



CODE OF BUSINESS CONDUCT



A message from our CEO	3	Our Commitment to Our Group	19
Our Purpose Statement & Values	5	Protecting Group Assets and Information	19
Our Purpose Statement	5	Intellectual property	19
Our Values	5	Confidential information	19
The purpose of the BME Group Code of Business Conduct	6	External communications	20
Am I doing the right thing?	6	IT & Data Security and Digital Media	20
Our Business Principles	8	Appropriate use of company technology	20
Introduction to the BME Code of Business Conduct	9	Data protection, retention, and data privacy	21
What is the Code of Business Conduct and why do we have one?	9	Accounting and other business records	21
Who is the Code of Business Conduct for?	9	Digital (or social) media	21
What are your responsibilities?	9	Conflicts of Interest	23
The importance of speaking up!	10	Fraud and Theft	23
Why is it important to ask questions and report concerns?	10	Fraud	24
What kind of issues should I report?	10	Theft	25
When I want to speak up, whom should I contact?	10	Reporting	26
Good faith reporting and non-retaliation policy	11	Gifts and Entertainment	26
What happens in case of a violation of the Code or law?	11	Our Commitment to the Environment and Our Communities	28
Monitoring, Assurance and Reporting	11	Environmental Sustainability	28
Our Commitment to Each Other	12	Political Contributions	28
Workplace Safety and Health	12	Charitable and Community Activities	29
Fair Social and Employment Policies	12	APPENDIX I – Relevant Contact Details	30
Equal Opportunities and Non-discrimination	13	APPENDIX II – Procedures aimed at Preventing Bribery	31
Prevent Bullying and Harassment	13	APPENDIX III – Fraud and Theft Reporting Procedures	32
Our Commitment to Our Customers, Suppliers, and Business Partners	14	APPENDIX IV – Checklist for Reporting actual, suspected or attempted Fraud and/or Theft	34
Treating Others Fairly	14	Our Operational Businesses	35
Our customers	14		
Our suppliers	14		
Our business partners	14		
Competing Fairly	16		
Refusing Bribery and Corruption	16		
Bribes and Facilitation Payments	16		
Money laundering	18		
Doing Business with Governments and Regulatory Officials	18		

A MESSAGE FROM OUR CEO



Dear colleague,

We have a clear and focused strategy to drive excellence across our businesses. We do this by putting our customer at the center of everything we do, though keeping our suppliers and our employees also on top of mind. This triangle is core to any distribution business and as such, we have defined hard and specific “promises” to each of these stakeholder groups within the triangle.

While doing our work, we are all confronted with obstacles, difficult choices, and dilemmas. In such moments, our Code of Business Conduct serves as our guide.

The key priority for us is to serve our customers in the best possible way and to succeed in the market. In that sense, we are a ‘commercially driven’ organization. We enable our people to succeed and we act with speed and decisiveness throughout the organization to make it happen.

To be successful as a company in the long run, we understand that our stakeholders need to have confidence in us. We intend to merit this trust, which we have earned over many

decades, by doing business in accordance with the values underpinning BME’s Code of Business Conduct (the Code).

While doing our work, we are all confronted with obstacles, difficult choices, and dilemmas. In such moments, our Code serves as our guide for good business conduct. Having a documented Code is important. However, our responsibility goes beyond paperwork and fulfilling legal requirements. The Code demonstrates to our customers, suppliers, and employees that they can rely on BME Group and its affiliated companies for full legal compliance and uncompromised business ethics. As employees, we all have a duty to uphold the Code, company policies and the law by performing our jobs in an open and honest manner.

Please familiarize yourself with our Code of Business Conduct. Join me in making the commitment to uphold it in all we do as BME Group employees. Our Code helps you to make the right decisions daily. The values in the Code relate to behaving with **care**, with **respect, integrity, honesty** and in a **straightforward** and **authentic** way. To emphasize the importance of our values, the Code sets out how BME commits to adhere to the behaviors by describing:

- Our Commitment to Each Other,
- Our Commitment to Our Customers, Suppliers, and Business Partners,
- Our Commitment to Our Group, and
- Our Commitment to the Environment and Our Communities.

Together we build!

The culture of our company is simply the sum of the behaviors of all of us. The success and reputation of our company depends on our behavior and our good business conduct, every single day.

If you have any questions about our Code of Business Conduct, please raise them. If you have concerns about potential misconduct, please speak up and talk to your immediate supervisor within your local company.

Thank you for taking our values and commitments as seriously as I do. When we do what is right, act with integrity and build trust, we make our company stronger. This is critical for our success.

Remco Teulings
Group CEO
BME Group



OUR PURPOSE STATEMENT & VALUES

Our Purpose Statement

Together, we deliver the best experience for our customers, our suppliers, and our people. We build leading distribution businesses, ultimately driving shareholder value.

colleagues, our suppliers, our competitors and our shareholders. Our values are not just written words. We expect our values to be expressed in our daily work. We expect that our values will guide us and help us in achieving our goals and realizing our ambitions.

Our Values

Values define who we are as individuals and as a company. Our values define who we are for our customers, our



Dare.

Consciously challenge the way things are. Approach work with an open mind. Actively look for (business) opportunities and take calculated risks. Drive change with a positive approach.



Care.

Respect and take care of people. Notice and act on signals given by colleagues, the organization, our communities and the environment. Build lasting relationships and keep each other safe.



Do it.

Drive towards top performance with integrity. Act now, push yourself to beat goals and overachieve. Look beyond the obvious. Love what you do and show engagement.



Be real.

Do what you commit to do. Be honest and forthright. Take your fair share of the workload. Take responsibility for your own mistakes. Maintain a reputation of authenticity, fairness and reliability.



Win together.

Engage with others to create partnerships. Do not 'give in' but compromise appropriately for results. Trust and build on each other's talents. Embrace diversity and champion inclusive communication.

THE PURPOSE OF THE BME GROUP CODE OF BUSINESS CONDUCT

The purpose of this Code of Business Conduct is to guide us all in maintaining our ethical standards based on which we conduct our day-to-day business. It provides information about our standards of integrity and explains some of our legal and ethical responsibilities.

Our Code of Business Conduct is really ours. That means that **all** employees, managers, members of our executive team and board of directors are held to this Code. We also expect our suppliers, business partners and other external parties working with BME and its affiliates to uphold similar ethical standards in working with us.

The purpose of this Code of Business Conduct is to guide us all in maintaining our ethical standards based on which we conduct our day-to-day business.

Even though we address many legal and ethical concerns in this Code, it is not possible to cover every situation that might occur. Therefore, when in doubt as to whether actions or behavior is appropriate, talk to your immediate supervisor.

In addition to our Code you should always keep our values in mind. Make sure that your decisions support these values in everything you do. It would be easy if 'the right thing to



do' would always be crystal clear. It is not. Life is not always easy. If the right thing to do is not obvious, remember our values and let those guide you in making the right decisions.

Am I doing the right thing?

In a challenging global environment, our values are designed to enable us to act and be perceived as responsible entrepreneurs. They serve as a basis for you

and your colleagues to perform your work in a sustainable and trustworthy manner. The Code is an essential foundation for the development and success of our

company and promotes correct and appropriate behavior in many business situations.

When you are not sure how to act in a certain situation please ask yourself the following questions:

- Does my behavior or action reflect BME's core values?
- How would I feel if this behavior or action were directed at me?
- If my action would become a headline in the news, would it make me proud or ashamed?
- Does my behavior or action harm my colleagues, my customers and/or my company?

If the answer to one or more of the above questions makes you feel uncomfortable, it is safe to assume it is not the behavior or action we stimulate within our company.

OUR BUSINESS PRINCIPLES

As said before, the purpose of this Code of Business Conduct is to guide us all in maintaining our ethical standards based on which we conduct our day-to-day business. It provides information about our standards of integrity and explains some of our legal and ethical responsibilities.

Our Code of Business Conduct covers several key areas and guiding business principles, which both determine our behavior. Read the following 10 principles carefully:

1. We **take care of each other** to ensure the health and safety of our people and our guests everywhere we work.
2. We **respect human and labour rights** and we provide equal, merit-based opportunities to all our employees. We value their diversity and reward them fairly.
3. We are **fair and honest** with our customers, suppliers and business partners and we only engage with those who share our commitment to ethical business practices.
4. We are especially mindful of our **responsibility** in competition law and compete energetically, fairly and always within the law.
5. We **do not tolerate any form of bribery or corruption** and are committed to the highest standards of business ethics in all our dealings everywhere.
6. We **use** our Group's **assets in a proper manner** and for their designated purpose.
7. We respect confidential information and are **professional** in all our communications.
8. We **avoid conflicts of interest** and we are alert to promptly report any suspected incidents of fraud. We only offer and accept appropriate business gifts and entertainment.
9. We **embrace sustainability** as a fundamental criterium to our future growth. We continuously strive to meet the highest standards of environmental management and we are fully committed to enhancing the lives of the communities which we serve.
10. Finally, if we see or hear something illegal, unethical, or unsafe – we **“Speak Up”!**

These principles are crucial to our success. We think it is necessary to underline their importance and our group's engagement to these principles. Therefore, we have structured this Code as a set of **“Commitments”** to pursue adherence with our guiding business principles:

- Our Commitment to Each Other,
- Our Commitment to Our Customers, Suppliers, and Business Partners,
- Our Commitment to Our Group, and
- Our Commitment to the Environment and Our Communities.

INTRODUCTION TO THE BME CODE OF BUSINESS CONDUCT

What is the Code of Business Conduct and why do we have one?

Our employees differentiate themselves by high ethical standards in their relationships with customers, suppliers, contractual partners, competitors, authorities, colleagues, and investors.

The Code of Business Conduct is for everyone who works for or on behalf of a BME Group company.

Our Code sets out the ethical standards that we must adhere to be successful. The Code acts as a guide to help us to live up to our values, respect the law and make ethical decisions.

Throughout this document reference is made to detailed policy documents and guidance notes in relation to:

- Competition/Anti-trust Compliance Code,
- IT Security Policy,
- Health and Safety Guidelines, and
- Supplier Code of Conduct.

Copies of these documents can be obtained from your local HR Officer.

Who is the Code of Business Conduct for?

The Code is for everyone who works for or on behalf of a BME Group company. This includes all employees of a BME Group company, including those who work part-time or are on fixed or temporary contracts, as well as all officers, executive and non-executive directors. All mentioned must read, understand, and comply with this Code. When in this Code reference is made to BME, or the BME Group, this also includes all group companies of BME.

Additionally, we also expect our suppliers to follow similar principles, as outlined in our separate Supplier Code of Conduct. Business partners who act on our behalf are also expected to share our commitment to the highest ethical standards.

What are your responsibilities?

We expect you and all employees to:

- **comply** with the Code and all applicable laws,
- **use** your common sense and good judgement in making business decisions and interactions,
- **ask** when in any doubt about how to proceed, and
- **speak-up** when things are not right.

THE IMPORTANCE OF SPEAKING UP!

Why is it important to ask questions and report concerns?

We are all aware of the devastating impact that unethical, illegal, or unsafe behavior can have on a company and its employees. We want to continue to safeguard our excellent record and reputation and need your ongoing support to realize this.

Since our Code cannot address every situation that could arise in our day-to-day business, it is up to each of us to continue to uphold the highest standards of integrity and to report matters inconsistent with responsible business conduct as provided for in the Code.



What kind of issues should I report?

You should report in good faith all potentially illegal, unethical, or unsafe acts or anything that seems contrary to the principles set out in our Code. “Good faith” means that you provide all the information you have about the situation and that it is true to the best of your knowledge.

It does not matter if you are not sure whether the issue is a violation of our Code or if it later turns out that you were mistaken. You should always feel free to ask questions

about anything that seems inappropriate to you or report something if it does not seem right – this is both your right and your responsibility.

When I want to speak up, whom should I contact?

There are several resources you can turn to any time you are unsure about the right course of action or wish to report an issue that concerns you:

- Your immediate manager,
- The Managing Director, the Finance Director or the HR Director of your Operating Company,
- The Group General Counsel or the Group Head of Internal Audit, and
- The BME Speak-Up Hotline.

(see appendix I for the relevant contact details)

Where local laws allow, you may report anonymously, though please keep in mind that this can make it more difficult for BME to properly investigate your report. For anonymous reports you can use the BME Speak-Up Hotline. This hotline is a tool that is managed by an external party and offers the possibility to report an issue and keep track of the developments in a subsequent investigation.

Speak up! In case of:

- Illegal acts and behavior
- Unethical acts and behavior
- Unsafe acts and behavior
- Anything that seems contrary to the principles set out in the Code

This is both your right and your responsibility!

Good faith reporting and non-retaliation policy

BME is committed to creating an atmosphere of non-retaliation. An atmosphere where all employees feel empowered to speak up when they have genuine concerns. You may always make a good faith report of any suspected violation of our Code or the law. Such a report can be made without fear of retribution or any negative impact on your employment because of the report. Retaliation or reprisals are never tolerated.

When a report is made, the information is forwarded to the Group General Counsel and the Group Head of Internal Audit for investigation. Every concern or allegation will be handled discreetly and professionally and in a confidential manner, to the extent reasonably possible and allowed by local laws.

Remember, violation of the Code of Business Conduct and/or the law places all of us at risk of a damaged reputation and negatively impacts our stakeholders. It may also subject us, as individuals and as a Group, to fines and civil or criminal liability.

What happens in case of a violation of the Code or law?

Violations of our Code or the law may carry serious consequences for the individuals involved and for BME. Those engaging in unethical or illegal activities and those who direct, condone, approve, or facilitate such conduct, are acting independently and against the Group's best interests. They therefore will be subject to disciplinary actions up to and including termination of employment without notice, as well as possible legal sanctions.

Monitoring, Assurance and Reporting

The Management Board of each Operating Company must annually review the operational status of the Code. The Managing Director should complete a compliance report annually to the Group General Counsel. This compliance report must contain a certificate and questionnaire which the Group General Counsel will make available each year.

The compliance report must be presented in a format to be prescribed annually at the start of the certification process. The Group General Counsel and the Group Head of Internal Audit will prepare a report for the Audit Committee on the overall operation of the Code.

OUR COMMITMENT TO EACH OTHER

Workplace Safety and Health

Our primary responsibility is to protect the safety of people who come to work or visit our many locations.

Providing a place where everyone feels safe and healthy and everybody goes home safe again at the end of each working day.

Our Safety & Health Policy requires us to:

- **comply**, as a minimum, with all applicable Safety & Health legislation. Continuously improving our Safety & Health stewardship, aiming all the time to meet or exceed industry best practice,
- **insist** that all employees and contractors respect our safety guidelines,
- **ensure** that our companies provide a safe and healthy workplace for all employees and contractors and take due care of customers and visitors at our locations, and
- **require** all employees and contractors to work in a safe and healthy manner as mandated.

Fair Social and Employment Policies

We are fully committed to human rights and support the principles set out in the articles of the 'United Nation's Universal Declaration of Human Rights' and the 'International Labour Organisation's Core Labour Principles' in so far as they apply to our companies.

Our position is that in our dealings with employees, contractors, customers and suppliers and in making investment decisions we are required to:

- **comply**, as a minimum, with all applicable legislation, continuously improving our social stewardship, aiming all the time to meet or exceed industry best practice,
- **manage** our businesses in a fair and just manner, meeting all our social responsibilities as both a direct and indirect employer,
- **support** freedom of association and recognize the right to collective bargaining,
- **prohibit** forced, compulsory and child labour,
- **apply** the principle of equal opportunity. Valuing diversity regardless of age, gender, disability, religious belief, ethnic origin or sexual orientation, while insisting that merit is the ultimate basis for recruitment and selection decisions, and
- **ensure** that we deal responsibly with our suppliers and customers in accordance with this Code and proper business practice.

We are fully committed to respect all human rights.

Equal Opportunities and Non-discrimination

Our employment policies are aimed at fostering individual initiative and collaboration, providing all of us with the opportunity to develop to our full potential.

Hard work, ability, and integrity are the principles that determine a person's opportunities for advancement in our Group.

Recruitment, selection and promotion decisions are made on individual merit and in line with the principles of equal opportunity and non-discrimination, as well as recruiting fairly and providing merit-based development opportunities. We also reward our people fairly, based on a "pay for performance" philosophy.

Prevent Bullying and Harassment

Bullying and harassment is totally inappropriate in the workplace and comes in many forms, including:

- verbal or written remarks or "jokes" related to religion, race, ethnicity, gender or age,
- physical or sexual advances or visual displays,
- threatening gestures or expressions of violence, and
- threats of violence.

Such behavior may come from co-workers, supervisors, suppliers, contractors, or customers. We all have the responsibility to ensure that there is mutual respect in the workplace. Bullying or harassment will never be tolerated.



It is important to treat our fellow employees with respect and dignity. Bullying or harassment will never be tolerated.

Our Commitment to Each Other:

- Safe working conditions
- Fair labour practices
- Equal opportunities
- No discrimination
- No bullying
- No harassment

OUR COMMITMENT TO OUR CUSTOMERS, SUPPLIERS, AND BUSINESS PARTNERS

Treating Others Fairly

Our customers, suppliers and business partners are very valued stakeholders. They contribute in so many ways to our Group's success. In return, we strive to be honest, and never engage in unfair practices. We firmly believe that relationships built on trust and integrity will be sustainable and beneficial for all.

We firmly believe that relationships built on trust and integrity will be sustainable and beneficial for all.

Our customers

The success of our business strategies relies on the support of our customers. It is therefore essential that we develop and maintain mutually positive and beneficial commercial partnerships based on fairness, honesty, and trust.

We are committed to supplying all our goods and services in accordance with all applicable laws relating to health, safety, and product requirements. Likewise, our product promotion and advertising should always be factual and presented in a way that is fair and reasonable. This means we never engage in misstatements about our products and services or those offered by our competitors.

Our suppliers

Our suppliers are critical to the performance of our business. We expect them to be quality driven, innovative, and efficient, providing BME with value at a fair cost, but never at the expense of ignoring laws, regulations, or sound ethical practices.

Our Supplier Code of Conduct sets out our requirements and related procedures that help ensure that we only work with suppliers who share our unwavering commitment to good ethical practices and meet our standards in respect of human rights, health and safety and environmental stewardship.

Our Procurement teams have oversight of risk-based processes for our principal direct and indirect suppliers and assist management teams to ensure local supplier relationships are appropriately managed.

Our business partners

It is normal business practice to engage the services of "Business partners". Business partners may include sales agents, consultants, advisors, intermediaries, sales distributors, lobbyists, and joint venture partners. Our business partners contribute to our business processes. They support us when we need their expertise in each subject area, market or geographic location. We carefully select business partners that operate on our behalf to assist in securing, preparing or negotiating bids for new contracts or the extension of existing contracts.

However, in order to protect the Company from any association with illegal or corrupt payments or the risk of such payments being made on our behalf, it is BME policy that the employees engaging business partners, must assess the perceived level of risk associated with that partner. This includes their location, reputation and behavior. Particular care must be exercised in engaging a business partner for use in any interactions on the Company's behalf with foreign government officials. In case of any doubt in relation to the reputation and behavior of the business partner, the relevant employee must consult with their manager, their local legal or Group General Counsel.

We also carefully document all contractual commitments to ensure that they reflect ethical business standards. BME does not tolerate any form of bribery. All employees and all those acting on BME's behalf are strictly prohibited from offering, paying, soliciting or accepting bribes. In order to prevent bribery BME has set the following standards:

- regular assessment of internal and external bribery risks,
- implementation of risk-based procedures preventing bribery, and
- compliance with anti-bribery and corruption laws.

(see appendix II for the procedures aimed at preventing bribery)

As with all of our third parties, compensation paid to these business partners must be proportionate to the services provided, properly recorded and approved and paid by cheque or bank transfer (not cash) in accordance with any agreed contract.

The following non-exhaustive list of red flags should be considered during the assessment of each business partner. The existence of one or more issues is a potential indication that the business partner is higher risk. Post-transaction, these red flags may also be considered as notice of possible bribery risks and be cause for investigation and appropriate remedial action.

Red Flags

- difficult to determine or complicated ownership structure where it is difficult to ascertain the controlling parties or the owners are based in high corruption risk locations,
- past or on-going investigations, charges and/or convictions for a regulatory offence,
- reputation for unethical conduct,
- inability to provide references (financial or business) or evidence prior experience,
- business partner has a close personal or family relationship to a government official, who would be in a position to influence decisions involving BME's business,
- business partner has a close personal or family relationship with an employee of BME,
- false or misleading documentation,
- abnormal commissions or price discounts,
- unusual payment requests, such as large up-front payments, payments to third parties, or midstream requests for additional compensation,
- press reports of improprieties,
- odd payments or unexplained accounts in financial records, and
- evidence of disproportionate or inappropriate corporate hospitality, gifts or expenses.

Business partner compliance must be kept under review and any breaches of contractual obligations or unlawful conduct must be reported.



Competing Fairly

BME aims to compete and excel in competitive markets. We are therefore fully committed to complying with competition/antitrust laws wherever we operate. Our Competition/Anti-Trust Compliance Code sets out how we do this in our day-to-day practice.

We believe that fair competition is in everyone's interest resulting in more dynamic markets with wider choice, better value and increased innovation.

Specifically, we cannot engage in any form of communication or establish an implicit or explicit agreement with a competitor which has the effect or attempts to:

- **fix, stabilize or control** prices, credit terms, discounts or rebates,
- **allocate** contracts, markets, customers or territories,
- **boycott** certain customers or suppliers, and
- **refrain** from or limit the manufacture or sale of any product or service.

It is particularly important that you familiarize yourself with our "Dawn Raids" Procedures, included in the Competition/Anti-Trust Compliance Policy so you know how to react appropriately in the event of an investigation by the Competition/Anti-Trust authorities or any other enforcement agency.

Violation of our Competition/Anti-Trust Compliance Policy poses a risk of serious civil, criminal, financial and other penalties being levied on the Group. Accordingly, it is essential that we fully understand our responsibilities in this area. Depending on your role, you may be required to undertake specific competition law training to ensure you understand how to apply our policies and procedures in practice, in addition to training on our Code of Business Conduct.

Refusing Bribery and Corruption

At BME, we do not tolerate any form of bribery and corruption. Some further guidance in relation to bribery and corruption is set out below.

Bribes and Facilitation Payments

A bribe is any financial or other advantage offered, promised, given or received with the intention of influencing the behavior of a person, company or public body. This intention, or purpose, is very critical as certain legitimate business transactions may constitute bribes if specifically undertaken to influence behavior. Bribes may include:

- gifts and hospitality, particularly where they are disproportionate, secret, frequent or made in the context of business negotiations,
- product discounts or credits that are disproportionate and not readily available to the general customer base,
- the uncompensated use of Company services or facilities,
- political or charitable donations made to a third party linked to or at the request of a customer,
- employment, business or investment opportunities,
- personal favors, or
- the assumption or forgiveness of debt,

regardless of the pretext under which such contributions, or payments are made (e.g. gifts, donations, etc.).

At BME, we do not tolerate any form of bribery and strictly prohibit all employees from offering, paying, soliciting, or accepting bribes. There are strict laws against bribery in many of the locations where we do business including international legislation. We will always abide by these laws, regardless of local custom or business practices.

At BME, we do not tolerate any form of bribery and strictly prohibit all employees from offering, paying, soliciting or accepting bribes.



Facilitation payments are also specifically prohibited. Facilitation payments, otherwise known as “grease payments” or “kickbacks” are typically small, unofficial payments made to secure or accelerate a routine action by a government or public official. For example, issuing a permit, license, consent, or immigration visa, scheduling an inspection associated with contract performance, providing services or releasing goods held in customs, etc. Typically, the consequence of not paying can be out of all proportion to the small payment demanded.

Paying a fee for the use of a recognized, legitimate, fast-track procedure that is open to all and not paid to an individual is not considered to be a facilitation payment. A payment may also be made where the life, safety or health of an individual is threatened. Any such payments must be approved in advance or if this is not practical, reported after the fact to your manager and the Managing Director of your company.

As with competition law, a violation poses serious reputational, legal, and financial risks. It is essential that we fully understand our responsibilities in this area. Depending on your role, you may be also required to undertake specific anti-bribery, corruption, and fraud training to ensure you

understand how to apply our policies and procedures in practice. In general, the following applies:

Employees:

- are expected to read and understand their obligations in regard to bribery,
- must participate in any relevant training program provided,
- if unsure, must seek advice in relation to any aspect of bribery from their manager, the Group Head of Internal Audit or Group General Counsel, and
- are required to notify either their manager, the Company Management or the Group General Counsel about any observations which give reason to believe that there is a case of bribery. Alternatively, the employees may anonymously report such observations to the BME Speak-Up Hotline.

No employee will suffer demotion, penalty or other adverse consequences for refusing to pay bribes or refusing to participate in other corrupt practices even if this means the Company loses business.

Company Management:

- must set an appropriate tone from the top and embed an anti-bribery culture across the Group,
- should support effective communication in regard to bribery and the provision of appropriate and regular training to employees,
- are responsible for the establishment and continued operation of adequate controls and procedures to prevent and detect bribery and the maintenance of accurate books and records to properly record, report and document the substance of all transactions,
- must participate in regular anti-bribery risk assessments,
- must ensure BME Speak-Up Hotline information is displayed prominently and available to all employees,
- should ensure immediate reporting of any breach or suspected breach to their Group General Counsel, and
- should ensure that appropriate disciplinary and, if required, remediation actions are taken where necessary in response to breach.

Failure to comply with this policy either intentionally or through negligence will result in disciplinary procedures being fully enforced including termination of employment and/or relevant contracts.

Money laundering

Money laundering is the process by which individuals or entities use legitimate businesses as channels to “clean” funds acquired through illegal activities. BME does not condone, facilitate, or support money laundering.

We must all watch out for irregularities in the way payments are made, especially large, or frequent cash payments and unusual transactions. In addition, we have a responsibility to conduct due diligence on our suppliers, intermediaries, and business partners and to report any suspicious behavior.

Doing Business with Governments and Regulatory Officials

When dealing with the government and regulatory officials and agencies you must not put our Group at risk of working outside the standards we strive to uphold, as special rules and regulations apply to these interactions.

Therefore, we have an extra responsibility always to:

- **know** and **comply** with all contract requirements,
- **follow** the limits on gifts and hospitality, which can be stricter for government officials than for the private sector, and
- **ensure** all reports, certifications and statements to the government are current, truthful, accurate and complete.

In certain situations, you may have contact with an official or be asked to provide information on the Group’s behalf in connection with a government or regulatory agency inquiry or investigation. As it is vital to ensure that you have all the information you need and all such information is accurate and appropriate for the purpose, speak to your manager before providing any such non-routine information.

Our Commitment to Customers, Suppliers and Business Partners:

- Treat others fairly
- Compete fairly
- Refuse bribery
- Refuse corruption
- Refuse money laundering

OUR COMMITMENT TO OUR GROUP

Protecting Group Assets and Information

Group assets and resources include, but are not limited to:

- property, plant & equipment and vehicles,
- stocks of raw materials, work-in-progress and supplies,
- funds (cash, bank, investments),
- time,
- intellectual property,
- accounting and other business records,
- confidential information,
- computer hardware and software, or
- electronic mail and internet access.

We all have the responsibility to ensure that Group assets and resources are used in a proper manner and for their designated purpose only.

You may make occasional, appropriate personal use of Group assets, if this does not interfere with your work or the work of others. Some further guidance in relation to some of these specific asset categories is set out below.

Intellectual property

You may have access to BME's intellectual property (IP) through the course of your work. IP includes immaterial property such as copyrights, patents, trademarks, design rights and logos. To the extent permissible by law, the rights to all IP created with Group materials, on company

time, at its expense or within the scope of your duties, belong to BME. We must protect these assets and enforce our IP rights if required.

It is also important that you respect other companies' confidential information and intellectual property. If you have authorized access to a customer's or supplier's IP, you must protect it as you would protect your own information. Likewise, you must not use illegally obtained, improperly licensed, or unlicensed software as this could expose us, both as individuals and the Group, to legal action.

Confidential information

You must also protect BME's confidential and proprietary information. This information generally includes any information not available to the public and can include:

- sales information or marketing plans,
- trade secrets, that is information that gives our Group a competitive advantage, for example, customer lists, process information or product specifications,
- policy and procedure manuals, or
- financial data.

You may share such confidential information only for legitimate business purposes and if you are authorized to do so. Please take special care to protect this information by properly securing your computer, documents, or other sensitive materials. In addition, avoid discussing such information. Be conscious of strangers being able to view information and avoid discussing such information in places where you can be overheard, including restaurants, hotels, conference centers, meeting rooms, taxis, airplanes etc.

As part of your employment with the Group, you also provide confidential information about yourself to the Group, including for example, your employment history, personal contact information, marital status and so on. If your work involves handling such information, you must take great care to safeguard it. Never share such information about a colleague with anyone unless there is a business need to do so, consistent with applicable law. Obligations in respect of confidential information continue even after your employment with our Group ends.

External communications

Communications with the outside world play a very important part in the reputational and financial evaluation of BME. Accordingly, all communications to the media relating to our financial performance, acquisitions, strategic plans or any matter which could have a reputational impact on the Group will be handled exclusively by the BME Group Communications team.

If you encounter anything in the media or on the internet that could potentially have a negative impact on our Group's reputation, please raise the issue with your manager immediately so they can ensure appropriate BME personnel are informed. Individual companies in our Group can deal with local trade and media as appropriate in relation to normal business matters arising.

IT & Data Security and Digital Media

Our IT Security Policy sets out the guidelines which we must follow and is summarized hereafter.

Appropriate use of company technology

We are all responsible for proper and appropriate usage of BME technology resources. This includes the email system, internet access, Group-issued mobile devices and computers and licensed software. Our IT systems always remain the property of the Group. You have a right to privacy to the extent provided by law, but not beyond this when using company systems.



BME technology resources should never be used in any way that would be unlawful, offensive, disruptive or harmful to other people. For example, by creating, accessing, displaying, storing or transmitting:

- sexually explicit messages or images,
- material that could be offensive based on race, ethnicity or religious beliefs, and
- otherwise discriminatory or inappropriate material.

We must take special care when drafting emails, remembering that electronic messages are permanent. They can be altered and forwarded without our consent and ultimately this can affect the reputation of our Group. We also must pay attention to instructions relating to backup, anti-virus defenses, encryption, access codes and system support.

The efficient operation and security of our IT systems and related data is essential for the smooth running of our companies.

Data protection, retention, and data privacy

As a Group, we collect a large amount of data. This data includes information relating to our suppliers and other third parties, as well as employees both past and present. We must properly store, use, and transmit this information, in compliance with applicable legislation and any BME and local data protection and retention guidelines.

Documents which are subject of legal procedures or investigations should not be altered or destroyed. Where required by law each of our Group companies must have registered with the appropriate data protection agency. Any known or suspected data breaches should be reported to your manager and the Group General Counsel. They can also help you with any further questions in this regard.

Accounting and other business records

Maintaining accurate and reliable business records, in written or electronic form, is critical to our Group's corporate decision-making process. Among other important uses, these records enable us to meet our various external reporting and legal requirements.

Our accounting functions must therefore always operate to the highest standards so that our records are maintained in accordance with applicable laws, relevant accounting standards and Group guidelines.

Digital (or social) media

Digital media are increasingly used in business services. They are tools and channels for social interaction, using

highly accessible communication techniques. They include, but are not limited to:

- social networking sites,
- online discussion forums,
- blogs and micro-blogs,
- instant messaging,
- message boards,
- video and photo-sharing sites,
- "Wiki" pages,
- RSS-feeds,
- social bookmarking and tagging, or
- other evolving communication tools.

Assume everything you communicate online is public, forever. So think before you post and when in doubt - don't!

We appreciate that these tools help us to communicate more effectively with our stakeholders. However, we also recognize that these emerging channels carry certain risks. When used inappropriately these channels can have unintended and potentially damaging consequences. The guidelines in this section should help you know when and how to best use these tools in a business context.

On the next page you will find some do's and don'ts in regard to digital (or social) media use.



Do....

- Only use digital media tools during work hours where they complement or support your role. If so, clearly identify who you are and note your role. Remember, very few people are designated as official spokespersons for our Group.
- Respect copyrights and acknowledge sources of information and photographs if appropriate.
- If you are publishing information about the company or your role, use a disclaimer, such as “The views expressed on this site are my own and do not reflect the views of my employer”.
- Take particular care not to violate competition or anti-trust laws in any comments on competitors or their products, services, prices, etc.
- Remember to be considerate, sensitive, and professional in your communications, consistent with the highest standards of conduct expected of you.
- Ensure material is accurate, complete and fairly stated and if you make a mistake, admit your error, and correct it as soon as you become aware of it.
- Ask your manager for guidance if you are in any doubt about how and when to use digital media for business purposes.
- Remember your loyalty towards the company when communicating in a private context as well.

Don't

- Speak on behalf of the company unless specifically authorized to do so by your manager.
- Disclose confidential, proprietary, or sensitive information.
- Access or distribute material that is prohibited by law or contains offensive language or content.
- Discuss customers, partners, suppliers, or fellow colleagues without their prior approval.
- Provide employment related references to current/former employees online.
- Post false or inaccurate statements about our company.
- Respond to any inappropriate post or comment about the company. Instead, please alert your manager as soon as possible.
- Communicate slanderous, untrue, and/or defamatory statements against your company.

Conflicts of Interest

A “conflict of interest” arises when you have a personal relationship, a financial or other interest that could interfere with your obligation to act solely in the best interests of BME. A conflict of interest also arises when you use your position with BME for personal gain.

We must be alert to any situations that may create a conflict of interest, whether actual or potential.

We must be alert to any situations that may create a conflict of interest, whether actual or potential. Some common examples of a conflict of interest include, but are not limited to:

- a “closely connected person” such as a member of your household, immediate family, close personal friend or partner is a supplier, customer, or competitor of the Group, or an employee of such a company,
- you or a closely connected person has a significant financial or other interest in a company or person that competes with, does business with or is seeking to do business with BME. Please note however that it is not an issue where the financial interest you have is in the form of securities that are listed on a regular stock exchange or are traded on an over-the-counter basis and constitute less than 1% of the total securities of the particular class,
- you have a direct or indirect reporting relationship with a closely connected person or can influence employment decisions for this person such as salary, promotion or performance evaluation,
- you take personal advantage of any business or investment opportunity presented to BME. This includes situations where you directly or indirectly own an interest or are further developing an interest in property, leaseholds, patents, or other rights in which BME has, or could have, an interest,

- you have outside employment or other activities with a company or individual that competes with BME, or does business with BME, or that affects your ability to do your work for our Group, and
- you serve as a director or officer of another company, or as an elected official. This does not include positions in trade associations that you accept at the request of BME or positions with non-profit, charitable or religious organizations that don’t interfere with your work.

If you find yourself in any of these kinds of situations or if you are aware of others having such potential conflict of interest, you must immediately report it to your manager. New employees must also disclose any such issues when joining the Group. This way, the situation can be properly reviewed and assessed, and an appropriate solution can be determined. You are expected to take any corrective actions requested of you.

Fraud and Theft

BME does not tolerate fraud or theft and requires all BME employees (and third parties who have commercial/ business relationships with BME) to demonstrate high standards of honesty and integrity in their work at, or on behalf of, BME Group companies consistent with the BME Code of Business Conduct.

BME does not tolerate fraud or theft and requires all BME employees to demonstrate high standards of honesty and integrity in their work.

Each BME employee has a personal responsibility to be alert against fraud and theft and to report any actual, suspected or attempted fraud and/or theft. Frauds and thefts can be complex but generally fall into three categories, depending on whether they are committed by:

- a BME employee against a BME group company,
- third parties against a BME group company, and
- BME employees against third parties.

Operating Company Management is required to establish and maintain sufficient controls to ensure that potential fraud and theft risks are properly identified, monitored and limited. BME requires all actual, suspected or attempted fraud and/or theft to be reported using appropriate, defined channels, as set out in Appendix III.

BME will investigate all actual, suspected or attempted fraud and/or theft and seek to recover any losses sustained. Appropriate disciplinary procedures (in compliance with laws) will be enforced against employees engaged (or being complicit) in fraudulent acts.

Each employee is required to:

- read and understand his/her obligations under the Code of Business Conduct in regard to fraud and theft,
- demonstrate honesty in the use of any BME and third-party assets, resources and funds, and
- report actual, suspected or attempted instances of fraud and/or theft.

Operating Company management must:

- set an appropriate tone from the top and embed an anti-fraud and anti-theft culture,
- establish and operate adequate controls and procedures designed to prevent and detect fraud and/or theft (including deterring attempted fraud and/or theft),
- regularly review fraud and theft risk assessment and activities to limit fraud and theft and complete an annual fraud and theft risk assessment,
- ensure appropriate and regular training is provided to employees on fraud and theft, and
- follow the prescribed fraud and theft reporting procedures (see Appendix III).

BME will investigate all actual, suspected or attempted fraud and/or theft and seek to recover any losses sustained.

Fraud and theft risk are best managed through preventative and detective control measures. Operating Company Management is responsible for the effective operation and monitoring of these control measures. Fraud and theft risk are assessed regularly as part of BME's risk management process. The Group's Internal Audit function also checks the effectiveness of the fraud and theft risk controls through audit risk assessments and planning, and the annual assessment of internal controls.

Detailed definitions, together with a number of examples of frauds and thefts, are stated in the following headings.

Fraud

Fraud is any intentional deception that could result in unlawful gain, profit, advantage, harm, or loss to BME or another party. It is important to note that the focus is on the 'intention' of the act, so whether there has been an actual gain or loss is not relevant to whether a fraud has been committed.

The definition of fraud extends to, but is not limited to:

- misappropriation of assets or resources or theft (inclusive of cash, sales proceeds or stock),
- bribery, forgery, extortion, corruption, conspiracy, and/or embezzlement,
- false representation of results in order to manipulate individual bonus or target amounts or to influence decisions of the users of financial reports,
- manipulation of balance sheet accounts to report higher operating results,
- incorrect recording of transactions which can include inaccurate reporting of an actual underlying transaction or reporting of a fictitious transaction,
- collusion with third parties, contractors or suppliers to commit a fraud or theft,

- accelerated revenue recognition on contract accounting,
- falsification of quality control reports, payroll records, customer invoices, change orders, contracts, etc.,
- manipulation of the dispatch process to hide inventory losses,
- unsubstantiated expense claims or inappropriate use of a company credit card or fuel cards,
- by-passing company security systems to facilitate third party theft,
- customer forged cheques and credit card frauds,
- theft of identity of any personnel, including when accompanied by attempted wire/bank transfer,
- customer, supplier, service provider misappropriation of BME funds, and
- failure to comply with regulatory or governmental reporting and disclosure requirements including records created or submitted under a public works contract.

In short, any act that intentionally conceals or misstates facts in order to mislead others is considered fraudulent.

Examples include:

- accelerated revenue recognition on contract accounting,
- falsification of payroll records,
- manipulation of product count records to hide inventory losses,
- unsubstantiated expense claims or inappropriate use of a company credit card or fuel card,
- theft of cash or inventory,
- by-passing of company security system to facilitate third party theft,
- colluding with suppliers by falsifying address and payee details for bank transfers,
- manipulation of balance sheet accounts to report higher operating results, or
- submission of false information to government authorities.

In any case where fraud and/or theft is attempted or suspected it should be reported. If you see something, say something.
Speak up!

We all must be alert to any warning signs that might indicate that fraud may be taking place, such as:

- unusual employee behavior, for example, foregoing holidays or refusing a promotion,
- key documents such as contracts or invoices or vouched expenses are missing,
- a sudden unexplained change of lifestyle or an employee lifestyle that is more prosperous than one would expect from their employment,
- close relationships with suppliers or contractors, for example suppliers/contractors who insist on dealing with one employee only, or an unexplained preference for a given supplier, despite higher prices,
- managers by-passing subordinates, subordinates by-passing managers and management frequently by-passing the internal controls, or
- lack of management oversight and insufficient supervision to ensure that controls work as intended.

In any case where fraud is attempted or suspected, it should be reported as set out in Appendix III. If you see something, say something. Speak up! Doing nothing can imply complicity in the fraud. Any employee who is found to be complicit in a fraud will be subject to disciplinary action up to and including dismissal.

Theft

Theft is taking any property or asset owned by the company, an employee or third party without consent.

In any case where theft is attempted or suspected, it should be reported as set out in Appendix III. If you see something, say something. Speak up! Doing nothing can imply complicity in the theft. Any employee who is found to be complicit in a theft will be subject to disciplinary action up to and including dismissal.

Reporting

It is the responsibility of you and all BME colleagues to report immediately any actual, suspected or attempted fraud/theft of which you become aware. When reporting a reasonably-held concern you will not suffer retaliatory action as a result of reporting. Any colleague (fellow employee, manager or otherwise) suspected of retaliation against an employee for having reported a reasonably-held belief of wrongdoing will be subject to investigation by BME. Following investigation and depending on the outcome, this person may be subject to the company's disciplinary sanctions, up to and including dismissal.

The reporting procedures are set out in detail in Appendix III, and are summarized as follows:

- **Individual discovering or suspecting actual or attempted fraud/theft**

Any employee who discovers or suspects an actual or attempted fraud or theft should report the matter immediately to his/her line manager. The individual also has the option to report to the Group General Counsel, Group Head of Internal Audit or through the BME Speak-Up Hotline.

- **Individual to whom actual, suspected or attempted fraud/theft has been reported:**

When a line manager (or other manager) is made aware of, or suspects, an actual or attempted theft/fraud, he/she must report the incident to senior management, the Group General Counsel and the Group Head of Internal Audit in accordance with the reporting procedures set out in further detail in Appendix III.

All reports of actual, suspected or attempted fraud and/or theft will be fully investigated. Should an employee be found to have committed a fraud and/or theft, the company will implement appropriate disciplinary procedures, measures and sanctions, up to and including immediate dismissal, in accordance with company policies and procedures and applicable law. The company may also report the matter to relevant authorities, such as the local police, as appropriate.

Gifts and Entertainment

We recognize that giving and accepting gifts and corporate hospitality can be a legitimate way to generate long-lasting goodwill in our business relationships. However, if gifts/hospitality are disproportionate or inappropriate they can cloud judgement, so always exercise caution. Specifically, gifts and hospitality must always be appropriate and represent bona fide business expenditures. They should not be offered or accepted if doing so could influence the outcome of a business transaction or be perceived as influencing such a decision.

Gifts and entertainment should not be offered or accepted if doing so could influence the outcome of a business transaction or be perceived as influencing such a decision.

Care is especially required in relation to gifts or hospitality involving government officials.

Appropriate....

- Modest, small, or inconsequential items (such as branded promotional items)
- Occasional or infrequent gifts/hospitality
- Consistent with customary business practices
- Gifts/hospitality given openly, not secretly
- Reasonable travel and accommodation expenses for legitimate business trips
- Hospitality for customers or suppliers as part of company meetings or events (in appropriate situations)
- Gifts/hospitality appropriate for the occasion

Not appropriate...

- Illegal or unethical gifts/hospitality
- Gifts of cash, vouchers, gift cards or shares
- Any item which could be offensive or would cause embarrassment
- Items or incentives which could seem to be bribes
- Gifts/hospitality given in response to, in anticipation of, or to influence a favorable business decision
- Gifts/hospitality in violation of a known policy of the recipient
- Extravagant or overly expensive gifts/hospitality
- Gifts/hospitality given in response to a specific request
- Gifts/hospitality given secretly



Examples of appropriate gifts and hospitality:

- branded promotional items of nominal value e.g. pens, calendars, T-shirts,
- reasonable hospitality given to customers or suppliers as part of Company meetings or events, or
- reasonable travel and accommodation expenses for legitimate business trips.

Individual Group companies may also have prescribed limits regarding the value of gifts and hospitality that may be given or received. Any question about whether a gift is in line with the Group and individual company policy should be directed to your Managing Director.

Our Commitment to Our Group:

- Protect our intellectual property
- Protect confidential information
- Appropriate use of company technology
- Ensure data protection, retention, and data privacy
- Maintain accurate and reliable business records
- Appropriate use of social media
- Avoid conflicts of interest
- Ensure the risk of fraud is minimized
- Refuse inappropriate or disproportionate gifts and hospitality

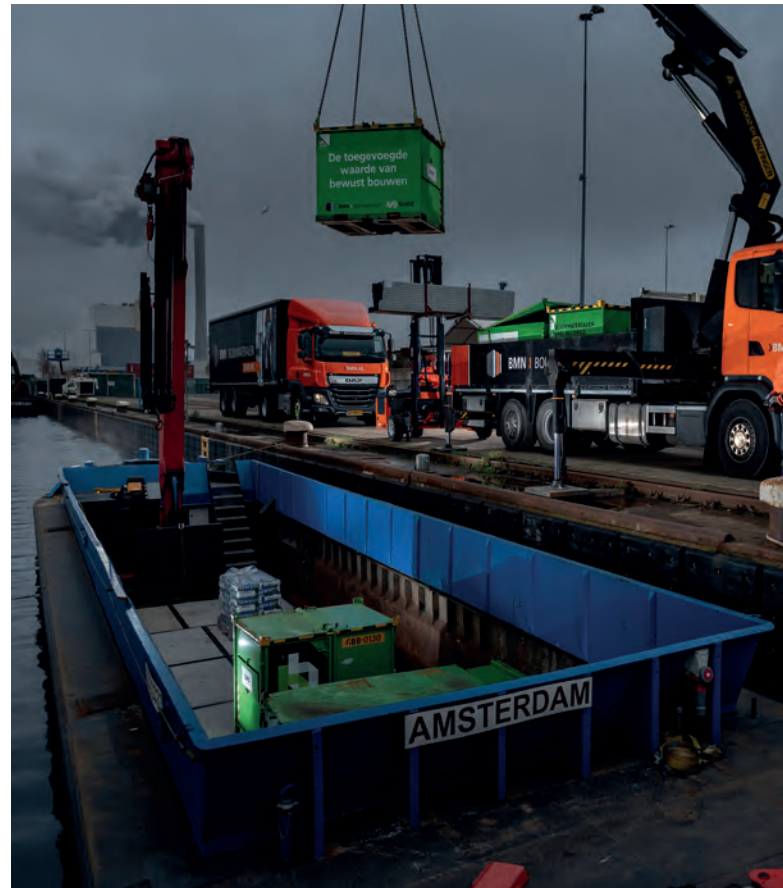
OUR COMMITMENT TO THE ENVIRONMENT AND OUR COMMUNITIES

Environmental Sustainability

Sustainability will continue to be the basis for our success as a Group. We continue to focus on achieving the highest standards of environmental management and control, and on proactively addressing the challenges of climate change. Our commitment to environmental stewardship requires us to:

- **comply**, as a minimum, with all applicable environmental legislation and continuously improve our environmental stewardship, aiming all the time to meet or exceed industry best practice,
- **ensure** that our employees and contractors respect their environmental responsibilities,
- **address** the challenges and opportunities of climate change proactively,
- **optimize** our use of energy and all resources,
- **promote** environmentally driven product and process innovation and new business opportunities, and
- **develop** positive relationships and strive to be good neighbors in every community in which we operate.

We constantly aim to improve energy efficiency, increase the use of alternative fuels, achieve air emission reductions, optimize water use, reduce waste and increase recycling.



Political Contributions

Political contributions include any donation made in cash or in kind to support a political cause, party, candidate or issue. They include contributions made to or through political parties, organizations or individuals involved in the political process. Further, "in kind" contributions can include gifts like the use of company property or services, advertising or promotional activities endorsing a political party, the purchase of tickets to fundraising events or the use of employees' time to assist with political campaigning.

The laws applicable to political contributions vary depending on location and circumstances. In some cases, contributions are prohibited, while in others, they are allowed but must be made public. At BME, one thing is certain - political contributions must not be made as a way of obtaining unfair advantage in a business transaction.

At BME, one thing is certain - political contributions must not be made as a way of obtaining unfair advantage in a business transaction.

Where a political contribution is deemed to be legal and appropriate, is not a means for unfair business advantage, and supports the democratic process, your Managing Director must approve the contribution in writing. All such contributions must be documented, receipted, and recorded.

Charitable and Community Activities

As a responsible corporate citizen, we participate fully in the communities in which we operate. We have a clear direction and focus for our activities, recognizing the value that these partnerships can bring for all. We set appropriate objectives and monitor the effectiveness of our activities, ensuring good governance and communicating openly on our activities.

We support charities and local community projects through donations and other assistance, actively encouraging employee participation.

Practices and customs vary across countries and regions. Therefore, it is appropriate for each business to set their own rules regarding charitable donations. These should recognize local circumstances and be consistent with BME objectives which require all donations:

- to be made for bona fide charitable or public relations reasons; they never should be made when there is or may be a potential conflict of interest or possibility that the donation could be used as a loophole for bribery,
- to be given to a legitimate and credible institution,
- never to be paid to the personal account of a named individual and generally not made in cash (i.e. in the case of financial donations),
- to be made directly not via third parties (e.g. customers or suppliers),
- never to be tied to the execution of a business transaction or government action, or give the appearance of such a tie,
- to be approved by the Managing Director, and
- to be documented, receipted and recorded in the company's accounts.

Our Commitment to the Environment and Our Communities:

- Provide environmental sustainability
- Make political contributions
- Support (local) charities
- Support community projects/activities

APPENDIX I

Relevant Contact Details

In case you would like to report any issue regarding the Code you can contact:

The Group General Counsel:

GeneralCounsel@bme-group.com

The Group Head of Internal Audit:

InternalAudit@bme-group.com

The BME Speak-Up Hotline:

Web intake form:

<https://bme-group.ethicspoint.com/>

Local phone numbers:

Country	Number
Austria	0800 068736
Belgium	0800 74 682
France	0800 90 22 24
Germany	0800 1873676
Netherlands	0800 0225036
Switzerland	0800 838 507

APPENDIX II

Procedures aimed at Preventing Bribery

Procedures aimed at preventing bribery include the following:

- financial and commercial controls are in place to minimize the risk of corrupt payments, including maintaining complete and accurate books and records,
- training is provided to all relevant employees and other key stakeholders as appropriate to their activities and the associated risks,
- risk of successor liability is mitigated by effective and comprehensive due diligence in advance of acquisition/ joint venture transactions and that acquired business units are appropriately integrated to comply with our anti-bribery policy and procedures,
- our business partners (including sales agents, business consultants and intermediaries, sales distributors, lobbyists and other partners (including short and long term joint venture partners) who work on our behalf to assist in securing, preparing or negotiating bids for new contracts or the extension of existing contracts), operate in compliance with applicable local and international anti-bribery and corruption law, and
- this policy and guidance is communicated to all relevant employees and business partners.

APPENDIX III

Fraud and Theft Reporting Procedures

Fraud and Theft Reporting Procedures

The procedures to be followed by BME employees in all cases of fraud and/or theft, whether actual, suspected or attempted, are as follows.

1. Immediate Reporting

1.a.

An employee should immediately report actual, suspected or attempted frauds and/or thefts to his/her line manager. If the employee believes it is not appropriate for whatever reason to report to his/her line manager, he/she should report the matter to any member of his/her management team. Alternatively, the employee can make a report to the Group General Counsel, Head of Internal Audit, or through the Speak Up Hotline.

1.b

Line Managers (or other managers) who have been notified of an allegation or other information reasonably supporting a case of actual or suspected fraud and/or theft (including attempted fraud/ theft) must immediately report the matter to:

A. Operating Company Managing and Finance Directors and Internal Audit where:

- The gross value of the fraud and theft (including attempted fraud/theft) is expected to be greater than or equal to €25k, so that senior management can provide input into the investigations process, and/or
- It appears on reasonable grounds that a member of management or the executive team is involved (regardless of the fraud and/or theft value),

and

B. the Group General Counsel and Head of Internal Audit where:

- The amount involved is expected to be greater than or equal to €100k, and/or
- It appears on reasonable grounds that a member of management or the executive team is involved (regardless of the fraud and/or theft value).

In these circumstances (where 1.b.B. above applies), Internal Audit must be engaged before taking any steps (such as commencing a local investigation) or taking any legal or disciplinary actions.

2. Reporting within Seven Days

Actual, suspected or attempted fraud and/or theft with a gross value expected to be between €25k and €100k must be reported within seven days. Investigations can be initiated by the business (with inputs from senior management as appropriate) prior to reporting.

3. Annual Reporting

Operating Companies must have procedures in place to ensure that all actual, suspected or attempted fraud and/or theft over €5k are reported to the Group General Counsel on at least an annual basis.

All actual, suspected or attempted fraud and/or theft under €5k must be fully investigated but do not normally need to be reported as above. However, where there are multiple low value incidents of the same fraud and/or theft (including attempted fraud/theft) or at the same physical location which, when combined, add to more than €25k, these incidents must be dealt with and reported as described in 1 and 2 above as appropriate.

The reporting procedures for actual or attempted frauds/ thefts, as set out above, are summarized in the following table:

Reports of actual, suspected or attempted fraud and/or theft may be communicated via e-mail, letter or phone call. All communications should include the information set out in the Fraud and Theft Reporting Checklist in Appendix IV.

As the investigation and evaluation of the matter proceeds, regular updates should be provided to the Group General Counsel and Head of Internal Audit. When completed, the report should contain the required information as set out in the checklist in Appendix IV. At all times, communications need to be dealt with in a confidential and sensitive manner and details maintained in accordance with applicable local law, such as data protection legislation.

Amount €	Reporting to Managing and Finance Directors and Head of Internal Audit	Reporting to Group General Counsel and Head of Internal Audit
Greater than or equal to €100k	Immediate	Immediate
Greater than €25k and lower than €100k	Immediate	Within seven days
Greater than €5k and lower than €25k	Company management informed immediately	Annually

4. Management

In addition to fulfilling the reporting requirements set forth in sections 1 and 2, Operating Company management must ensure that an appropriate investigation is undertaken (in consultation with the Group General Counsel and the Head of Internal Audit). Operating Company Management will decide, in consultation with the Group General Counsel and the Head of Internal Audit, the conduct and scope of any investigation.

Following each investigation, management must issue a written report of their findings (using the Checklist for reporting in Appendix IV) to the Group General Counsel and Head of Internal Audit. Where a suspicion of fraud or theft involves potential legal issues, management should also consult a legal counsel from the earliest stages of an investigation.

APPENDIX IV

Checklist for Reporting actual, suspected or attempted Fraud and/or Theft

1) Checklist for initial Fraud/Theft report to the Group General Counsel and Internal Audit (illustration set out below is by way of example guidance)

Information to be documented and forwarded:

- Nature of the fraud/theft and a brief description
 - a) suspected or attempted fraud/theft (no evident loss at time of reporting to BME)
 - b) fraud/theft resulting in asset (inventory/equipment) or /cash (or credit card) loss
 - c) falsification of records
- How the fraud/theft was discovered and reported and by whom
- Estimated gross amount of the fraud/theft involved
- Name or e-mail of the person reporting an issue and their title
- Names of involved parties and their relationship to the employer (employee, vendor, etc.)
- Relevant dates – when the fraud/theft became apparent, frequency, when reported, overall timeframe
- Name of company where issue arose and location
- Names of others who have knowledge of the issue, including management personnel
- How much has been or could be recovered through insurance, prosecution and/or payback
- Advise if known who the perpetrator of the fraud/theft is:
 - a) unknown
 - b) external party or
 - c) employee
- Any control failings identified
- Personnel actions taken
- Other actions taken

Additional Information for fraud/theft issues reported by telephone call:

- The location of the incoming call
- Other observations (e.g. was the caller aggressive, upset)

2) Checklist for final Fraud/Theft report to the Group General Counsel and Internal Audit (illustration set out below is by way of example guidance)

- Summary of the investigation
- Name of parties involved in the investigation and method of investigation
- Was the person reporting the issue contacted? Was the reported issue supported or valid? How does the contact know about the issue? Any additional information received by contacting the person? Any eyewitnesses / documentation?
- How the investigation was completed, and the information compiled as appropriate
- Details of outcome and resolution including details of suggested actions required where applicable and, as appropriate
- How legal and communication aspects have been dealt with

Operational Businesses

We operate in Austria, Belgium, France, Germany, the Netherlands and Switzerland.

AUSTRIA



BELGIUM



lambrechts..



FRANCE



GERMANY



Detering



NETHERLANDS



SWITZERLAND



