management control or impaired growth
- Actions regarding enhanced or additional controls required to prevent, detect, remediate or recover from cyber security incidents more effective

The Cyber Security Incident Response Team shall assess, organize and drive the communication work stream and provide adequate proposals for communication towards the relevant external stakeholders to be reviewed and approved by the board of directors of the entity(ies) affected by the incident before disclosure.

Notification to supervisory authorities

Data protection authority

As part of the investigation and provided that it has been ascertained that the cyber security incident led to a personal data breach as defined under GDPR (General Data Protection Regulation - EU Regulation 2016/679), the board of directors of the entity(ies) concerned from a GDPR perspective shall be notified, and a notification in accordance with GDPR shall be prepared.

GDPR defines a data breach as a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The Cyber Security Incident Response Team shall ensure that the data controller, as defined by GDPR, shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority in accordance with Article 55 of GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Financial Regulators

Cyber security incidents can have a significant operational, financial and/or reputational impact on financial institutions concerned and may even endanger the entire ecosystem or serve as an early warning for future incidents.

As such, a number of reporting obligations exist towards financial supervisory authority as regards reporting IT and cyber incidents and attacks in order to keep the supervisory authority informed of such incidents.

The Cyber Security Incident Response Team shall assess if the cyber security incident falls into the financial regulator reporting obligation and notify the board of directors if applicable of such reporting obligation, providing a draft notification for the board of directors for review.

Whistleblower Policy

Introduction

CIC Hospitality has implemented this whistleblowing policy in order to ensure that all employees can express their concerns in a responsible and effective manner internally if they discover censurable conditions at the Company. The Policy shall also ensure a proper handling of whistleblowing notifications in the Company.

The Policy sets forth routines for internal whistleblowing in accordance with Norwegian legislation.

All employees and hired-in personnel (jointly referred to as **employees**) have a legal right, and in some cases a duty, to report censurable conditions that occur in connection with the business of the Company. We encourage all employees to report censurable conditions that they become aware of in relation to their work.

Whistleblowing is an important method for uncovering illegal conditions and unwanted business culture within the Company. Whistleblowing allows the Company to rectify problems and prevent the problems from growing.

It is a management responsibility to ensure that whistleblowing notifications are handled in a responsible manner. It is also a management responsibility to ensure that employees who make reports (the **whistle-blower**) are protected against all forms of retaliation.

What to report?

1.1 Censurable conditions

All employees are encouraged to report their concerns if they discover any censurable conditions[4] at the Company. Examples of such conditions are:

- Breach of applicable legislation or the Company's policies
- Danger to life or health
- Danger to climate or environment
- Corruption or other financial crime
- Abuse of authority
- Unjustifiable working environment, including harassment, human and labor rights violations
- Breach of personal data protection regulations

Matters that only apply to the employee's own employment relationship will generally not be considered censurable according to law, unless the matter otherwise is compromised by the definition above. Examples of circumstances that generally are not considered censurable according to law, and thereby may not be dealt with in accordance with this Policy, are:

- Dissatisfaction with salary or other working conditions
- Disagreement with leaders or other colleagues about handling of work assignments, professional inquiries, etc.
- Disagreement with feedback or criticism from a manager if it is within the framework of routines and requirements of the Company and is presented in an objective, constructive and reasonable way.

[4] Conditions that violate laws and regulations or policies and procedures adopted by the Company or conditions that contravene ethical norms that are widely recognized in the society

1.2 Right and duty to report

Employees that become aware of circumstances that they believe are of censurable character as described above, have a legal right to report the matter, cf. the Norwegian Working Environment Act ("**WEA**") (*No.* arbeidsmiljøloven) Section 2 A-1.

Employees have a legal obligation to report if they become aware of harassment or discrimination in the workplace, or circumstances that may endanger life or health which the employee cannot correct him-/herself, cf. the WEA Section 2-3.

2. Procedures for reporting

Any expression and reporting shall be done in a responsible manner. A report in accordance with this Policy is always considered to be made in a responsible way.

Reports can be made orally or in writing. The receiver of the report shall write down the reporting if it is made orally.

As a main rule, reports should always be made internally in the Company, and primarily to your immediate superior. If this is not possible or appropriate (e.g. because it is a matter concerning your superior), you may report to the People of Culture manager.

Anonymous whistleblowing reports shall also be handled. However, it is helpful, and sometimes required, for the recipient to be able to contact the whistle-blower, in order to raise follow-up questions and obtain information necessary to assess the report.

The employee may always report externally to relevant public authorities.

Provided that the employee is in good faith regarding the content of the report, the report regards misconduct which has public interest and the employee has tried internal reporting first or has reason to believe that internal reporting will not be appropriate, the employee may report to the media or to the public in general.

Handling and following-up of whistleblowing reports shall be the responsibility of the People of Culture Manager. Reports can always be made directly to the WB Responsible. If the report concerns the WB Responsible the report shall be communicated to the CEO of CIC Hospitality, who will be responsible for the follow-up of the report.

3. Protection against retaliation and confidentiality

3.1 Non-retaliation

Whistle-blowers that report in a responsible way shall be protected against any adverse act or omission as a consequence of, or a reaction to, reporting the matter (retaliation). This includes becoming subject to:

- threats, harassment, unjust discrimination, social exclusion or other unfair treatment
- warning, unjustified change of work tasks, relocation or degradation; or
- suspension, termination (with notice or by summarily dismissal) or disciplinary punishment.

The Company shall ensure that the whistle-blower has a safe and proper working environment. If necessary, the Company shall implement measures to protect against retaliation against the whistle-blower.

3.2 Confidentiality

All reports made in the Company will be handled with confidentiality. This means that:

- The whistle-blower's identity shall be disclosed strictly on a need-to-know basis, only to those receiving and handling the report. Anyone receiving and handling the report shall keep the whistle-blower's identity confidential to the extent possible and permitted by law.
- The handling of the report is confidential and information about the content of the report is only disclosed to people on a strictly need-to-know basis. The fact that a report has been made, what the report concerns and that it is investigated can be communicated to the organization, the authorities, media or others, if deemed necessary.

4. Follow up of whistleblowing notifications

4.1 Routines upon receipt of reports

Any person who receives a whistleblowing notification in accordance with this Policy shall immediately communicate it to the WB Responsible.

All reports received by the WB Responsible will be taken seriously. The whistle-blower will receive a written confirmation from the WB Responsible that the report has been received.

The WB Responsible evaluates all received reports on a case-by-case basis. Reports regarding censurable conditions (ref. item 2.1) shall always be subject to appropriate investigation and be handled within reasonable time.

With respect to reports regarding other types of concerns/circumstances that evidently does not concern censurable conditions according to item 2.1, the WB Responsible may close the case without further actions or refer it to be handled by other relevant functions in the Company. The whistle-blower shall nevertheless be notified that the case has been closed/referred to another function, as well as an appropriate explanation of the reason. If the WB Responsible believes that the case should be followed up in another manner (personnel case, etc.) the whistle-blower shall, to an appropriate extent, receive guidance on how he/she can proceed.

4.2 The WB Responsible handling of whistleblowing reports

The WB Responsible shall assess and examine the report in a competent, objective and independent manner.

The WB Responsible can conduct his/her own investigation and conclude when it deems appropriate to do so based on the facts and proper assessment based on applicable law and internal policies and guidelines. The WB Responsible shall consult the CEO of the Company if in doubt about the handling of a report, or where there is need for more comprehensive investigations and reporting.

Upon consulting with the CEO, the WB Responsible may also engage internal resources or appoint external advisors to handle and investigate a report in the event of more serious or complex matters. If external advisors are engaged, a written mandate for handling further investigations of the report shall be prepared and the external advisor shall provide a written investigation report to the WB Responsible with assessment and recommended actions.

The WB Responsible shall give a preliminary response to the whistle-blower within two weeks from receipt of the report, regardless of whether the report is still under evaluation. To the extent possible, the response should also include an estimate of when the case may be expected to be concluded.

Any conversations or interviews with the whistle-blower shall be recorded in minutes. The whistle-blower's identity shall not be stated in any written material, unless approved by the whistle-blower. A copy of the minutes shall be provided to the whistle-blower upon request.

The person(s) being the subject of the report shall, as a principal rule, be made aware of the circumstances that are being investigated and the information that have been revealed. The person concerned shall have the opportunity to comment on the matter before the WB Responsible concludes on follow-up actions (the right of contradiction).

The WB Responsible shall always inform the CEO of the Company if a report contains information that makes it necessary with immediate measures like cessation of work or closure of premises, or if the report contains allegations of serious criminal offences. The CEO shall, in accordance with internal crisis management procedures, in a swift matter inform the Chair of the Board, of such received notifications.

4.3 Closing of a whistleblowing case

Based on an assessment and examination of the available facts, the WB Responsible shall reach a decision in the whistleblowing case and, if relevant, determine suitable follow-up actions of the reported concern. The WB Responsible shall document its assessments and conclusions in writing, including the factual and legal basis on which the assessment is based.

Once the case is concluded, the whistle-blower shall be informed about the outcome of the case. The same applies to the extent possible to the person(s) being the subject of the report. Other individuals who have been involved in the case may be informed about closure of the case if deemed appropriate.

When follow-up of the case is concluded, the WB Responsible shall provide a report to the CEO of the Company (or to any other person appointed by the CEO) on how the case was handled and whether it has brought any disciplinary actions with respect to personnel or revisions of the Company's compliance routines, internal controls etc.

5. The collection and processing of personal information

The employee must be aware that for the purpose of handling a whistleblowing report, personal information might be collected and processed. Whistle-blowing reports are likely to contain personal data. Examples of types of personal data that may be processed are:

- Name, position and contact details of the whistle-blower and the person(s) being the subject of the report, as well as any witnesses or other individuals affected.
- Details of the misconduct of the individual(s) concerned.

Any personal data collected via handling of whistleblowing reports will be processed for the purpose of administering and investigating allegations raised, and dealing with discovered misconduct, as described in this policy.

If you have any other questions, please don't hesitate to contact the People and Culture Manager.

Social Media Policy & Guidelines

These guidelines apply to CIC Hospitality employees who create or contribute to social networks, blogs, web newspaper conversations, online commentary or any other kind of social media, or that uses social media platforms as a means of communication.

CIC Hospitality's continued success is contingent on the trust from current and prospective business partners; groups which are heterogenous and have a diversity of opinion that we must respect. While all CIC Hospitality employees are welcome to participate in social media, we expect everyone to understand and to follow these simple but important guidelines, to secure our reputation and assets:

- **Confidential information:** Do not share confidential information relating to the Company or any third-party. Confidential information may for example include non-public information regarding business plans and strategies, trade secrets or privacy protected information.
- **Legal processes:** Do not comment on legal or regulatory matters pertaining to the Company.
- **Tone of voice:** Post meaningful, respectful comments. When disagreeing with others' opinions, keep it appropriate and polite.
- **Add value:** Statements must be true and not misleading; all claims must be substantiated, and opinions should be separated from facts.
- **Express *your* opinions:** Only authorized personnel may make statements on CIC Hospitality behalf on social media.
- **Openness:** Be transparent and state that you work at CIC Hospitality if commenting on issues pertaining directly or indirectly to the Company's activity and i.a. its competitors.
- **Respect your own privacy**: Do not send or post personal information.
- **Company photos:** It's not allowed to post photos from CIC Hospitality conferences, meetings, office retreats or any other company setting on social media, with the exceptions of marketing of CIC Hospitality seminars, approved by Øyvind Frisak.
- **Password:** Don't use the same passwords for your corporate accounts as for your accounts on social media.

For each post, repost, comment and "like" that you make, please consider whether and how the activity protects and builds CIC Hospitality reputation. This is particularly important for, but not limited to, activity on professional/work-related social media. When posting content on LinkedIn, or any other professional/work-related social media, assume people you are communicating with will associate you with CIC Hospitality.

Our overall goal is simple: To participate online in a respectful and relevant way that protects and builds our reputation. If you are in doubt whether a potential post will conflict with any of the above guidelines, do not post.

Social media platforms, including Messenger and WhatsApp, shall not be used for work related communications if not previously approved by CIC Hospitality. Documents with sensitive information shall always be sent on a secure connection to assure that the documents cannot be accessed by a third party.

Do you have any questions relating to these guidelines, please contact Øyvind Frisak.

Crisis Management Policy

1. Introduction and purpose

In CIC Hospitality we are committed to conduct business in compliance with applicable laws and regulations, and with the highest ethical standards and integrity as reflected in the Company's Code of Conduct.

Early identification and appropriate handling of potential breaches of internal policies and procedures and/or applicable laws and regulations ("**Compliance Matters**") is paramount for mitigating CIC Hospitality legal and reputational risk. Adequate handling of Compliance Matters may also mitigate the negative effects of a crisis for our employees, contracting parties and shareholders.

The objective of this Crisis Management Policy (this "**Policy**") is to minimize the negative impact of unwanted events such as unethical business behavior, work-related injuries, environmental pollution, or cyber-attacks.

Compliance Matters will vary, both in nature and severity. They may also come to the Company's attention in various forms, e.g. by way of a whistleblowing report, adverse media pertaining to a third-party contractor etc.
It may be difficult to conclude on the seriousness of a matter at an early stage. An issue that appears less problematic may turn out to be critical for the Company – and vice versa. Therefore, all suspicions of breach of policies and procedures and laws and regulations shall be appropriately dealt with according to this Policy. Taking into consideration the wide spectrum of potential Compliance Matters (see item 2 below), each incident must be managed on a case-by-case basis and based on a concrete crisis management plan. The measures to be carried out according to this Policy shall be proportional to the identified risk and the potential severity of the case. Assessments and remedial actions shall always be appropriately documented.

Identifying the risks pertaining to our business activities and knowledge of key applicable regulations are prerequisite factors for effective crisis management. Updated risk assessments with associated threat scenarios combined with crisis training and testing (see item 14 below) are therefore critical.

2. In which cases does this Policy apply?

All Compliance Matters shall be handled in accordance with this Policy. This Policy does not apply to compliance cases that with certainty do not represent any legal or reputational risk to the CIC Hospitality

Examples of Compliance Matters that always shall be handled under this Policy are suspicions relating to:

- Breach of the Company's policies and procedures
- Violations of legislation relating to corruption and bribery, money laundering and terrorist financing, sanctions/export control and other economic related crimes
- Anti-competitive behavior (anti-trust)
- Internal fraud such as embezzlement, misrepresentation of assets, and IP theft
- Violations of applicable laws and regulations in the Company's supply chain, such as labor rights and human rights violations
- Serious workplace injuries
- Offenses relating to harassment of employees

- Pollution and environmental damage caused by the Company or any third-party while acting on behalf of the Company
- Violations of non-compete clauses by employees/former employees
- Cyber-attacks
- Other adverse matters that expose the Company to legal risk and/or reputational damage

A Compliance Matter may come to CIC Hospitality attention through a whistleblowing report. Such matters shall be handled in accordance with CIC Hospitality's whistleblowing policies. This Policy shall act as a supplement to the whistleblowing policies. In the event of conflict, the whistleblowing policies take precedence.

3. Roles and responsibilities

CIC Hospitality is responsible for implementing this Policy in the organization, and to ensure that all employees are familiar with its content and have the necessary preparedness to act in accordance with it.

4. Remediation plan

Based on the initial information available relating to a Compliance Matter, the CEO shall ensure that a remediation plan is prepared as soon as possible. The plan shall specify what specific measures that need to be taken, at what time, their priorities and internal responsibilities for execution. Topics listed in items 5-13 below that are relevant to the Compliance Matter shall be addressed in the remediation plan.

The remediation plan shall frequently be updated based on the developments of the Compliance Matter.

CIC Hospitality shall, in accordance with item 3 above, assess whether the remediation plan (or part of the plan) shall be approved by the Chair/Board before being executed. Any interaction with public authorities in relation to a Compliance Matter shall be pre-approved by the Board, cf. item 10 below.

5. Ceasing illegal or otherwise unwanted activity

Ceasing illegal activity is paramount to avoid further liabilities for CIC Hospitality and its employees, and to mitigate reputational damage. A priority of CIC Hospitality is to ensure that all measures are put in place to cease any potential illegal activity. As the fact-finding process (cf. item 6 below) can identify new elements of illegal activity, CIC Hospitality shall constantly assess whether to adopt new measures to ensure that unlawful activity does not take place.

Below are set out some examples of Compliance Matters where it is paramount to instigate measures to stop illegal/unwanted activity:

- Security measures that reduce the risk of further human or environmental damage
- Suspension of all transactions with contracting parties in case of suspicion of bribery, money laundering/terrorist financing or sanctions/export control violations.
- Instigating IT measures to mitigate the consequences of a cyber-attack

6. Targeted fact finding

In responding to a crisis, accurate information and understanding the root cause of the Compliance Matter is key. An adequate and detailed remediation plan requires a targeted and objective

investigation to establish the facts surrounding the event -- the what, who, when and how -- of the Compliance Matter.

The scope of the fact-finding and choice of methodology must be tailored to each case.

Fact-finding may be based on reviewing all available written material (e-mails, documents, etc.) and/or interviews with employees. As an example, it may be beneficial to utilize a keyword-based approach when dealing with large amounts of data.

Due to confidentiality considerations obtaining information from external parties should be carefully assessed on a case-by-case basis.

CIC Hospitality should at an early stage of a fact-finding process assess the need to engage an external counsel to secure a robust and legally privileged fact-finding process.

7. Securing data and access to employee emails etc.

Relevant data (e-mails, documents, etc.) through PC, smart phones, servers etc. and hard copies of documents that are not stored electronically must be identified and be secured as fast as possible to avoid the potential of loss of data/evidence.

The securing of data can be executed either by internal IT-resources or by external service providers. In cases involving potential misconduct by employees, the use of an external service provider should on a case-by-case basis be considered to ensure independence and chain of custody.

Employee e-mails and other electronic documents may only be accessed in line with current privacy and GDPR regulations.[5]

8. Legal assessments

An (external) legal assessment of the Compliance Matter should be made as soon as sufficient facts have been collected to assess (i) whether there has been a violation of internal policies and procedures and/or laws and regulations; (ii) to clarify the Company's civil and criminal liability risk and (iii) identify appropriate mitigating measures under applicable legislation.

9. Ensuring confidentiality and legal privilege

The Compliance Matter must be treated with confidentiality and information may only be shared internally on a strict need-to-know-basis. On-boarding of additional internal resources must be pre-approved by the CEO, and such resources must be instructed to keep any information pertaining to the Compliance Matter strictly confidential.

In a court proceeding, CIC Hospitality may be under legal obligation to disclose relevant internal and external correspondence in relation to handling a Compliance Matter. Having to disclose such documentation can increase both CIC Hospitality legal exposure and reputational damage. Hence, it is of importance to be cautious on the content of information that is exchanged in internal emails, e.g. between management colleagues.

Exempt from the said legal disclosure obligation is privileged correspondence to and from CIC Hospitality's external lawyer.

---

[5] For Norway: See regulations on employers' access to e-mail and other electronically stored data: https://lovdata.no/dokument/SF/forskrift/2018-07-02-1108

10. Interactions with public authorities

In certain instances, a company will have legal obligations to report to the authorities, e.g. in relation to serious human injuries or environmental damage. In matters in the economic crime area the Company will often not have a legal obligation to self-report[6]. However, timely and proactive cooperation with the authorities in such matters can (significantly) reduce corporate legal liability. Approaching the authorities with a Compliance Matter can also mitigate reputational damage, e.g. by way of reducing the risk of unannounced searches of premises by public authorities.

On the other hand, self-reporting to the authorities can lead to investigations against the Company and its employees, which may have significant adverse impact for the Company.

In Compliance Matters where there is no legal obligation to self-report, CIC Hospitality shall, with the involvement of the Chair, assess whether it is in the best interest for CIC Hospitality, considering all relevant factors (pro et con assessment), to report to the relevant authorities. Any decision to contact public authorities shall be pre-approved by the Board.

Dawn Raids is an inherent risk associated with Compliance Matters. Dawn Raids can impose massive reputational damage to the Company and dealing properly with the authorities in this context is paramount. CIC Hospitality has developed separate guidelines for how to handle unannounced inspections from public authorities. Referring to **Inspections of by authority Policy**

11. Disciplinary actions

In Compliance Matters where it is suspected that Company employees have been engaged in illegal or improper conduct, proportionate disciplinary actions should be legally assessed and executed. The same principle also applies towards the Company's contracting parties that may have acted improperly. Under certain legislation, instigating adequate disciplinary actions may reduce a company's legal liability risk and may also be a prerequisite to fulfill the requirements of self-cleaning under the public tender regulations[7]. Also, under private contracts a company's self-cleaning actions may be necessary to mitigate legal and commercial risk.

12. Crisis communication

Ensuring adequate external communication during a crisis is paramount. The CEO shall consider engaging an external communications expert at an early stage of a Compliance Matter to ensure that an optimal strategy for communication is developed. The CEO shall consult with the Board prior to engaging an external communications expert and before making any statements to the media. Only the CEO (or the Chair) shall speak to the media on CIC Hospitality behalf.

13. Improvements to the compliance program and lesson learned

Managing a Compliance Matter may represent valuable knowledge to the Company. Measures to prevent recurring situations shall be evaluated and implemented as part of the remediation plan. Examples of potentially relevant measures are:

- Targeted amendment of policies and procedures, e.g. revision of the Company's anti-corruption policy Enhancing HSE measures
- Strengthening IT systems/- procedures

[6] Under Norwegian law there are no legal obligations to self-report, but the Company must on a case-by-case basis closely observe whether such obligations exist under foreign law.

[7] For Norway: See Anskaffelsesforskriften § 24-5 c): https://lovdata.no/dokument/SF/forskrift/2016-08-12-974

- Organizational changes
- Implementing and/or improving targeted internal controls
- Training of employees

14. Training and testing

It is the responsibility of CIC Hospitality to ensure that the organization is appropriately prepared to manage a Compliance Matter. As part of the overall compliance training activities of the Company, CIC Hospitality shall ensure that relevant personnel receive appropriate crisis management training (e.g. through workshops addressing realistic crisis scenarios). Training and attendance shall be documented.

Inspections by authorities Policy

These instructions shall be followed in case representatives of public authorities request access to the company's premises with the purpose of searching for evidence. This may be officers of the Norwegian competition authority (Konkurransetilsynet), the EFTA Surveillance Authority (ESA), The Norwegian Labour Inspection Authority (Arbeidstilsynet), the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) / the police, the Norwegian tax authorities, or other public authorities. Any of the public authorities might be assisted by the police.

1. Ask for identification documents for each officer, copy the documents or register name and the authority which they represent. If relevant, hand out visitor cards. The officers might refuse to identify themselves before the person the officers are asking for is present.

2. Immediately notify the person the inspectors are asking for, and notify at least one of the following persons in the company, irrespective of whether they are engaged in meetings or telephone calls. Inform that inspectors from the relevant authority have arrived. Contact the responsible Operation Manager where the authorities visit.

- Thomas Furulund	thomas@cichospitality.com
- Øyvind Øhman	oyvind.ohman@cichospitality.com
- Kenneth Røynås	kenneth@cichospitality.com
- Mark Emil Grenaa	mark@cichospitality.com
- Theis Nørskov	theis@cichospitality.com
- Morten Næssvik	morten@cichospitality.com

3. In case the inspectors do not accept that the Operation Manager t is being notified, inform them that the company routines instruct you to contact **external counsel**. See point 6 below.

4. Ask for the document that authorizes the inspection and make a copy. This can be a decision from the district court or from the relevant authority. The officers might refuse to hand over this document before the person the officers are asking for is present.

5. Ask the inspectors to wait in the reception or other locations without access to documents and archives until any of the persons listed above or the executive officer/head of department have arrived. Do not answer any questions about the company, and refer to one of the persons listed in point 2 above. In case the inspectors insist on immediate access, do not obstruct them. If possible, follow the inspectors into the premises.

6. Contact the company's attorney in **Advokatfirmaet Schjødt AS at tel 22 01 88 00.** Ask for one of the following persons, stating that you need immediate contact as a matter of urgency:

   - **Metta Eiane (**mobile 97 400 830)
   - **Dag Sigvart Kaada** (mobile 928 81 390)
   - **Andrea Nilsen** (mobile 953 33 214)

Antitrust Compliance Policy

CIC Hospitality is committed to conducting business in accordance with the highest ethical standards. Maintaining these standards has never been more important than in today's competitive and rapidly changing business climate, and I am committed to ensuring that our company consistently demonstrates a reputation for integrity.

As employees of the Company, we are all expected to be familiar with the Company's antitrust compliance policy as further set forth herein. Although we cannot anticipate every situation or decision we might face, this document outlines the principles for observance and compliance with antitrust/competition laws and regulations and identifies the channels and procedures we have established to answer your questions.

In every business decision we make, it is essential that we follow the ethics and principles of antitrust compliance policy and fulfill our responsibility to report anything that might violate the principles set forth herein. Our goal is to create an open atmosphere that encourages employees to voice concerns about compliance issues without any fear of retaliation.

I expect that all of us will conduct our responsibilities according to the letter and spirit of the principles and guidelines outlined in this Policy. Failure to do so could constitute grounds for disciplinary action or termination.

I, however, do not expect you to become an expert in competition law or to undertake any legal analysis. We have our deputy CEO Andreas Buestad for that and he is available to you to answer your questions and guide you in your decisions, and will engage outside counsel as necessary. Should you, for any reason, feel that you wish to speak to any other person, please always feel very free to reach out to me personally or to the chair of our board of directors.

Respectfully,

Matthias B. Tanski
CEO

Introduction

1.1 Overview

Depending on the circumstances, the Company may be subject to antitrust/competition laws and regulations ("**competition laws**") in Norway, the EU/EEA, the United States, or elsewhere. While the legal requirements vary across these jurisdictions, competition laws generally share the same objective: to ensure that markets operate efficiently by providing competitive prices, product choice and innovation. This means, for example, that buyers should have a range of independent competing sellers who have not acted together to reduce the degree to which they compete. Likewise, a seller should be faced with competing buyers who are acting in their individual best interests to reduce costs.

In addition to coordinated conduct, the competition laws also prohibit certain types of unilateral conduct that might significantly impair competition. Where a company significantly dominates a certain market such that it can operate without taking much account of any impact on competitors and customers, it must be careful not to damage competition through anticompetitive behavior.

1.2 Enforcement

Any violation of competition laws within our organization may subject the Company (including all companies under the control of or under common control with the Company) to substantial sanctions and fines[8] and would represent a risk to the Company's reputation and may lead to invalidity of contracts and exclusion from public tenders. Violation of competition laws may also subject individuals to criminal liability. Moreover, a third party who suffers loss as a result of actions in breach of such rules may be able to bring private damages claims before national courts. Such civil litigation is burdensome, expensive and time-consuming for all concerned, even for those to whom the outcome would ultimately be favorable.

1.3 Scope

This antitrust compliance policy (the "**Policy**") includes the following:

(a) A statement of the Company's general policies on competition law matters, including the responsibilities in this regard for each employee (in Section 2);

(b) Guidelines to assist you in understanding and fulfilling your responsibilities to comply with the Company's antitrust compliance policies (in Section 3);

(c) Guidelines for conduct when dealing with actual or potential competitors (Section 4);

(d) Guidelines for conduct when dealing with actual or potential suppliers or customers in the course of our operations (Section 5);

(e) Additional guidelines to Section 5 for dealing with distributors/dealers (Section 6); and

(f) Guidelines for conduct of mergers and acquisitions (Section 7).

1.4 Reporting potential misconduct

We strongly encourage you to speak up if you ever come across violations of competition laws or this Policy within our organization.

Any discovery of actual or potential breaches of applicable competition laws must immediately be reported to the CEO or to the chair of our board of directors who will always ensure confidentiality of such report and the person(s) making it and be responsible for the further handling and conclusions thereof, including any notification of relevant authorities.

General statement

The Company has adopted this Policy to set forth and communicate our standards and expectations with respect to observance and compliance with competition laws. This Policy is founded on the following key principles:

1. All business decisions shall be made on an independent basis and any coordination and cooperation with competitors should be avoided to the extent that it may impair competition between us.

[8] Fines may amount to (but not exceed) 10% of annual company group turnover.

2. In markets where the Company may be deemed to hold a dominant position (whether locally, domestically or beyond), we must ensure not to restrict competition through abusive actions or practices.

3. It is the individual responsibility of all personnel to comply with all applicable competition laws.

4. Employees in management positions are personally accountable not only for their own actions but also for the conduct of their subordinates. Therefore, each manager should take care to implement appropriate internal controls to reduce the risk of antitrust violations.

5. Employees have no authority to engage in, permit other employees, agents or other representatives of the Company to engage in, approve or tolerate any conduct that violates applicable competition laws or this Policy.

6. Any personnel who violates the terms of this Policy may be subject to disciplinary action, up to and including termination.

7. If ever in doubt about competition laws, this Policy or whether any activities are permissible thereunder, discuss with your superior or a Responsible Officer.

8. The Company will provide materials and training as needed that explain in a practical manner what is expected of personnel who are likely to face antitrust/competition law issues in connection with their day-to-day responsibilities.

9. The Company, and all of its personnel, shall actively cooperate with relevant competition authorities in relation to any inquiries or investigations of the Company's activities[9].

Consistent with the foregoing principles, all personnel must personally comply with applicable competition laws and this Policy. No personnel have the authority to direct or approve any violation of the competition laws, nor will the Company condone any conduct that could give rise to breach of competition laws.

Guidelines for compliance with competition laws

Competition laws affect virtually every activity of a company, from general management to engineering, sales, after sales, marketing, international operations, pricing, and purchasing. The purpose of this document is not to train you to answer competition law questions but to help you recognise potential issues so that you can obtain advice from a Responsible Officer and, if necessary, the Company's outside counsel.

As all other Company personnel, you are responsible for reading and understanding the following guidelines.

Below are some critical highlights to keep in mind to avoid competition law problems:

1. **Never** discuss competitively sensitive information with the Company's competitors, such as prices, the timing of price changes, costs, margins, contract terms, discounts and rebates, capacities, tender/bids for business, new projects, strategies, business plans, suppliers, customers, or any other similar information. This prohibition applies at all times

[9] A specific dawn raid manual is available and provides guidance on how to engage with competition authorities in case of a dawn raid and evidence seizures.

and locations, including trade association activities, on social occasions and in social/media.

2. **Never** attend a conversation or meeting with a competitor at which the subject of price or other competitively sensitive information (as further explained above) is likely to be exchanged or discussed. If sensitive information is discussed in such conversation or meeting, then immediately leave the conversation/meeting (and do not share the information received with anyone).

3. **Never** suggest to anyone that the Company does anything other than compete vigorously, that its prices are based on anything other than its own business judgment, or that the Company's public statements or actions are intended as "signals" to competitors for them to follow the Company's stated actions.

4. **Never** agree with a customer or competitor not to deal with other companies.

5. **Never** require a customer to purchase from the Company as a condition of you purchasing from such customer, or threaten a customer that unless he or she buys from the Company, you will not purchase from such customer (so-called "reciprocal dealing').

6. **Never** do any of the following without the prior approval of an Operation Manager[10]:

   - limit the territory in which a customer may resell the Company's products;
   - limit the persons or companies to whom a customer or distributor may resell the Company's products;
   - require a customer purchasing one product or service to purchase another product or service (so-called 'tying arrangement');
   - prohibit a customer from purchasing from the Company's competitors (so-called 'exclusive dealing arrangement'); or
   - terminate a significant customer.

7. **Never** overstate the Company's share of any market or use terms such as "dominant", "market leader" or "without/with little competition" in describing the Company's position in the markets that it addresses.

8. **Always** compete hard, but focus messaging (including internal messaging) on the benefits our products have for customers rather than the harm that our success will cause to our competitors. In particular, avoid phrases like "we want to crush/ eliminate the competition."

9. **Always** report suspected competition law issues to an Operation Manager.

The above guidelines are intended as an aid to assist you in understanding and fulfilling your responsibility to comply with the Company's antitrust compliance policies. They are not intended to make you an expert, but rather to help you identify competition law issues that could arise in the course of your job responsibilities. Also, note that the practices described above do not encompass every type of arrangement or agreement which may be held to violate competition laws. Any arrangement which restricts commercial opportunities or commercial freedom of competitors or

[10] National or international trade/economic sanction laws and regulations may require the Company to impose restrictions of the kind listed in this section 6, which will generally be permitted. However, an Operation Manager should still be consulted.

customers may raise potential concerns under applicable competition laws. Any proposed agreement which may appear to have such an effect should be brought to the attention of a Responsible Officer to ensure compliance with the law.

Dealings with competitors

The basic premise of competition laws is that each company must make its business decisions independently of other competitors. Arrangements among actual or potential competitors to fix prices, to reduce price competition by allocating customers or markets, or to exclude other competitors from the market represent the most serious violations of competition laws. Such arrangements are almost always held to be illegal *per se*, which means that they cannot be justified by arguments about market efficiencies or the reasonableness of the prices charged.

Guidelines for conduct when dealing with competitors:

1. **DON'T** enter into arrangements with competitors that relate to pricing or other contract terms, production/output, customers, bids (or abstention to bid) or sharing or allocating markets, and consult with a Responsible Officer before entering into any other arrangements with a competitor.

2. **DO** gather competitive intelligence[11] from publicly available sources but **DON'T** gather or share information from or with competitors. **DO** carefully document your sources for any competitive intelligence.

3. **DO** keep your writings, statements and actions regarding competitors as clear and unambiguous as possible to avoid any impression that any arrangements exist with a competitor or that competitively sensitive information is being exchanged with a competitor.

4. **DO** consult with a Responsible Officer before engaging in trade association activities or events, strategic alliances, joint arrangements, industry surveys, or other activities that could involve meetings with or communications with competitors.

For completeness, please note that companies that directly or indirectly are under the control of, or under common control with, the Company are not considered competitors under competition laws.

Relationships with customers and suppliers

Relationships with suppliers and customers are extremely valuable business assets and must be protected. A company generally is free to choose its suppliers and customers, and to refuse to do business with any particular company. However, some arrangements such as forced reciprocal dealing (as further explained in Section 3 above) and exclusivity requirements may raise competition law issues. Moreover, no personnel should misstate the price or terms received from another supplier to induce the offer of a discriminatory price. There may be limited exceptions to these rules, but any conduct of this type must first be discussed with a Responsible Officer. When dealing with suppliers and customers, the Company's purchasing and buying decisions should be made independently and focus on the merits of the transaction itself.

Guidelines for conduct when dealing with suppliers or customers:

[11] See further explanation of competitively sensitive information under section 3 above.

1. **DON'T** agree or suggest to a supplier that the Company's purchases from the supplier will be based on that supplier's purchases from the Company.

2. **DON'T** misrepresent the price or terms received from another supplier to induce the offer of a discriminatory price.

3. **DON'T** discriminate among similarly situated, competing customers unless the differential treatment is justified by lower costs or is extended to meet a lower offer, without first obtaining approval from a Responsible Officer.

4. **DON'T** condition the purchase or sale of goods or services on a promise of exclusivity without first obtaining approval from a Responsible Officer.

5. **DON'T** condition the sale of one product or service on the sale of another product or service without first obtaining approval from a Responsible Officer.

6. **DO** consult with a Responsible Officer before placing any restrictions on a supplier's ability to deal with competitors of the Company.

7. **DO** obtain approval from a Responsible Officer before engaging in below-cost pricing, long-term agreements, bundled discounts, volume commitments, or any refusal to deal with a willing buyer.

Distribution/ dealer issues

In addition to the general rules for dealing with suppliers and customers set forth in Section 5 above, discriminatory treatment and interactions with distributors and dealers can raise unique competition concerns. Below are certain typical antitrust issues that need to be considered whenever the Company reaches customers through distributors/dealers.

Guidelines for conduct when dealing with distributors:

1. **DON'T** force or pressure a distributor regarding its pricing policies or engage in activities that might appear to be an effort to control resale pricing (however merely 'recommended prices' or maximum prices are generally permitted).

2. **DON'T** speculate about the prices or terms offered by an independent distributor or imply that the Company controls the distributor's pricing (e.g. by providing price quotes to a customer on behalf of the distributor).

3. **DON'T**, in situations where the Company is competing with one of its independent distributors, discuss price or other terms of sale, and do not engage in any other activity that would be prohibited under "Dealing with competitors" in Section 4 above.

4. **DON'T** provide discounts, services or materials to one distributor unless you make equivalent terms available to competing distributors.

5. **DO** consult with a Responsible Officer before imposing any restrictions on a distributor's sales to customers (including restrictions pertaining to customer groups or territories that the distributor may address) or its right to deal with competitors of the Company.

6. **DO** consult with a Responsible Officer before imposing any requirement that a distributor or customer purchases multiple products or services together, deal only with the

Company, or enter into any of the arrangements referred to under “Relationships with customers and suppliers” in Section 5 above.

Mergers & acquisitions: conduct of transactions and merger control

Competition laws apply also in the context of corporate transactions involving mergers and acquisitions. Firstly, competition laws are relevant to how transactions and negotiations are conducted, the further terms of such transactions as well as the transacting parties’ conduct in the market until completion. Secondly, competition laws include specific merger control rules which may require the notification of a transaction to relevant competition authorities for their review and consent, in which case the transaction may not be completed until it has been cleared by relevant competition authorities.

Guidelines for conducting M&A-processes

1. **DO** involve the CEO before proceeding with a transaction to consider whether it may trigger mandatory merger filing obligations in any jurisdictions as well as the risk that any competition authorities may prohibit or require remedies (divestments, etc) to clear the transaction.

2. **DON’T** exchange competitively sensitive information[12] with any transacting party or its affiliates or representatives without first obtaining approval from a Responsible Officer.

3. **DON’T** divulge competitively sensitive information relating to other transacting parties to any of our personnel responsible for the Company’s day-to-day operational business decisions without first obtaining approval from a Responsible Officer.

4. **DO** operate the Company in the ordinary course and independently of the other transacting parties until completion of the transaction has occurred, unless a Responsible Officer has approved otherwise.

5. **DON’T** carry out steps that may imply or contribute to a change of control in the target company if the transaction is subject to mandatory notification with any competition authority and said authority has not yet cleared the transaction.

6. **DON’T** in the course of the transaction engage in, or agree to engage in (whether in the transaction agreements or otherwise), with the transacting parties any activity that would be prohibited under “Dealing with competitors” in Section 4 above.

[12] See further explanation of competitively sensitive information under section 3 above.

Anti-corruption Policy

In CIC Hospitality we are committed to conduct business in compliance with all applicable laws and regulations, and with the highest ethical standards and integrity as reflected in the Company's Code of Conduct.

Corruption is unacceptable business conduct, constitutes a threat to fair competition and undermines legitimate business activities. We oppose corruption in all forms – direct as well as indirect, and in both the private and the public sector. Any violation within our organization may subject both CIC Hospitality and individuals to criminal liability, and would represent a risk to our reputation.

The policy is developed with the purpose of describing our standards and expectations to conduct with respect to anti-corruption. The policy aims at providing practical guidance to create a common ground in CIC Hospitality with respect to compliant behavior.

I encourage you to get familiar with the guidelines and speak up if you are in doubt about what is the right thing to do.

Matthias B. Tanski

Introduction

1.1 Scope and purpose

CIC Hospitality opposes corruption in all forms – direct and indirect, in the public sector and the private sector.

This Anti-Corruption Policy is prepared to provide practical guidance and instructions on how to best deal with situations that may constitute corruption. Corruption often occurs in connection with other types of crime, such as money laundering, which is also covered in this Policy.

This Policy does not purport to be all-inclusive, and it is expected that you use your own judgment at all times to follow the high ethical standards to which the Company is committed.

The Policy applies to all employees (including hired personnel) and directors of the Company. It also applies to the Company’s subsidiaries and majority owned joint ventures, as well as to sales representatives, agents and others who act on the Company's behalf. The Policy shall formally be made part of the agreement with such third-parties.

It is required that everyone working for or on behalf of our Company familiarize and act in accordance with this Policy. This means that you must understand what types of payments, transactions and business activities that may expose yourself and the Company to corruption and money-laundering risk.

1.2 Important information and instructions

Any questions you may have regarding this Policy may be taken to the CEO of the Company.

If you are in doubt whether your actions are interfering with the policies in the current moment, also consult the CEO.

Any inquiry or clarification within the scope of this Policy shall be properly documented. It is the responsibility of the person(s) receiving the inquiry/report to properly document the matter.

Any contract or other arrangement entered into other than in the regular course of business shall require the prior written approval of the CEO.

1.3 Reporting misconduct

Any violation of this Policy may subject both the Company and individuals to criminal liability and other severe legal consequences and would represent a risk to our reputation.

We strongly encourage you to speak up if you ever come across possible violations of the Policy.

All potential/actual corruption and money laundering discovered shall be reported immediately according to the Company's Whistleblowing Policy[13] or directly to the CEO. Such reports, the handling thereof and conclusions made shall be properly documented.

The CEO or the board of directors may initiate internal and/or external investigations to clarify relevant facts in relation to a report on possible corruption and money-laundering. Findings may be reported to the relevant public authorities.

1.1 Consequences of breach

Any breach of this Policy may put the Company and individuals at severe risk, and we take appropriate actions to mitigate such violation. The Company may take remedial actions that could have adverse consequences for the employee's employment or a business partner's relationship with the Company.

With respect to employees, breaches could for example result in written warning, dismissal, civil claims, and/or reporting to public authorities that could result in criminal investigations and convictions.

2. Legal context

The Company is subject to Norwegian law and under Section 27 of the Norwegian Penal Code Companies may be held criminally liable when a penal provision (e.g. the corruption or money laundering provision) is contravened by a person who has acted on behalf of the company.

Further, our Company's foreign subsidiaries and affiliates may be subject to local anti-corruption laws. The Company's policy is to comply with all applicable anti-corruption and anti-money laundering legislation in the countries of our operations. The Company's activity may also be subject to certain extraterritorial laws, such as the US Foreign Corrupt Practices Act and the UK Bribery Act. Exposure under such laws should always be taken into consideration and may influence the Company's decision-making.

[13] Details and guidelines with respect to reporting concerns are set out in the Company's Whistleblowing Procedure

3. Anti-Corruption

3.1 What is corruption?

Corruption means offering, promising or giving any person (directly or indirectly), or requesting, receiving, accepting or soliciting for oneself or others, an improper advantage in connection with the person's performance of a position, office or assignment.[14]

- Corruption in the private sector and the public sector is prohibited.
- Both an active and a passive corrupt act is prohibited. Active refers to the act of promising or giving the bribe, as opposed to the act of receiving a bribe (passive). The term does not mean that the active party has taken the initiative, since the bribe may have been demanded by the receiving party (who commits “a passive corrupt act”).
- Note that simply the act of offering someone a bribe is sufficient to be held liable under many anti-corruption laws, even if that offer is rejected. No actual transfer of money, goods etc. has to be made.

An advantage may constitute anything that the recipient finds in his/her interest or can derive benefits from. For example, cash, loans, gifts, favors, entertainment, education, job positions within the Company and travels.

Important factors when determining whether an advantage is improper, are i.a. the purpose, value and frequency/recurrence of the advantage. If the advantage is intended to influence the recipient’s execution of its professional duties it will normally be regarded as improper.

Aiding and abetting corruption is also prohibited. For instance, an employee that authorizes a money transfer knowing, or holding it likely, that the payment represents a bribe, can be held criminally liable for aiding and abetting, even if he/she has had no involvement in the planning or setting up the corruption scheme.

3.2 Examples of prohibited conduct and characteristics of corrupt payments

The below list set forth examples of actions that you are prohibited from conducting:

- Offering, promising or giving a financial or other kind of advantage to another person with the intention to (i) induce a person to perform improperly a relevant function or activity, or (ii) in order to reward a person for the improper performance of such a function or activity.
- Offering to pay, paying or authorizing the payment of money or anything of value to a public official in order to influence any act or decision of the public official in his or her official capacity, or to secure any other improper advantage in order to obtain or retain business.
- Paying a facilitation/grease payment (see further guidance in section 3.4 below).
- Requesting, accepting or receiving a financial or other kind of advantage for yourself or others to i) improperly perform your duties, function or activities, or (ii) as a reward for the improper performance of such a duty, function or activity.

[14] The Norwegian Penal Code Section 387

- Aiding and abetting to the above listed conduct, e.g. by approving a corrupt payment.[15]

Typical characteristics of corrupt payments that you should be observant to are:

- Personal enrichment of decision makers (in public or private sector) or of someone in the Company.
- Payments or other things of value given to influence decisions, such as a tender or contract negotiations, or a permit or license from a public office.
- Payments or other things of value not offered, given or received in a transparent way.
- Measures are taken to hide or camouflage the money trail.

3.3 Gifts and hospitality

3.3.1 Why is this a concern?

Gifts may constitute, or be perceived to constitute, an improper advantage.

Hospitality expenses may be misused for bribery purposes, even though reasonable, proportionate and bona fide business hospitality expenses are not prohibited under applicable anti-corruption laws. The term 'business hospitality' should be taken to mean meals, travel, accommodation and entertainment that is related to a business meeting or otherwise has a clear business purpose.

3.3.2 Company policy on gifts and business hospitality

a) Gifts and business hospitality should always be given, offered and received in a transparent way and in a professional context.

b) It is not permitted to offer or give gifts or business hospitality to public officials. Because of their trusted positions, public officials will be subject to strict rules, and no representative of our Company should ever try, or be perceived to try, to influence the decisions of a public official by the use of any improper means. For example, it is not permitted to offer or provide a benefit in relation to persons exercising authority or decisions on public procurement. This also includes in relation to employees or officers of public agencies or government/publicly owned or controlled companies.[16]

c) Gifts or business hospitality shall never be offered or provided to persons exercising authority, or who may influence the decision, in a tender or contract negotiation that the Company is involved in.

d) Gifts and business hospitality must never be extravagant and should be in accordance with customary business practices.

e) Cash or cash equivalents may never be offered, given or received.

[15] The Norwegian Penal Code Section 15 cf. Section 387

[16] Any officer or employee of a government owned or controlled entity may be considered a public official under the U.S. Foreign Corrupt Practices Act. Furthermore, employees and officers of government owned companies that exercises a public function are considered public officials in relation to the UK Bribery Act. Under Norwegian law, employees of listed or private limited companies that are owned or controlled by the Norwegian government, e.g. Equinor ASA, are as a main rule not considered public officials or deemed to be trusted with public authority.

f) You must not donate gifts or other benefits on behalf of the Company (or its associates) for the purpose of achieving benefits in return for yourself or the Company (or its associates).

g) A gift may be offered or received in relation to employees or contractors of privately owned companies when it is in line with the abovementioned requirements, it is moderate and does not exceed a value of 1.000 NOK

h) Business hospitality may be offered or received in relation to employees or contractors of privately owned companies when it is in line with the abovementioned requirements, it has a proper business context and does not exceed a value of 2.000 NOK

i) If you receive or become aware that you will be offered a gift or business hospitality that is not in accordance with the requirements set out above, your immediate superior shall be informed and shall decide whether accepting such gift/business hospitality might affect your impartiality and therefore whether it may be accepted/kept or rejected. When in doubt, the superior shall consult [the head of compliance/legal or the CEO].

j) All expenses must be accounted for in compliance with applicable laws and internal guidelines. You are responsible for reporting any gifts or benefits received from third parties to the tax authorities and/or other public authorities in accordance with applicable laws and regulations at any time.

3.4 Facilitation/grease payments

3.4.1 What are facilitation payments?

Facilitation payments or “grease payments” describe payments that are made to speed up decisions and approvals the Company is legally entitled to receive, even without making the payment. Facilitation payments are typically made to a public official in order to secure or expedite routine, non-discretionary government actions to which a company is entitled. Typically, facilitation payments will only affect the timing of a decision and not the outcome. In many countries, facilitating payments is considered a corrupt act and is prohibited.

3.4.2 Examples of facilitation payment

- Paying a small sum to a public official to obtain or expedite certain approvals which are needed to conduct business in that country, and we are legally entitled to because we have met all the requirements.

- Making a small payment to a public official responsible for checking entry visa on arrival to get his/her approval to enter the country, in a situation where you have a valid entry visa.

- Making cash payments to customs officials to release unrightfully held goods in customs.

3.4.3 Company policy on facilitation payments

a) You are prohibited from making facilitation payments.

b) The prohibition does not apply to situations where you must make such payment to avoid a serious medical or safety emergency.

c) If you are ever requested by someone to make a facilitation payment, you should immediately report it to the CEO.

d) In the event you must make a facilitation payment to avoid a serious medical or safety emergency, you should as far as possible seek prior approval before making the payment from the CEO. Further, the details of the payment should be promptly reported to the CEO after the event.

3.5 Conflict of interest

3.5.1 What is a conflict of interest?

Conflict of interest may give rise to situations exposing the Company to corruption risks. A conflict of interest occurs when an individual's personal relationships, participation in external activities or interest in another venture could influence, or could be perceived to influence, the individual's decision making when acting for the Company.

Personal relationships considered to have the potential of causing conflict of interests are close family relations (spouse, children, parents and siblings) and close friends.

3.5.2 Examples of conflict of interests

- The spouse of the Company's purchasing director is the CEO of a potential supplier. In such a case, the purchasing director could have conflicting interests with regards to a preference for this supplier that is not necessarily in the best interest of the Company. It must be assessed whether he/she should be excluded from decision making relating to rendering of services from the supplier.

- A sales manager of the Company holds an ownership stake in a company that provides certain services that may be in competition with parts of the Company's services. In such cases, the sales manager could have conflicting interests with regards to tendering for certain projects where the two companies may be competitors. It must be assessed whether he/she should be excluded from negotiations and other dealings with the tender.

3.5.3 Company policy on conflict of interests

a) Act in the best interest of the Company and take necessary steps to avoid situations or positions that may conflict with, or that could be perceived to conflict with, the Company's interests.

b) You should avoid ownership, board positions or other assignments in any business that competes with or provides services to the Company, if it affects your objectivity in carrying out your responsibilities in the best interest of the Company.

c) Any directorships, engagement or other assignments in other companies that have, or may be expected to have, commercial relations to the Company, must be pre-approved in writing by your immediate superior.

d) Conflict of interest situations may occur and should be dealt with in an open and transparent manner. If you consider yourself to be in a potential conflict of interest situation, you should immediately report it to your immediate superior. The superior shall ensure that conflicted individuals are not involved in any operation, influence, and/or decision-making process associated with the subject of the conflict.

4. Trading in influence

4.1 What is trading in influence?

Trading in influence means giving or offering any person, or requesting, accepting or receiving for oneself or others, an undue advantage in return for influencing the conduct of another person's position, office or performance of an assignment.[17]

The offense is similar to corruption with one important difference: trading in influence concerns the "middleman", or the person that serves as the go-between the decision-maker and the party that seeks an improper advantage. The decision-maker may not even be aware of the illicit exchange between the “middleman” and the company.

4.2 Examples of trading in influence

- The Company's lobbyist or agent offers to use his/her influence in government or connections with persons in authority to obtain favors or preferential treatment for the Company, usually in return for payment.

- A legislator receives a payment from a company to attempt to convince fellow legislators to support amendments that would benefit that company.

The line between legal lobbyism and illegal trading in influence can be challenging to draw. However, key characteristics of illegal trading in influence are lack of transparency with respect to i) the principal and ii) that the interests are being promoted by the lobbyist in return for remuneration.

4.3 Company policy on trading in influence

a) Offering or giving an improper advantage to a third party in exchange for this person trying to influence the conduct of someone else is prohibited.

b) Engagement of a business development agent or a lobbyist must always be approved by the board of directors and shall follow the steps set out in the *Third Party Risk Management Procedure*.

5. Anti-money laundering and terrorist financing

5.1 What is money laundering and terrorist financing?

- Money laundering is the illegal process of making funds generated by criminal activity appear to have come from a legitimate source.

- Applicable money laundering legislation imposes broad prohibitions on any dealings with the proceeds of crime.[18] Proceeds from any crime is comprised by the provisions (sanctions violations, corruption, tax evasion, fraud etc.) Proceeds comprises anything gained from or connected to a crime (gains from stolen property, payments under a corrupt agreement, cost savings as a result of tax evasion etc.)

- Terrorist financing means any dealings with funds or other assets for the purpose of financing terrorism.[19]

[17] For Norwegian entities: The Norwegian Penal Code Section 389
[18] The Norwegian Penal Code Section 332 and 337
[19] The Norwegian Penal Code Section 135

5.2 Examples of money laundering

- The Company has a customer in Brazil, which utilizes its associated company incorporated in the British Virgin Island to make payments to the Company. The payment to the Company may constitute proceeds of crime, due to the risk that the customer and the BVI company are involved in tax evasion offenses towards Brazilian authorities.

- The Company's JV has obtained a public license due to the JV-partners corruption of a local decision maker. By receiving share dividends from the JV, the Company is exposed to the risk of receiving proceeds of crime, since the JV's profits are gained under a corrupt contract.

5.3 Company policy on anti-money laundering

a) The Company shall not be involved in money laundering.

b) Anti-money laundering should, on a risk based approach, be among the risks assessed as part of our due diligence in relation to onboarding of business partners, ref. the Company's *Third Party Risk Management Procedure*.

5.4 Accurate books and record keeping

- Any transactions must be recorded accurately and in reasonable detail in the Company's books and records. A failure to do so may constitute a criminal offense under applicable laws.

- Managing risks related to third parties

- If buying services from or forming partnerships with other companies, we expose our Company to a liability for the violation of anti-corruption and anti-money laundering laws by others. The Company's procedures and requirements for onboarding and follow-up of third parties are set out in the *Third Party Risk Management Procedure*.