GOOD BUSINESS PRACTICE

How we do business at Vion

Vion
FOOD GROUP

T +31 88 995 3555 | www.vionfood.com

Vion
FOOD GROUP

GB-02

TABLE OF CONTENTS

MESSAGE FROM OUR CEO 4

CODE OF CONDUCT 7

1 Introduction 8
2 General 9
3 Legislation 10
4 Competition 10
5 Animal welfare 11
6 Food safety and product integrity 11
7 Confidential information and privacy of personal data 12
8 Conflict of interest 13
9 Receiving and offering gifts and entertainment 14
10 Company assets and resources 15
11 Integrity of records 16
12 Bribery/corruption and records of transactions 17
13 Contributions to political parties and insider trading 18
14 Employee relations 19
15 Alcohol and drugs 20
16 Communications with third parties 20
17 Violations 21
18 Reporting inappropriate, unethical or illegal behaviour 22
19 Compliance 23
20 Further guidance 23

WHISTLEBLOWER POLICY 25

1 Introduction 26
2 What types of matters should be reported under this policy? 27
3 How can a matter be reported? 28
4 Follow-up after a report 29

WHAT YOU SHOULD KNOW ABOUT INFORMATION SECURITY, FRAUD AND CYBERCRIME 33

1 Introduction 34
2 Vion's ten commandments for cyber and information security 35
3 Stop and think 37
4 Examples of fraud 39
5 Examples of cybercrime 45
6 Recognition of the red flags for fraud 47
7 Key actions to prevent fraud 49
8 Do's and don'ts when dealing with fraud 51

APPENDIXES 52

REFERENCES 57

MESSAGE FROM OUR CEO

Everyone has the right to safe, healthy and sustainable food. That is why it is Vion's aim to bring people together, to build future- proof protein chains and provide **'Food that Matters'**. This objective is based on our company strategy of **'Building Balanced Chains'**, and it helps us to offer solutions to the food challenges that we as a company are confronted with in a fast-changing world.

Within Vion, we have a clear way of working throughout the company. This way of working is defined by our core values **'Sharp, Connected and Brave'**, which are gradually becoming part of our company-wide DNA. Thousands of employees from more than 40 nationalities work in our production locations in the Netherlands and Germany. We value and respect the hard work they perform, and make every effort to ensure their working environment stays pleasant and safe.

It is important for us, as employees, to protect Vion's good name. That is why integrity and ethical behaviours are important parts of our company culture. Everyone makes their own contribution and is responsible for upholding and complying with Vion's rules and legal principles. We have drafted the Good Business Practice Guide to explain these principles to everyone that works in our company, including employees with a flexible contract.

This guide consists of the following parts:

- **Our Code of Conduct.** This guideline explains how to do your work as well as possible, and how to make our core values part of your daily work situation. The document is divided into 20 topics that are particularly relevant for Vion's operating activities. In a case where you notice behaviour that is not in agreement with these principles, we urge you to communicate it. If necessary, Vion has provided you with an effective way to do this through our whistleblower policy, which is a way to report such cases without the risk of retaliation.

- Practical examples **information security** and **cases of fraud**.

When you work at Vion, you will receive the Good Business Practice Guide and are expected to read and understand it. I ask all of you to always act in accordance with the contents of this guide.

Ronald Lotgerink
Chief Executive Officer

CODE OF CONDUCT

1 INTRODUCTION

Vion has a mission statement that sets out our core values and business principles. Correct ethical behaviour, sincerity, trustworthiness and integrity are the guiding principles within Vion. This is laid down in a company code, the Code of Conduct (or simply the Code). The Code is applicable to all employees[1] of Vion Holding N.V. and its subsidiaries (Vion, or the Company) anywhere in the world.

The Code provides all of us who are employed at Vion with a clear set of guiding principles on integrity and ethics in our business conduct. The Code governs our business decisions and the actions throughout our Company. It applies to both company actions and the behaviour of individual employees when conducting Vion's business. These rules formulate the minimum requirements of behaviour and are not all-encompassing.

The management at each operating company has the freedom to specify rules over and above those stated in the Code for the conduct of a local business, provided that such rules are consistent with our business principles in general and this Code in particular, and with safeguarding Vion's good reputation worldwide.

It is the responsibility of the Executive Committee and each operating company manager to ensure that Vion's Code is communicated to and observed by all employees. In addition, Vion considers that the application of its Code is of prime importance when deciding to enter into or continue relationships with contractors and suppliers, and to participate in joint ventures.

The Code, which has been adopted by the Management Board, is reviewed on a regular basis and revised if necessary.

1 An employee, in the Code, means all employees of Vion, temporary workers and freelancers working for Vion, as well as workers employed by external parties carrying out work for Vion.

2 GENERAL

The Executive Committee refrains from any conduct whatsoever that could damage the business as a whole. It ensures that its employees also refrain from such objectionable behaviour. It avoids any real or potential conflict between its personal activities and the interests of the business.

The Executive Committee ensures that conduct with regard to expense claims is correct. The underlying principle is that claimable costs must be of a business nature.

The Executive Committee also ensures that all transactions carried out in the name of the business are accurate and properly substantiated in the financial reporting, in accordance with the reporting guidelines and subject to verification by external auditors. Irregularities that are identified or whose existence is suspected are notified directly to the Management Board or the Supervisory Board.

3 LEGISLATION

Vion is committed to observing all relevant applicable laws and regulations and expects all of our employees to uphold this commitment and to comply with all such laws and regulations. This includes all laws and regulations in any country in which the employee is based, or in which he or she is acting on behalf of the Company.

4 COMPETITION

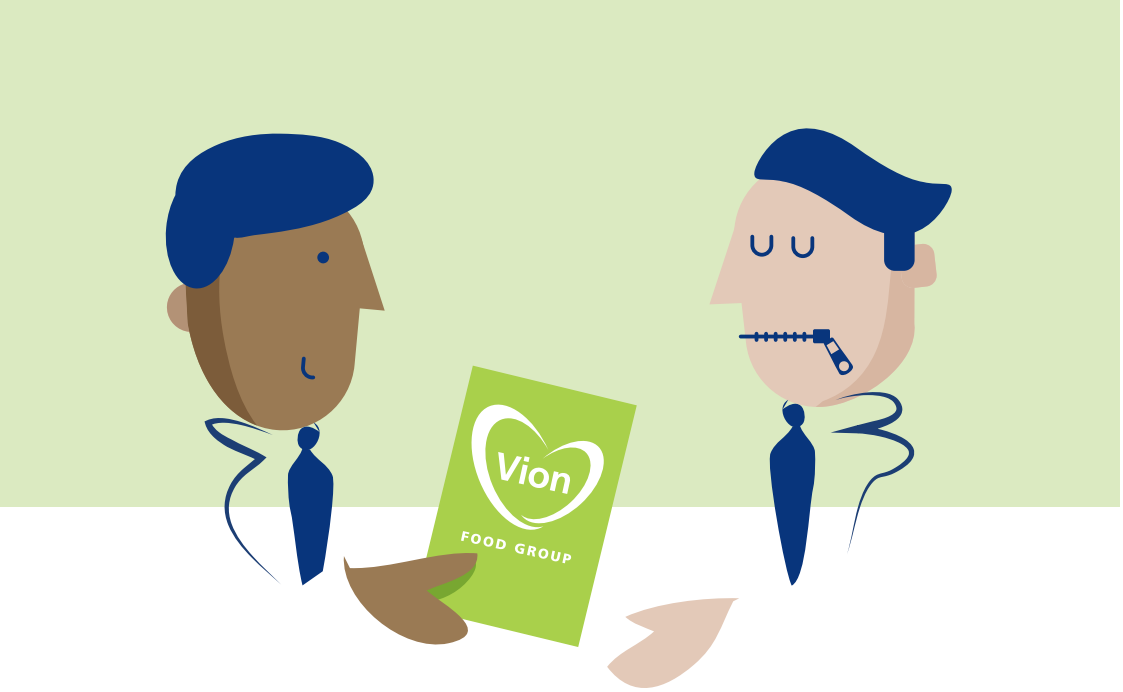
Vion believes in vigorous yet fair competition and supports the development of appropriate competition laws. Vion companies and employees will conduct their operations in accordance with the principles of fair competition and all applicable laws and regulations.

5 ANIMAL WELFARE

We handle thousands of animals every day. It is the obligation of all employees to respect animal welfare and the integrity of the animal in all our operations, ranging from transportation to our slaughtering activities. We expect every single person in our operations to be fully aware of this engagement, to apply this in their own work and to be an active provider of solutions in case of misconduct or the malfunctioning of a piece of equipment. Vion is constantly re-evaluating its infrastructure and operations and has systematically invested in its equipment, training of employees and has installed cameras to monitor and learn through surveillance.

6 FOOD SAFETY AND PRODUCT INTEGRITY

Wholesome and safe food is what the consumer expects from Vion. In order to achieve this, Vion works according to a globally accepted Vion-HACCP. Each employee who is working with Vion's products must follow these internal rules, and should be sufficiently trained to understand and apply these rules. Personal hygiene and working according to the internal rules are critical, and this includes the rule that when an employee or a visitor is feeling ill, this needs to be reported immediately. Product integrity is core to Vion. Customers can trust that *"what is on the label is in the package"*.



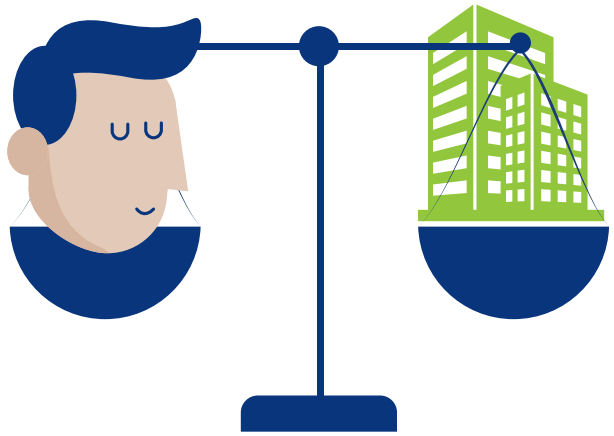
7 CONFIDENTIAL INFORMATION AND PRIVACY OF PERSONAL DATA

Employees shall treat all Company information as confidential and they shall not disclose Company information to third parties, without the express consent of their direct supervisor. Employees have a duty to respect and protect Company information, including information held on computers and other devices, and to not disclose any Company information even after they end their employment.

We protect the privacy and security of the personal data belonging to our employees, our suppliers and customers and others we do business with. Personal data may only be used for legitimate business purposes and to the extent permitted by law. Employees that suspect there has been a breach of the Company's data security should report it immediately.

8 CONFLICT OF INTEREST

All employees are expected to conduct their activities with the Company's best interests in mind. Employees shall avoid any conflict of interest (including behaviours that, in themselves, are not strictly conflicts of interest, but which may appear or be seen as conflicts of interest by others) between the interests of the Company and the employee's personal interests. In particular, conflicts of interest that are not allowed are business transactions between the Company and suppliers and/or customers in which the employee or any of his or her family members have a financial or management interest, unless such a transaction has been explicitly agreed and accepted by the local or higher management, in the event that the local management is involved. Any conflict of interest shall be reported to the direct supervisor of the employee concerned. In the event of doubt, the employee should discuss the matter with his or her direct supervisor.



9 RECEIVING AND OFFERING GIFTS AND ENTERTAINMENT

As a general rule, employees shall not accept gifts or entertainment from, nor offer gifts or entertainment to, suppliers, customers and others with whom the Company has a business relationship and that exceed a value that can be considered as a customary courtesy (maximum value of € 50). Cash shall never be accepted or offered. The Company recognises that, in some cultures, business gifts and entertainment play an important role. Should refusing a gift carry the risk of jeopardising a business relationship, then the employee should refer the matter to his or her direct supervisor.

10 COMPANY ASSETS AND RESOURCES

Each employee is responsible for the proper use, protection and conservation of Vion's assets and resources, as well as for the confidential information disclosed to us by our business partners. This includes Vion's properties, assets, proprietary interests, financial data, trade secrets, information and other Vion rights. Vion's assets and resources, as well as opportunities, are to be used to pursue and achieve Vion's goals and not for personal benefit. A person who believes he or she might have a conflict of interest should discuss the issue with his or her immediate superior.

11 INTEGRITY OF RECORDS

Vion's business records form the basis of reliable and accurate reports to management, shareholders, creditors, government bodies and others. Thus, all official records of Vion's business must be accurate, honest and complete. Vion does not condone the concealment of any payment by means of passing it through the accounts of third parties, such as through agents or consultants. All Vion operations must comply with all local and national laws and regulations relating to the accurate and complete maintenance of financial accounts and records.

12 BRIBERY/CORRUPTION AND RECORDS OF TRANSACTIONS

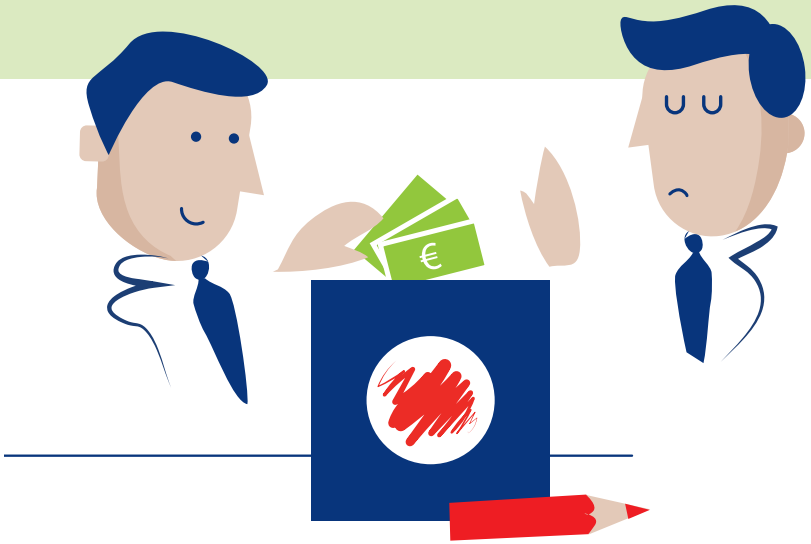
Vion competes for business fairly, on the merits of its products and services. Bribes in any form are unacceptable to Vion. Any personal payments or bribes to individuals employed by Vion's customers or suppliers, to government or regulatory officials, or receipts of bribes or personal payments by Vion employees are strictly prohibited. Even in jurisdictions where such activities might not be illegal, it is absolutely prohibited by Vion's policy. We believe in promoting good governance and the fair and impartial administration of law. It is also, therefore, strictly prohibited to give anything of value directly or indirectly to a government official in order to influence his or her judgement in the performance of official duties.

Vion strives to comply with the highest levels of transparency and accountability throughout the company. Records of transactions should be maintained in an accurate, complete and timely manner in accordance with the Vion accounting principles. No unrecorded funds or assets should be established or maintained.

13 CONTRIBUTIONS TO POLITICAL PARTIES AND INSIDER TRADING

Vion's basic policy is that Vion funds or resources may not be used to support any political candidate or political party anywhere in the world. Vion neither supports political parties nor contributes to the funds of groups whose activities performed are to promote party interests. Vion's policy does not permit the use of any Vion facilities or resources by employees for political campaigning, political fundraising or party political purposes.

Although Vion is not a listed company, either it or its subsidiaries may engage in or consider business transactions with publicly listed companies. Any employee who has knowledge of any business transaction or potential business transaction with a publicly listed company shall not engage in trading in any shares, options or other securities of that public company during the period when such a business transaction is not public knowledge.



14 EMPLOYEE RELATIONS

The Company is committed to equal opportunity and a respectful workplace. Employees shall not discriminate on the basis of race, religion, gender, national origin or any other legally prohibited status. Sexual harassment is not accepted.

15 ALCOHOL AND DRUGS

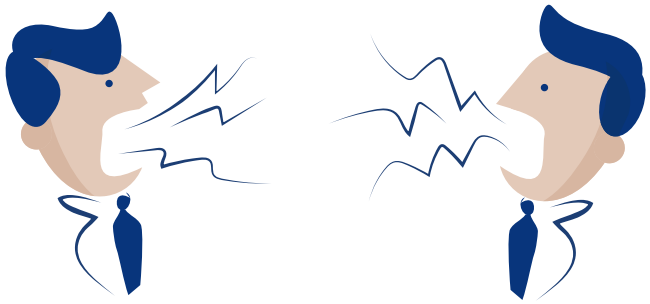
As a general rule, the consumption of alcohol and/or illegal drugs in Vion premises, offices or on the shop floor is not allowed. Likewise, employees shall not be admitted to and/or shall be removed from their office or from the shop floor when they are under influence of alcohol and/or drugs.

16 COMMUNICATIONS WITH THIRD PARTIES

Only authorised employees are permitted to speak to the media, shareholders, creditors, vendors and other third parties on behalf of the Company. Employees who are authorised to act or speak on behalf of the Company must adhere to the limits of their authority and may not take any action to exceed or circumvent these limits.

17 VIOLATIONS

Violations of the Code may result in disciplinary measures against the employee concerned. The Company reserves the right to deal with any such violation as the Company sees fit in the circumstances.



18 REPORTING INAPPROPRIATE, UNETHICAL OR ILLEGAL BEHAVIOUR

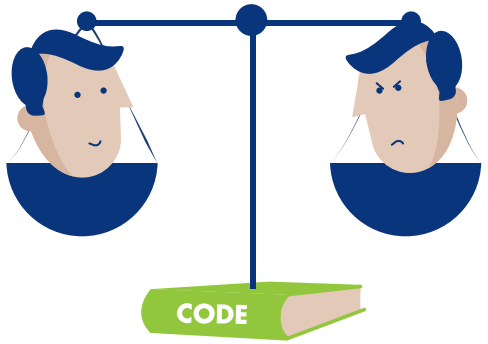
We strive to create a culture based on trust and individual responsibility. Employees may, however, encounter unethical or illegal behaviour within Vion. Vion wants to provide an environment in which its employees can express any concerns they may have about wrongdoing in the workplace. We are committed to providing a safe and fair way for such behaviour to be reported in good faith. It is the responsibility of each employee to report violations to their direct supervisor or a senior executive or, if necessary, to report it anonymously. Each Vion operating company has procedures which enable its employees to report inappropriate behaviour safely. Further procedures exist to facilitate the effective investigation of any claim so that, where necessary, corrective actions can be taken.

19 COMPLIANCE

Reporting on compliance with the principles of this Code is an integral part of the quarterly letters of representation issued by the local management, and as such they are embedded in Vion's internal control framework. The compliance processes and procedures are audited by Vion's internal audit department.

20 FURTHER GUIDANCE

This Code aims to address the principal areas of ethical behaviour that the Company expects from its employees. The Code cannot anticipate every legal or ethical issue that may arise and the Code may not be sufficiently specific on a certain subject. Should any employee have questions about the Code or wish for guidance in a certain situation, he or she should always consult his or her direct supervisor, who will address the matter as seriously as possible. Also, any employee may seek advice or guidance from the Legal or Human Resources Department of his or her operating company, or from the Director of the Legal and Tax Department or the Group HR Director at the Vion head office.



WHISTLEBLOWER POLICY

1 INTRODUCTION

Vion Holding N.V. (Vion, or the Company) is committed to ensuring that Vion and its Executive Committee, officers and employees act at all times in compliance with all applicable laws and regulations, the Vion Code of Conduct (the Code), the authority limits as laid down in the Vion Bill of Authorities and all other Company policies.

Vion's whistleblower policy (the Whistleblower Policy) aims to support compliance with the applicable laws, integrity in financial management, food safety and animal welfare, a healthy and safe work environment and effective corporate governance.

Vion conducts its business based on the principles of fairness, honesty, integrity and respect, and accordingly, wants to ensure that any employee of Vion can make a report under the Whistleblower Policy without the risk of retaliation and with the assurance that all reports are treated confidentially and are promptly investigated.

The Whistleblower Policy applies to all employees[1] of Vion and its operating companies anywhere in the world.

The Whistleblower Policy, which has been adopted by the Management Board, is reviewed on a regular basis and revised if necessary.

1 An employee in this policy means all individuals who carry out or have carried out work for Vion, including individuals who do not work or have not worked on the basis of an employment agreement.

2 WHAT TYPES OF MATTERS SHOULD BE REPORTED UNDER THIS POLICY?

An employee's report of suspected irregularities should be substantive, submitted in good faith and related to one of the following issues or matters of conduct:

1. Conduct that is corrupt, dishonest or fraudulent.
2. A (threat of) violation of the Code, authority limits or Company policies.
3. A (threat of) criminal activity or violation of any applicable law or regulation.
4. A (potential) danger to the public or the employees' health, safety and security, or to the environment.
5. Theft or fraud against Vion.
6. Purposeful misinformation or false statements to or by the Company management, to internal or external auditors or to public authorities.
7. Inappropriate accounting, financial reporting practices or internal controls.
8. Mismanagement or abuse of authority.
9. Conduct that is detrimental to the interests of Vion.
10. Intentional suppression, destruction or manipulation of information regarding the issues or conduct as described in points 1 through 9 above.

3 HOW CAN A MATTER BE REPORTED?

Under this Policy, employees can report suspected irregularities in the ways set out below.

3.1 Option one: INFORM YOUR MANAGER

Employees are encouraged to report matters in the first instance to their manager. Reporting concerns to management is the fastest and preferred way to address a work-related issue, to clear up any misunderstandings and to ensure a good and open work environment. If appropriate, your manager will involve Human Resources to assist in the investigation of a report received under this Policy.

3.2 Option two: INFORM HUMAN RESOURCES

The employee can also report a matter directly to the responsible Human Resources Department or the Confidential Advisor[1], particularly when:

1. you feel it is not an appropriate issue to discuss with your manager;
2. you do not feel comfortable discussing it with your manager; or
3. you have previously reported the matter and believe no action was taken.

3.3 Option three: INFORM THE COO/CEO/CFO/CHAIRMAN

If necessary, the employee is also free to report issues to the COO of a division, or to the CEO or the CFO or the Chairman of the Supervisory Board, all of whom are identified on
www.vionfood.com. Only alleged irregularities possibly involving members of the Management Board should be reported to the Chairman.

A report made using one of the three options above should explicitly state that it is a report made under the Whistleblower Policy. In this way, all individuals involved are made aware that the provisions of the Whistleblower Policy will apply.

1 The Confidential Advisor for the Whistleblower Policy is the Group HR director as identified on www.vionfood.com.

3.4 Option four: USE THE CONFIDENTIAL REPORTING LINE OR REPORTING WEBSITE

An employee also has the option of using Vion's external, independent confidential reporting line or confidential reporting website to report an issue or conduct concern in any instance, as is explained below.

The employee may report an issue or conduct concern under this Policy to Vion's external independent confidential reporting line or website, operated by People Intouch (see Appendix A for contact information of the People Intouch SpeakUp phone system and website). People Intouch employees are not in any way affiliated or associated with Vion. The People Intouch operators of the confidential reporting line are trained and experienced specialists dedicated to dealing with whistleblowers and their concerns. Calls may be made at any time, 24 hours a day. If you place a call to the confidential reporting line, you may leave a message in your native language. You may also leave a message (in your own language) on the confidential reporting website.

More information about the SpeakUp phone system and web service may be found in Appendix A.

4 FOLLOW-UP AFTER A REPORT

4.1 What happens once a report is made?

All reports received under this Policy will be the subject of an investigation with the objective of locating evidence that either substantiates or refutes the information provided by the whistleblower. All reports will be dealt with in a confidential manner. Confidentiality will be maintained to the fullest extent possible, consistent with the need to conduct an adequate investigation of the report and the privacy laws of the country(ies) involved. Additionally, an employee has the possibility to indicate that his report should be treated confidentially. The actions to be taken by the Company management upon the receipt of a report under this Whistleblower Policy are described in Appendix B.

As soon as reasonably possible, but at least within 8 weeks, the responsible manager within Vion will complete the investigation of the report and will notify the whistleblower (if the report was anonymous, then the notification will be delivered via the website / confidential reporting line.) If the investigation is not completed within 8 weeks, the whistleblower will be informed of the expected completion date.

You may also receive a request to provide further information. Any person against whom an allegation is made, if identified, will be informed of the report as soon as is practicable and will be given the opportunity to respond.
If a report is found to be false, the record will reflect such a finding and any misinformation will be noted. Vion is committed to implementing the findings and recommendations of any investigation with a view to rectifying any wrongdoing as far as this is practicable in the circumstances.

4.2 What happens if a report is anonymous?

Vion encourages its employees to report any issues or conduct under this Policy directly and openly. If no other option is feasible, the issue or conduct can be reported anonymously via the People Intouch confidential reporting line or website. Vion will investigate all anonymous reports; however, please realise that reporting anonymously via one of the options 1-3 outlined in Paragraph 3 above could hinder or complicate the investigations and possibly prevent an appropriate action from being taken, as it may be impossible to reach you for further information.

4.3 Will an employee be penalised for reporting a matter?

Any employee who reports a matter in good faith or participates in an investigation of a report (and is not found to have been involved in the issue or conduct reported) will not be penalised or personally disadvantaged due to this participation (e.g. by suffering harassment, discrimination, demotion or a dismissal.) An employee who believes that he or she has been penalised because of the employee's status as a whistleblower or due to participation in the investigation of a report, should immediately report the conduct through one of the methods identified in this Policy. Any employee or manager who is found to have dismissed, demoted, harassed, discriminated against, or in any other way retaliated against, a whistleblower or a participant in an investigation of a report by a whistleblower, due to their status as a whistleblower or a participant, will be subjected to disciplinary measures that may include dismissal.

4.4 What if the whistleblower intentionally makes a false report?

While not intending to discourage any employee from reporting matters of genuine concern, it is strongly suggested that the employee ensures, as far as possible, that a report is factually accurate, complete, from first-hand knowledge, presented in an unbiased fashion (with any possible perception of bias of the whistleblower disclosed), and without a material omission. Where it is established that an employee is not acting in good faith, or that the employee has intentionally made a false report, the employee may be subject to disciplinary measures that may include dismissal.

4.5 What should a manager do if a report is made to him/her?

The manager to whom a report is made directly under this Whistleblower Policy shall take the actions as described in Appendix B of this Whistleblower Policy.

WHAT YOU SHOULD KNOW ABOUT INFORMATION SECURITY, FRAUD AND CYBERCRIME

1 INTRODUCTION

In your daily activities you are faced with all sorts of risks, and handling those risks is a part of your normal work. Nonetheless, these risks increasingly include the loss of confidential or personal information through fraud and cybercrime. In this section, we would like to give you some guidelines about information security and the specific risks involved in various categories of fraud and cybercrime.

To maintain **information security,** the focus is on the proper treatment of confidential and personal information. **Fraud** is defined as an intentional, knowingly dishonest act that imposes a regulatory sanction on Vion, or that involves a breach of Vion's internal polices and standards that causes a financial loss to Vion. **Cybercrime** is any criminal or other offence that is facilitated by, or that involves, the use of electronic communications or information systems, including any device or the internet.

Some examples of fraud that you may encounter include the stealing of cash or assets, illegal agreements with competitors or intentionally false representations. Later in this section, we will give examples of the kinds of fraud and cybercrime that have materialised at Vion, to make the issue more concrete, including how the cases could have been detected and what we have learned from these experiences.

We will conclude the section with some guidance on how to recognise the red flags of fraud, and the key actions that can be performed to prevent fraud.

2 VION'S TEN COMMANDMENTS FOR CYBER AND INFORMATION SECURITY

1. Ensure effective access controls are in place.
2. Avoid opening unknown links and suspect emails or attachments.
3. Do not leave confidential documents and personal information in an area without supervision.
4. Be aware of the safety and security risks when surfing online.
5. Verify any suspect or unusual requests.
6. Respect everyone's privacy.
7. Immediately notify the IM&T Service Desk if a Vion device has been lost or stolen.
8. Use your common sense.
9. STOP and THINK before you act.
10. Notify the IM&T Service Desk of any suspicious activity (+31 88 99 53 911).

3 STOP AND THINK

Vion uses various types of security software in order to prevent as many problems as possible in relation to information security and cybercrime. Unfortunately, in spite of these technical tools, we cannot prevent every problem. You, as a Vion software user, are also a guardian of our digital gateway. You can take the first steps to prevent and block many attempts of fraud. How? It's simple: Stop and think! Do not immediately click on any links, or open emails and attachments without thinking. By unconsciously doing so, viruses may infect our systems or confidential and personal information may be disseminated.

By thinking first and being alert to suspicious situations, you can prevent the occurrence of many unwanted events. View this as a mental step which must be undertaken before your daily activities – and certainly in suspect or unknown situations. Doing so gives you the possibility to recognise risks and to consider the correct actions, for instance deleting suspect emails, or verifying them by informing the IM&T Service Desk. By making this a habit, we can arm ourselves against many forms of fraud.

4 EXAMPLES OF FRAUD

EXAMPLE 1 – CARTEL FORMATION AND ILLEGAL PRICE AGREEMENTS

Vion received a fine of € 3 million due to a cartel formation and illegal price agreements

Functions involved: Directors
Processes impacted: Sales and Receivables

Fraud type: Illegal price agreements, cartel formation

Scenario

- 21 meat manufacturers jointly held meetings at a hotel to discuss the market developments and agreed on illegal price settlements
- Representatives of one of Vion's entities joined at least one of these meetings, which led to the accusation of Vion's involvement in the cartel

Detection

An anonymous tip about a cartel formation was provided to the German Anti-Cartel Authority, and the cooperation with the authorities by several repentant manufacturers initially involved in the cartel led to an investigation by the German Anti-Cartel Authority.

Red Flags

- Changes in the competitive relations
- Product margin increases
- Anonymous tip

LESSONS LEARNED

Corrective measures to be undertaken:

- A policy has been set up that states how to deal with our competitors and any potential illegal agreements regarding price and market settlements

EXAMPLE 2 – THEFT OF MONEY

More than € 40K in cash was stolen from the Vion premises

Functions involved: Financial Staff, Meat Shop Personnel
Processes impacted: Cash and Banking

Fraud type: Theft

Scenario

- Large amounts of cash were available in the Vion premises as a result of revenue from the meat shops.
- These amounts of cash were not properly safeguarded, and there were no other proper security measures implemented over the weekend.
- Cash was stolen via burglaries during the weekend.

Detection

The burglary was discovered after the opening of the premises on the first working day after the theft (Monday).

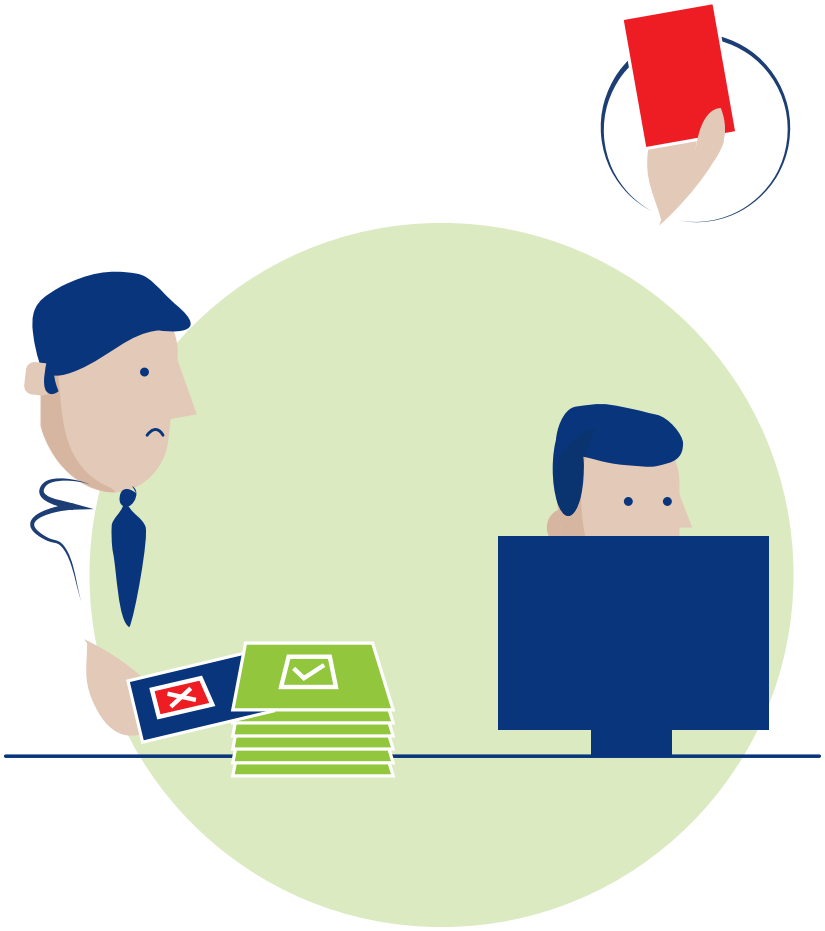
Red Flags

- Amounts of cash were left available in the premises over the weekend, which is not in line with the Vion Cash Policy
- No safes were available, or there was an insufficient number of safes to store the cash
- There was a lack of other proper security measures to prevent burglaries

LESSONS LEARNED

Corrective measures implemented:

- The Vion Cash Policy obliges limited amounts of cash to be available
- Proper safes are provided for cash storage



EXAMPLE 3 – FALSE INVOICES

An employee attempted to steal money by presenting a false invoice.

Functions involved: Finance Staff
Processes impacted: Purchasing and Creditors

Fraud type: Misappropriation

Scenario

- A former employee of the Finance Staff had access to the SAP Vendor Master Data.
- The employee was also responsible for recording the vendor invoices and payments.
- Falsified invoices were created in the name of an existing vendor in the SAP Vendor Master Data.
- No internal control procedures were in place to discover the falsified payments.

Detection

During a regular tax audit at the end of the year, it was discovered that one of the falsified invoices contained a questionable VAT rate, which led to further internal investigations.

Red Flags

- Uncontrolled access to the SAP Vendor Master Data
- There was no segregation of duties in place for the various financial functions
- Lack of internal control procedures during the payment process

LESSONS LEARNED

Corrective measures implemented:

- The responsible person was fired
- Segregation of duties was implemented regarding the various financial functions

5 EXAMPLES OF CYBERCRIME

EXAMPLE 1 – PHISHING EMAILS

Stealing of digital credentials for future fraudulent activities

Functions involved: All employees
Processes impacted: All business functions

Cybersecurity type: Receipt of phishing emails

Scenario

- Phishing emails are received which are suspected to come from one of the national telecommunication providers within the Netherlands.
- Employees receive an invoice via email that includes a link inviting them to login on their personal page to view the invoice details.
- When this is done, the username and passwords of the employee are copied and used for identity theft and fraudulent activities.

Detection

Personal vigilance is required, along with the knowledge that it is suspicious to suddenly receive personal email through the corporate mail account.

Red Flags

- Receipt of unusual personal email through the corporate account
- The mail addresses from the sender contained deviant domain names

LESSONS LEARNED

Corrective measures to be undertaken:

- All employees actively receive communication about the cybercrime risks when such campaigns are active on the internet

EXAMPLE 2 – RANSOMWARE ATTACKS

Unavailability and loss of data stored on a local hard disk or a shared network due to encryption

Functions involved: Financial Staff
Processes impacted: Financial Administration

Cybersecurity type: Infection with crypto-ransomware

Scenario

- A virus-infected attachment is received in an email from an illegitimate source, which goes undetected by the anti-virus software.
- On opening of the attachment, the virus encrypts parts of the documents leaving them inaccessible.

Detection

After the infection, the computer system was blocked and documents could no longer be opened. A pop-up screen showed that the computer had been taken hostage and stated that money needed to be paid in order to release the documents.

Red Flags

- The mail address from the sender contained deviant domain names
- Unusual emails with attachments were received

LESSONS LEARNED

Corrective measures to be undertaken:

- All employees receive active communication about the cybercrime risks when such campaigns are active on the internet
- Continuous updates of the anti-virus software

6 RECOGNITION OF THE RED FLAGS FOR FRAUD

To recognise the red flags for fraud, be attentive when an employee:

- While currently in a "sensitive" position, refuses to be promoted to a new job for unclear reasons
- Changes, without explanation, to a lifestyle that is obviously above his/her wage revenue
- Systematically refuses to take holidays, stays late and works during weekends without a real business need
- Is in a situation with a conflict of interest
- Resigns unexpectedly

Also be cautious regarding the following events:

- Unexplained inventory shortages or adjustments
- Increased amounts of scrap/wastage
- Excess amounts of purchases
- Too many credit memos
- Significant increases or decreases in the account balances
- Cash shortages
- Unreasonable expenses or reimbursements

7 KEY ACTIONS TO PREVENT FRAUD

The three key elements of fraud prevention within Vion are:

- A strong culture that promotes ethical behaviour and transparency
- Strong internal controls
- An effective anti-fraud programme that is based on an updated fraud risk assessment

The following ten key actions can help with the prevention of fraud within Vion:

1. Ensure that the behaviour of the senior management is exemplary, as the "tone at the top" influences the behaviour of employees
2. Train the employees to understand what is acceptable and what is not
3. Promote the commitment of managers to adhering to Vion's core values and Code of Conduct
4. Make sure that all employees are aware of Vion's Whistleblower Policy
5. Ensure that the appropriate procedures and processes are formalised, communicated to all relevant employees, and applied within the workplace
6. Train key personnel on the objectives, benefits and components of the internal controls
7. Ensure that an appropriate segregation of duties is efficiently applied (with no access to incompatible activities)
8. Ensure job rotations for sensitive positions (procurements, cash management, inventory management, IT, sales, etc.)
9. Make sure that compensation is based on performance, so that it will not lead to fraudulent behaviour
10. Investigate each credible fraud allegation, take corrective measures and initiate internal communicates regarding sanctions

8 DO'S & DON'TS WHEN DEALING WITH FRAUD

The DO's

- Analyse each fraud allegation to assess its credibility and its impact on your company
- Seek advice from the Legal Department, or from any contact listed on the last page of this booklet, to learn what may or may not be done, especially regarding compliance with the local regulations
- In any case, involve your hierarchy – for significant cases, involve the Internal Audit Director or the Company Secretary
- Make sure that all possible proof is conserved (paper and electronic documents, emails, videos…)
- Proceed with an adequate investigation in compliance with the local laws, and document each part of the investigation
- Implement appropriate corrective measures
- Decide, in accordance with your hierarchy, on the sanction(s) for significant fraud – internal disclosures of the sanctions may also be used to deter other potential fraudsters

The DON'Ts

- Do not ignore any fraud allegation
- Do not hide fraud allegations and cases that should be discussed with your hierarchy or disclosed to the group members
- Do not disclose the source of the fraud allegation, in order to prevent the informant from experiencing undue retaliation or a hasty dismissal
- Do not talk about the fraud allegation to the person(s) suspected of fraud before collecting proof of his/her/their guilt or innocence
- Do not dismiss or sanction the suspected person(s) before collecting the necessary proof of his/her/their guilt
- In significant cases, do not take any action (especially legal actions or the filing of a complaint) before receiving advice from the Legal Department

APPENDIX A

The SpeakUp phone system and web service reporting channels

CONFIDENTIAL REPORTING BY TELEPHONE

- **Telephone –** employees can call a country-specific Freephone number and record a voice message in their preferred language which InTouch then transcribes and translates
- **Web service –** employees can log on to www.intouchfeedback.com/vion and leave a report in their preferred language

Telephone – the Freephone number and access code is specific to each country

Country	Languages	Freephone	Access Code
Bulgaria	English, Bulgarian	00800 115 4437	84684
China	English, Mandarin, Cantonese	10800 440 0163	84664
Denmark	English, Danish	80 88 5812	84683
France	English, French	0800 918215	84666
Germany	English, German, Polish, Romanian, Turkish	0800 180 0094	84667
Greece	English, Greek	00800 441 45224	84668
Hungary	English, Hungarian	06 800 17858	84669
Italy	English, Italian	800 920034	84670
Netherlands	English, Dutch, Polish, German, Turkish	0800 024 9798	84660
Poland	English, Polish	00800 441 1617	84674
Portugal	English, Portuguese	00800 10005647	84675
Romania	English, Romanian	0800 894784	84676
Russia	English, Russian	810 800 2258 1044	84677
Slovenia	English, Slovenian	0800 80278	84678
Spain	English, Spanish	900 811498	84679
Sweden	English, Swedish	0207 96145	84680
Switzerland	English, French, German	0800 56 1580	84685
Ukraine	English, Ukrainian	0800 503 577	84681

CONFIDENTIAL REPORTING BY TELEPHONE

Web – log on to www.intouchfeedback.com/vion

Country/Site	Languages	Access Code
Bulgaria	English, French, German, Italian, Dutch, Swedish, Danish, Spanish, Slovenian, Czech, Hungarian, Bulgarian, Latvian, Lithuanian, Polish, Portuguese, Romanian, Slovakian, Welsh, Malay, Ukrainian, Russian, Turkish, Greek, Japanese, Chinese and Arabic	84684
China		84664
Denmark		84683
France		84666
Germany		84667
Greece		84668
Hungary		84669
Italy		84670
Netherlands		84660
Poland		84674
Portugal		84675
Romania		84676
Russia		84677
Slovenia		84678
Spain		84679
Sweden		84680
Switzerland		84685
Ukraine		84681

APPENDIX B

Whistleblower Policy – steps following a whistleblower report		Steps to be taken following a whistleblower report
Via the employee's **own manager**	Preferred route	**The Manager / HR Manager who receives a report shall:** **1** report to his line manager (or his line manager's superior if appropriate) **2** discuss the report with the Confidential Advisor **The Confidential Advisor shall:** **3** inform the Vion CEO and Company Secretary and discuss and decide with them on the next steps **4** communicate the next steps to the Manager/HR Manager **The person who is to take the next steps shall:** **5** discuss the report with the employee who submitted it; obtain more information if necessary; make a written record of this conversation **6** inform the person against whom an allegation is made (if identified) of the report, if this information does not constrain the investigation and any disadvantages for the employee reporting in good faith are not to be expected **7** start the investigation **8** report the findings to the Confidential Advisor **The Confidential Advisor shall:** **9** report the findings to the CEO and Company Secretary **10** discuss and decide on any measures to be taken to address the irregularities confirmed in the investigation, if any, and who will communicate/ implement them
Via **HR** OR the **Confidential Advisor**	• if not appropriate / uncomfortable to discuss with the employee's own manager • if previously reported to the employee's own manager but no action was taken	
Via **COO of the Division or the CFO / CEO or Chairman** of the Supervisory Board	"This route is always possible" **NB** The Chairman may be contacted via the Company Secretary. **NB** Reports concerning members of the Management Board should always be submitted to the Chairman	The Company Secretary who receives a report for the Chairman shall immediately and confidentially inform the Chairman. **The COO/CEO/CFO or Chairman shall:** **1** if appropriate, ask the Confidential Advisor to conduct and investigate the allegations, take Steps 1-7 as described above, and then report back **2** the Confidential Adviser (or the Company Secretary as the case may be) shall report the findings to the COO/CEO/CFO or to the Chairman **3** the COO/CEO/CFO or the Chairman will discuss and decide on any measures to be taken to address the irregularities confirmed in the investigation, if any, and who will communicate / implement them **4** these measure will include reporting back to the employee who submitted the report about the completion of the investigation or of the expected completion date, which shall be done in any case within 8 weeks after the report was made
Via **InTouch** (telephone or website) See Appendix A	Notably, if the person who makes the report wants to do so anonymously.	**InTouch:** **1** The person who wants to submit a report leaves a spoken message via the confidential telephone line, or a written message via the confidential reporting website **2** InTouch will translate the message (if necessary) and will send it as soon as possible to the Confidential Advisor **3** The Confidential Advisor will the take Steps 1, 3, 4, 6, 7, 9 and 10 as described above; if he requires more information from the employee who has submitted a report he will leave a message via InTouch; this message will be given to the employee when he next dials in or logs in to the InTouch confidential reporting line or website

REFERENCES

For further references, see the Vion Policy House for the following:

- Code of Conduct
- Whistleblower Policy
- Competition Policy
- Corporate Social Responsibility Reports
- Other policies, forms and procedures

The Policy House is a repository of the current and authorised charters, policies and manuals in place within Vion. The scope of these documents is aimed at compliance to Vion's external and internal rules. The address is: http://qol.vionfood.local/. The user name is the same as the domain username.

The Good Business Practice Guide can also be found on VIONline and on Vion's website: www.vionfood.com