Compliance

Code of Conduct

The Dutch Authority for the Financial Markets

August 2021

AFM

Table of contents

1. The Code of Conduct – Your foundation 4
   - 1.1 The importance of the integrity of the AFM 4
   - 1.2 Principles and practical application 4
   - 1.3 Handling dilemmas 5
   - 1.4 Applicable to employers and contractors 5
   - 1.5 Entry into force 5
   - 1.6 Reading guide 6

2. Integrity Values 7
   - 2.1 A straightforward compass 7
   - 2.2 Reliability and diligence 7
   - 2.3 Personal responsibility 7
   - 2.4 Independence and impartiality 7

3. What it means to be a good employee 8
   - 3.1 Being a good employer 8
     - 3.1.1 Duty of care, integrity policy and HR policy 8
     - 3.1.2 Dual responsibility for line managers 8
   - 3.2 Being a good employee 8

4. Specific rules and standards 10
   - 4.1 Preventing actual or apparent conflicts of interest 10
     - 4.1.1 Incompatible activities 10
     - 4.1.2 Activities on behalf of the AFM 11
     - 4.1.3 Incompatible activities prior to entry into service 12
     - 4.1.4 Private investments 12
     - 4.1.5 Benefits – Gifts, invitations or payment in return for external activities 12
     - 4.1.6 Cooling-off period 12
   - 4.2 Handling data with care 13
   - 4.3 Insider files 16
   - 4.4 Prudent use of facilities and resources 16
   - 4.5 Social conduct and personal relationships 17
   - 4.6 Communication 18
   - 4.7 Privacy management 19

5. Prevention and enforcement 21
   - 5.1 Reliability systematically tested 21
   - 5.2 Suspected or actual abuses and integrity violations 21
   - 5.3 Investigations and sanctions 23

Appendix 1:	Definitions and explanations	25
Appendix 2A:	Private investments regulations	30
Appendix 2B:	Work instructions for updating the closed list	37
Appendix 3:	Explanatory notes on insider files	43
Appendix 4:	Regulations on reliability screenings	44
Appendix 5:	Reporting scheme for actual and suspected abuses and integrity breaches	53
Appendix 6:	Regulations on integrity investigations and sanctions	59
Appendix 7:	Regulations on complaints of undesirable behaviour	65

1. The Code of Conduct – Your foundation

1.1 The importance of the integrity of the AFM

You are employed at an extraordinary organisation. The AFM has an important public role with respect to the financial markets. For this reason, society must be able to have full confidence in us. This means that you, along with all others who work at and on behalf of our organisation, bear a great responsibility. Together, we commit ourselves to an outstanding reputation.

1.2 Principles and practical application

Protecting the AFM's integrity is our shared responsibility. By doing this, we also inspire confidence in the AFM. However, what does it mean to act with integrity and due care? How can you contribute to our integrity? This Code of Conduct will guide you in this.

Nevertheless, the code cannot provide for any scenario that could arise. There will always be circumstances in which the right thing to do will not be obvious. This is because acting with integrity is about more than simply applying rules and guidelines. And this means it is normal to have doubts from time to time. Values and standards are not always straightforward to apply and might sometimes contradict each other. In other cases, your integrity as an individual could be at odds with your integrity as an AFM employee. It is only in daily practice and the discussions we have among ourselves that the true meaning of integrity takes shape. Integrity is about being conscious of interests and possible consequences, and reflecting and making choices. Discussions with colleagues and line managers will not always provide an immediate answer. In addition, often you will find that there is more than one way to resolve an integrity concern. What does not change, however, is that the responsibility for acting with integrity rests with you, including when a specific scenario is not addressed in the Code of Conduct.

The Code of Conduct offers protection and helps you to recognise risks and resist external pressure and temptations. This is important because people within and outside of our organisation could challenge your integrity and hold you accountable.

You might face situations in which the guidance given in the Code is not sufficient. If this happens, it is important that you raise questions, concerns, dilemmas and breaches regarding compliance with the Code of Conduct and related regulations in a timely manner. You are personally responsible for your conduct but that does not mean you are left to face things on your own. Discussing difficult situations among ourselves allows us to learn from each other and help each other evaluate what our course of action should be. Raising concerns could also help to prevent integrity violations. If you don't feel comfortable speaking to your (immediate) colleagues, your line manager or the most senior line manager, you can raise the issue with AFM employees who focus specifically on integrity, such as our confidential counsellors and compliance officers. They can provide further guidance for most questions, concerns and dilemmas. The guiding principles are that an employee's position should not play any role in finding a solution, employees should receive equal treatment, and decisions must be made in an objective and independent manner.

1.3 Handling dilemmas

Our expectation is that you conduct yourself within the limits of the Code of Conduct. However, the distinction between what is and is not permitted or acceptable is not always crystal clear. The steps below are intended to provide more guidance when navigating grey areas.

Explore the dilemma

Describe the dilemma and identify the interests and interested parties. Assess how the dilemma impacts on companies subject to supervision, workers, management boards, supervisory boards and society.

Identify relevant rules and processes

Check whether rules and/or processes have been developed with regard to the situation at hand. Review whether they might help you with your dilemma. If these are not adequate and offer room for improvement, tell your line manager.

Talk to your line manager and colleagues

Your line manager and colleagues could offer new perspectives that help to resolve your dilemma. What are their thoughts about your approach and is there anything they could add?

List possible solutions

List all possible solutions, together with the advantages and disadvantages of each. Be aware a solution cannot always be to the satisfaction of everyone. What you can do, however, is ensure it is the best solution overall by carefully weighing all interests.

Decide

Use all the information to select the solution that you believe to be the best. Have courage and own your decision. Ensure you are able to substantiate it and that the decision is consistent with what the AFM stands for and our integrity values. In case of doubt, please get in touch via compliance@afm.nl.

Feedback

Afterwards, there is the option to discuss your decision with your line manager and/or colleagues if you wish. Use this as an opportunity to learn together.

1.4 Applicable to employers and contractors

As a rule, the Code of Conduct applies to everyone working at or on behalf of the AFM. After all, the exact nature of the relationship between an individual and the AFM is not of interest to the outside world. Anyone who has an employment contract with the AFM regularly carries out work for the AFM or is seconded to the AFM, such as temporary workers, external staff and placement students must be familiar with the Code of Conduct and comply with the agreements made with them. The same applies to the members of the AFM Executive Board and the AFM Supervisory Board.

1.5 Entry into force

At the same time as this Code was drafted, a number of regulations were revised and either integrated in the Code itself or included in its appendices. This Code of Conduct and its appendices will come into force on 1 January 2021. The entry into force of this Code of Conduct

will not affect the validity of any specific arrangements agreed between employees and compliance officers based on earlier regulations.

1.6 Reading guide

Chapter 2 introduces you to the key principles for acting with integrity. Chapter 3 then looks at the different roles in relation to integrity, and considers the parts played by the employer (and line managers) and employees respectively. Chapter 4 delves into the significant part: the regulations that combine to create the core of our Code of Conduct. Chapter 5 concludes by outlining how the Code of Conduct is enforced and how it has been embedded in policies.

For convenience, this Code of Conduct does not describe all regulations in full detail. Instead, the full texts, some of which are more legal in nature, have been included in the appendices.

The easier it is to talk about what acting with integrity does and does not look like, the more natural it will become to embed integrity in all our decisions.

2. Integrity Values

2.1 A straightforward compass

Our core values of diligence, thoroughness, autonomy and connectedness guide us when making choices and dealing with dilemmas. They help us to be the professional, expert, discrete and ethical supervisor that we aim to be. We have developed 5 integrity values to explain what acting with integrity means to us. These are reliability, diligence, personal responsibility, independence and impartiality. Together, they can serve as a straightforward integrity compass. There will be times when more specific standards and rules apply. These are described in greater detail in Chapter 4 and the appendices.

2.2 Reliability and diligence

Conduct that proves unreliable or lacks due care undermines the trust placed in the AFM. This is why you stick to agreements and never make any commitments you cannot deliver on. You refrain from sharing confidential and sensitive privacy data with others. You will also prevent unintentional disclosure. You ensure resources are used in a prudent and efficient manner. Your decision-making process takes account of all relevant interests. Your conduct towards others, both within and outside of the AFM, is correct, appropriate and respectful at all times.

2.3 Personal responsibility

Working at the AFM implies a great deal of responsibility. You will sometimes have an impact on key social topics and the well-being of individuals and organisations. Or you could suddenly find yourself in the public eye. This means there are high standards to be met when it comes to your skills and personal responsibility. You must be keenly aware of the fact that you might have to account for your conduct at any time. This is why you need to take responsibility for your conduct and be prepared to provide justification if needed.

In addition, our expectation is that you not only take responsibility for your own conduct but also help to safeguard the integrity of our organisation as a whole. You should support others in striking the right balance and challenge them if they behave in a way that is improper. You cannot be a bystander.

2.4 Independence and impartiality

We must arrive at our decisions in a way that is independent, impartial, and consistent with the regulations applicable to the AFM. This means we do not allow ourselves to be guided by self-interest or inappropriate motives. An example of self-interest is when you derive personal benefit from a decision taken by you in your capacity as an AFM employee. An improper motive is said to exist when your decision is based on discriminatory grounds or when a conflict of interests applies.

3. What it means to be a good employee

3.1 Being a good employer

3.1.1 Duty of care, integrity policy and HR policy

It is important to the AFM to be a good employer. As a public sector employer, we also have a duty of care towards our employees. Part of this is having an effective integrity policy. The aim of this is to protect you against integrity risks in the best way possible, for example by ensuring work processes are well organised (segregation of duties), providing facilities (confidential counsellors), putting in place this Code of Conduct and keeping it up to date.

Another aspect of being a good employer is ensuring we create a safe environment in which you and your colleagues can speak up about integrity concerns. The AFM has embedded integrity in all aspects of its work, operational management and HR policy – from recruitment, selection and onboarding to work instructions, work meetings and training.

3.1.2 Dual responsibility for line managers

Line managers represent the AFM as an employer in day-to-day operations. Aside from being a good employee, they must also act as a good employer. As part of this, they must support and protect employees who raise concerns about unethical conduct. Line managers must also challenge improper behaviour by employees and, if necessary, take action.

Line managers, at whatever level, cannot have credibility unless they themselves set the right example. They are expected to inspire with their leadership and role model the right behaviour. They should keep this front of mind at all times, convey the importance of integrity and explore the topic. They must also ensure they identify integrity risks in good time, describe them and tackle them properly.

It follows from the above that the AFM also has a specific responsibility towards line managers. They will require guidance and support to be able to properly fulfil their role. It is also important for line managers to discuss integrity and related issues peer to peer. This allows the management team to assess on an ongoing basis whether integrity is being adequately protected.

3.2 Being a good employee

Being a good employee means carrying out your work duties to a high standard, and in a committed and conscientious manner. Our public mission comes first and outweighs any other loyalties. You are fully aware of your responsibilities and do what is right, including when this might not be so easy and could lead to a conflict between you and a colleague, a line manager or the organisation. For you, our five integrity values come first.

Being a good employee requires excellent judgement, as the circumstances will be different each time. You act in the public interest and will weigh up the legitimate interests of the parties who call upon you. Making the right decision requires commitment, insight and courage:

- Commitment to the AFM and the public interest;
- Insight to arrive at the right decision in difficult circumstances;
- Courage to be decisive and translate your moral judgment into ethical actions.

Professional integrity is about the way we go about our day-to-day activities and is not confined to our workplace or working hours. For example, we live in a digital world with options for flexible

working and a very fine line between work and home. This is precisely why it is important that you are clear on the risks and boundaries. We must always put integrity first, including in special circumstances, for example in times of crisis when lines become blurred. It is essential that you properly consider this, not least because actions in your private life can also have an impact on your capacity to be a good employee.

4. Specific rules and standards

4.1 Preventing actual or apparent conflicts of interest

For your own credibility and that of the AFM, it is important to be aware of risks that could lead to your integrity being called into question. In this context, it is important to ensure you prevent any actual or apparent conflicts of interest. This risk arises when your duty to act solely in the interest of the AFM – and as such in the public interest – is compromised by a personal interest, an interest associated with an incompatible activity or a transfer to a company subject to supervision. It is key that you recognise such risks and report them immediately, even if you are unsure.

Preventing risks

In order to prevent conflicts of interest, you are not permitted to participate on the AFM's behalf in any opinion, decision or other activity that is of material importance to the AFM and which involves:

- A related third party;
- A legal entity in which you or a related third party has a financial interest;
- A legal entity where a third party related to you holds a position on the executive board;
- A legal entity where you yourself hold the position of policymaker or co-policymaker.

As an employee, you must keep an eye out for the above scenarios. You should also refrain from using non-public information available to you because of your work or position for the purposes of carrying out a transaction for either a related third party or yourself.

Related third party

Related third party is an individual with whom you maintain a close connection that could leave you open to conflicts of interest. In specific terms, this refers to your partner, blood relatives and relatives by marriage in the direct line, first degree and second degree, and anyone else with whom you run a shared household.

Reports and disclosures

If you are involved in an actual or potential conflict of interests or relevant irregularity in relation to compliance with rules and standards, you must at all times report this to your line manager and the compliance officer immediately. When doing so, please ensure you always mention all relevant circumstances.

In addition to this, you should also use BAS to disclose any ancillary activities you wish to undertake, any benefit you have been offered and wish to accept, or any investment account you wish to open which this Code of Conduct or another specific regulation requires you to disclose. The compliance officer, having obtained your line manager's approval as appropriate, will assess whether your disclosures could be deemed an actual or potential conflict of interest, incompatible activity or improper advantage. The compliance officer may then impose measures and/or conditions aimed at preventing undesirable situations.

4.1.1 Incompatible activities

The AFM welcomes that employees dedicate time and effort to activities outside their work duties at the AFM, if those activities are consistent with the objectives, interests, responsibilities and work

of the AFM. Activities are considered incompatible with your employment at the AFM if they could result in:

- Damage to the AFM's reputation or interests;
- An actual or apparent conflict of interests;
- Too much time being taken up, as a result of which you are prevented from properly carrying your duties;
- Any influence on the policy or results of a company under supervision.

An incompatible activity could exist if one or more of the criteria below are applicable in your case (but this list is not exhaustive):

- You have been approached for an ancillary activity as a result of your position at the AFM (or this is suspected to be the case);
- An overlap exist between the ancillary activity and your role at the AFM, for example in terms of your field of work, expertise or duties;
- You might have dealings with the AFM, for example because you will be using AFM data or might have contacts with other AFM employees;
- You might have dealings with a company subject to supervision, for example because you are the treasurer of a club and need to co-sign for any loans the club wants to take out;
- The organisation on whose behalf you are carrying out the ancillary activity is less well regarded;
- The activity could result in negative publicity or reputational damage for the AFM.

Examples:

- If you are taking up a volunteering role with a local sports association, you will not always need to report this. The exception is when you will be handing financial matters for the association.
- You have just moved in with your partner and want to let your former home. You will not need to disclose this. However, that changes if you offer rentals on a more commercial scale.
- You decide to put your coaching training to good use in your spare time. You offer paid coaching to people in your immediate and more distant surroundings. You must report this ancillary activity.
- It is not automatically possible for you to teach or write about things like the operation of financial products in a personal capacity. If there is a risk of damage to the AFM's reputation or interests, the activity is not compatible with your duties at the AFM. However, you might be able to carry out this activity on behalf of the AFM.

4.1.2 Activities on behalf of the AFM

If an activity arises from your work at the AFM or forms part of your role at the AFM, there is no requirement to report this to the compliance officer. An example would be membership of a specific consultative or other committee where you represent the AFM. You will need approval from your line manager for this and you will need to contact the Communications department in advance with regard to any external communications, such as speeches, presentations or articles. Any payment for the activity must be transferred to the AFM in full. Ask the Planning, Control and Finance department how to do this.

If you are not permitted to undertake an activity in a personal capacity – for example because there is too much overlap between the ancillary activity and your work for the AFM – it might be still possible to carry out the activity on behalf of our organisation.

4.1.3 Incompatible activities prior to entry into service

It might be that you undertook activities incompatible with your duties at the AFM before you took up employment with the AFM. In such cases the compliance officer can attach conditions to your start date and the nature of your duties at the AFM. The compliance officer will do this in consultation with your line manager.

4.1.4 Private investments

If you or a related third party wish to make private investments, this is only permitted subject to conditions. This is because private investments carry risks. Appendix 2 explains the strict conditions and limitations that apply in this regard. In case of any doubt or ambiguity, please always refer to the compliance officer.

The risks of private investments are particularly high for AFM employees since the AFM has access to confidential data – data that is not publicly available and use of which could lead to insider trading, which is prohibited by law.

4.1.5 Benefits – Gifts, invitations or payment in return for external activities

You will sometimes receive a gift, invitation or payment in return for an external activity. These are considered a risk as they can give rise to an actual or apparent conflict of interests. For this reason, you can only accept if a number of conditions are met:

- With regard to any contributions made by you, such as a presentation at a company subject to supervision, you will be permitted to accepts gifts up to a value or estimated value of EUR 50. Your line manager must approve these and you must record them in BAS within 7 working days following receipt.
- The offer of the benefit must be based on a valid reason and the benefit must be proportionate to the activity performed. This means you must critically examine the reason, the relationship between the AFM and the organisation (supervision or other business relationship) and current circumstances (any ongoing investigations). As a general rule, you are not permitted to accept event tickets from a company subject to supervision.
- If the value or estimated value exceeds EUR 50, you will need your line manager's approval, followed by approval from the compliance officer via BAS. In case you and your line managers disagree with the decision made by the compliance officer, the Executive Board will make a decision.
- It is not permitted to accept cash but you can accept vouchers with a value below EUR 50. Payments for an external activity are an exception to this (please see the final item).
- If an invitation to an event is offered, this must have demonstrable relevance for the AFM and/or the employee's role. The employee can be accompanied by their partner if this is accepted practice and/or necessary to ensure the AFM is appropriately represented. As is the case for any expenses for travel and accommodation, the number of AFM employees invited must be proportionate.
- Payments for an external activity must be transferred to the AFM in full. Ask the Planning, Control and Finance department how to do this.
- Small gifts such as note blocks and pens do not need to be reported.

The rules applicable to accepting a gift, invitation or payment for activity apply in equal measure to the offering of such benefits on behalf of the AFM.

4.1.6 Cooling-off period

A move to a new employer could be subject to a cooling-off period. Such a period will apply if there is any actual or apparent conflict of interests. An example is if you were to move to a

company subject to supervision. A cooling-off period might also apply if your employment is terminated at the decision of the AFM. A cooling-off period will be separate from any notice period stipulated in your employment contract.

As a general principle, contractors are not subject to cooling-off periods. In relation to specific roles, however, the responsible Head of department or manager may decide the cooling-off period does apply to a contractor. If applicable, candidates will be notified about this before their entry into service and arrangements will be made that will be documented in their contract.

Notify your departure in good time
If you decide you wish to leave your role at the AFM, you must notify HR and your line manager about this in writing as soon as possible. Your line manager, consulting the compliance officer as needed, will then analyse the risk of any actual or apparent conflict of interests and determine the length of the cooling-off period. Your line manager will also pass this information to HR.

Actions in the event of a risk
If it is established that your move carries the risk of a conflict of interests, the following measures will apply in order to protect you and the AFM:

- HR will revoke your access to the file management system within two working days after the determination was made.

HR will tell you about this so you can use these two days to finalise and handover your work. Once your access has been revoked, you can only work with files through your line manager or together with a senior employee.

- Cooling-off periods are set at a maximum of two months.

During the cooling-off period, you will no longer be able to access the AFM's systems and premises. The length of the cooling-off period will be determined by your line manager, who will consult the compliance officer as needed. The cooling-off period will be a maximum of two months and will cover the time until you take up employment with your new employer.

Cooling-off policy for the AFM Executive Board
The AFM Executive Board is subject to a separate cooling-off policy. This has been set out in the employment contracts of the Board members.

4.2 Handling data with care

Working at the AFM often means handling sensitive information – information that is confidential and at times even secret. You are expected to play your part in keeping this information safe at the AFM. This has been formally documented in the non-disclosure agreement signed by you, which will become effective after you leave the organisation.

8 rules for protecting information

1. Stay alert, always

   Always be mindful. Consider which work things you can and should not talk about at home. Who might overhear what you are sharing about your work? The responsibility rests with you. Do not share confidential or highly confidential information with others and ensure you have permission before you share such information with colleagues who do not need it for work purposes. When sharing anonymised information, for example in the context of exchanging knowledge with members of your team or other colleagues, you must also ensure the information cannot be traced back to individual files.

2. **Apply the data categories**

   The AFM uses what is known as a data classification system. This system uses the impact of a potential disclosure to determine how confidential information is. Apply the classification to decide how you should look after the information that is made available to you.

3. **Handle data carriers with care**

   Ensure you do not intentionally or unintentionally provide unauthorised third parties with access to information. Follow the instructions provided when you begin using IT assets issued by the AFM, such as tablets, smartphones and laptops. Do not use personal storage on an AFM smartphone to keep AFM data. The same rule applies to personal portable data carriers (such as CD's and USB sticks).

4. **Stay safe when working remotely**

   A secure IT solution called e-werken (e-working) is available for working remotely. Use of this secure solution is mandatory whenever you work away from the office.

5. **Stay safe when you carry out online research**

   If your duties at the AFM require online research, your online conduct might be visible to outsiders. This might unintentionally allow them to glean insights or information. It is therefore important that you follow a course on making online research safe first and then apply your learnings. Talk to your line manager and ask the Digital Research team about training and measures.

6. **Look after your computer**

   If you step away from your workstation, whether at or outside of the office, always lock your computer, tablet or smartphone. Our information is not intended for your housemates, partner or friends. Be aware of the risks. If you are on a trip, a train or a plane, use a privacy filter for your laptop.

7. **Treat hardcopies with care**

   Ensure your desk is clear at the end of a day and never leave confidential documents out. Do not print documents unless you need to and do not keep printed information you have used outside of the office. Always take documents to the office and dispose of them by placing them in the dedicated secure paper bins. Non-public information can be put in with regular waste.

8. **Security and visitors**

   You must carry your personal AFM access card with you whenever you are in the AFM building. Do not leave your card unattended at any time and do not lend it to others. Report visitors to reception ahead of time. Your visitors are your responsibility. This means you should collect them and escort them back to the exit afterwards. You must only receive visitors in the conference rooms on the ground floor. This rule also applies to former colleagues or staff from other supervisory authorities who do not have a personal AFM access card. Receiving visitors on upper floors is restricted to the Executive Board.

Be transparent

Treating information with care also implies that you must not withhold or manipulate relevant information if that would be beneficial to you or the AFM. Your role is to serve the public interest and this means all available information must be accessible and considered in an objective manner. If, in spite of this, you think there are grounds to exclude specific information, you must do this in a transparent manner and document this in the file. In this way, the reason for excluding the information can always be verified.

Take special care when emailing and browsing

Wi-Fi-networks

Never share login credentials with others. Only use Wi-Fi networks that can reasonably be assumed to be safe, such as the AFM network or home Wi-Fi. Do not use public Wi-Fi networks. Alternatively, you can enable the hotspot function on your smartphone.

Emails and confidentiality

You must never use email or the internet to send non-public information externally. Use Cryptshare instead. Assess the sensitivity and use the Normal, Confidential or Private security option in Outlook. Check carefully that you have used the correct email address and that you have included your external digital signature, containing your name, role, department and address details.

No external email services

Never use external email services, including your personal email account, for work. It is also not permitted to share AFM data using any other cloud service than Cryptshare.

External surveys

If you need to gather information from external parties, consider the best way to go about this. An example is when you might want to send questionnaires to a (significant) number of companies subject to supervision. The AFM has technical solutions that enable you to organise this in a safe and efficient manner, and which prevent non-public or other information of companies subject to supervision from falling into the wrong hands.

Data classification table

Public	Information that was actively brought into the public domain by the AFM or another party.
Internal	Information which, based on its content or nature, is appropriate to share with colleagues at the AFM, provided this is useful for the recipient.
Confidential	Information which, based on its content or nature, should only be distributed in a limited circle.
Highly Confidential	Information which, based on its content or nature, should only be distributed in a very limited circle.
Secret	Information which, based on its content or nature, should not be distributed, or only in an extremely limited circle. Information in this category will only be distributed if, strictly necessary to ensure the proper functioning of the AFM or the financial markets.

Email sensitivity

Normal	This is the default setting for emails. Anyone with access to the recipient's email account is able to view the email.
Confidential	This indicates that the email needs to be treated as confidential. However, anyone with access to the recipient's email account will be able to view the email.
Private	This indicates that the email needs to be treated as highly confidential. The addressee can only open the message. Not anyone else who has access to the email account will be able to do this.

4.3 Insider files

For any project involving of the use of non-public information, which could result in financial or reputational damage if it is intentionally, or unintentionally disclosed, there is an option to designate the project an insider project by using an insider file. This reduces the chances of a leak by restricting the number of employees involved. The file coordinator, usually the project manager, will invite you and register you with the compliance officer using BAS. Insiders can only share file-related information with colleagues appearing on the same insider list. For more information on working with insider files, please see Appendix 3.

Insider projects are commonly used in the following scenarios:

- The continuity of a company subject to supervision is at risk and the AFM is considering drastic measures, such as the appointment of a trustee in bankruptcy or the imposition of a hefty administrative fine.
- The information available constitutes inside information and the circumstances are such that an additional measure taking the form of an insider project is necessary.
- The case involves a decision by the AFM, in relation to which the AFM, a company under supervision and/or its (co-)policymakers run a significant reputational risk if the information becomes public knowledge or is made public prematurely.

4.4 Prudent use of facilities and resources

The AFM puts a range of facilities and resources at your disposal. Please ensure you use them carefully and sparingly, and only for their intended purpose. Our facilities also include the option to have costs reimbursed. Use this only for work-related expenses that you have actually incurred and that you have not already be declared elsewhere.

Private use of facilities and resources

Work and home lives increasingly intersect in our world and as such, the AFM allows appropriate personal use of facilities and resources. Abuse, however, will not be permitted under any circumstances. What do we mean by abuse? It would be impossible to provide an exhaustive description. The key here is to use good judgement and your own moral compass. If you are unsure, talk to your line manager and put things in writing.

Examples of private use that is not permitted:

- Making extensive use of work copiers for private purposes;
- Offering work tools or materials for sale;
- Downloading illegal or other software (not even for work purposes);
- Using AFM resources to carry out inappropriate activities such as gambling, gaming or viewing porn.

Official travel regulations

Employees who travel for official purposes on behalf of the AFM can have related expenses reimbursed, subject to conditions. For the applicable rules, please refer to the Reimbursement Policy.

Extending official travel

If they wish, employees who are travelling on official business can use leave to extend their trip for personal reasons. However, the interests of the AFM must continue to come first and abuse will not be tolerated. Always ask for permission first. The additional costs will need to be covered by the employee.

Accompanying partners

The AFM will only cover travel for an accompanying partner if that partner has been specifically invited and/or his or her attendance is necessary to ensure the AFM is appropriately represented. The relevant board member must grant permission and the form for the accompanying partner must have been completed.

4.5 Social conduct and personal relationships

At the AFM, we interact with one another in a collegial and appropriate manner. We also ensure our behaviour towards external parties is appropriate and respectful. Amongst other things, this means we take each other seriously, we listen, show courtesy and respect each other's privacy.

Undesirable behaviour

The AFM does not tolerate nuisance, insults, discrimination, sexual harassment, intimidation, bullying, aggression or violence. It is also forbidden to send any pornographic, racist, discriminatory, insulting, offensive or (sexually) intimidating texts and/or images, or any messages that could incite hatred and/or violence.

Challenge colleagues who behave inappropriately and support colleagues who are being victimised. It can be difficult for a victim to talk about or report undesirable behaviour, especially when a line manager is involved. In these cases in particular, it is essential that we help one another and make use of one of the dedicated channels put in place by the AFM. These dedicated channels are: the line management, the HR advisor, the compliance officers, the confidential counsellor or the complaints procedure (see Appendix 6).

Personal relationships in the workplace

It can happen that employees are not just colleagues but also partners, friends or family members. Whenever this is the case, it is particularly important that the parties involved continue to act in a professional and objective manner, and are mindful of the integrity risks that can be associated with these personal relationships. Scenarios in which there is a hierarchical relationship between partners or family members and in which they evaluate, review or approve one another's work, are not permitted. This type of scenarios can be a source of risks, including the risk of actual or apparent conflicts of interest, preferential treatment or sharing of confidential information. Should you find yourself in such a situation, you must report this directly to your line manager or the most senior manager or, in exceptional circumstances, the compliance officer. You must do this even if you feel the relationship poses no risk.

Friendships at work can contribute to a good working climate. Also for these friendships, counts that your personal integrity may never be compromised and you remain objective and

professional. Friendships in a hierarchical relationship require you to remain alert and will need to be disclosed if your relationship could pose a risk. Again, you should immediately notify your line manager or the most senior manager or, in exceptional circumstances, the compliance officer.

Your line manager will treat this disclosure with respect and consider your privacy. You and your manager will look at the possible risks and solutions together, and involve the compliance officer as needed. You will agree working arrangements, transfer to another department or have your duties adjusted as necessary. As part of this, the circumstances of both the line manager and the relevant employee will be considered.

Undesirable personal contacts

Employees have a right to respect for their private lives and freedom of association. However, this right should not be detrimental to your performance or the proper functioning of the AFM. Personal contacts could be harmful and compromise your integrity and that of the AFM. The extent of the impact will depend on your role and the circumstances.

The risk of image problems as a result of damaging personal contacts will be greater for some roles than for others. This depends on the nature of your duties, your visibility to the outside world and your position within the AFM.

Undesirable personal contacts are understood to refer to individuals regarding whom you know or ought to know that they are in breach of standards and legislation to a greater or lesser extent. Also included is membership of an organisation that regularly gives cause for scandal or discussion, for example as a result of criminal activity or vandalism, even if the association itself is not illegal. If you suspect that a personal contact or membership could be deemed undesirable, please speak to your line manager or a confidential counsellor. Being open means that measures can be put in place to protect you and the AFM, should this be necessary.

4.6 Communication

Each citizen has the right to freedom of expression. Although this right also applies to you, there are limitations in connection with your work at the AFM. Think carefully before openly giving a personal opinion. You cannot simply write, say or post anything you like.

Basic principles

Apply these basic principles when communicating privately or for work purposes:

- Recognise at all times that you are part of the AFM;
- Always comply with your duty of confidentiality;
- Be courteous and respectful in your communications;
- Do not make any statements that would harm your performance or the functioning of the AFM.

The exact interpretation of these basic principles will depend on your role and your involvement with whatever topic is at hand. Context matters too, such as the topicality and sensitivity of an issue and the time and manner of your statement.
Be aware that the AFM may challenge you about statements you have made, including those made in a personal capacity. In other words, always consider any possible consequences of your actions.

External contacts

The AFM's goal is to be transparent towards society. This could mean you will have regular dealings with external contacts. You must bear in mind that you are a representative of the AFM in those instances and contacts will consider you the face of the AFM.

Media

Be particularly vigilant in any dealings with the media. Contacts with the media should be handled via the Communications department. Do not speak to journalists yourself unless this department has granted permission. If you are contacted directly by a journalist, refer them to the Communications department and notify the department about this.

Public bodies

Dealings with public bodies such as the Ministry of Finance and the House of Representatives are to be conducted through your colleagues at the Strategy, Policy and International Affairs department. If you are approached by a public body or need to get in touch yourself, please liaise with Strategy, Policy and International Affairs.

Be vigilant when communicating online

You must be particularly vigilant when communicating online, whether for work or private purposes. Online communications are quick, immediate and can reach a wide audience, which means there are additional risks you cannot always anticipate. Make sure your communications are careful, targeted and measured. Consider the medium you are using and keep a close eye on the dividing line between personal and work-related matters. Take extra care when communicating online:

- Your identity is easy to trace.
- Posts can spread quickly and widely, whether this is your intention or not.
- Posts are out there forever and can always resurface.
- Whether you intend or not, you could put people in the public eye against their will.

4.7 Privacy management

The aim of the AFM is set the right example when it comes to protecting personal data. In light of this, we ask that you use due care in this regard when carrying out your duties. Ensure you are familiar with the statutory and regulatory requirements, as well as our own privacy policy. You must also follow our privacy regulations at all times. If you think an exception is necessary, please talk to one of our specialists first. These are the privacy coordinator for your department, the data protection lawyers in the Legal Affairs department or the Data Protection Officer. Always be transparent about what you are doing and keep a written record.

Processing of personal data

Employees who handle personal data must do so in a careful and confidential manner. Ask one of our specialists whether a Data Protection Impact Assessment (DPIA) must precede specific processing activities. Processing activities involving personal data must be based on a legal ground in accordance with the General Data Protection Regulation. In addition, personal data can only be used for the purpose and period for which they were obtained. Always ensure personal data are processed in line with our own privacy policy and privacy regulations.

Obtain advice

The AFM can draw on a great deal of in-house knowledge in the field of privacy. If you are in any doubt at all, please refer to one of the specialists listed previously – the privacy coordinator for

your department, the data protection lawyers in the Legal Affairs department or the Data Protection Officer. See the internal AFM privacy page for all information on privacy at the AFM.

Report data breaches or security incidents

Protecting personal data also means that you must immediately report actual or suspected data breaches or security incidents to your line manager and our helpdesk. Also, make them aware of any email you suspect to be a phishing attempt. One way in which you can recognise these is their context – does the message include strange links or words? Do not click suspicious links and delete suspicious emails immediately. Always submit a report, even if you are not sure. Find out more about this in the Mandatory Reporting of Data Breaches Guideline.

A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data. Examples are when a laptop or bag containing documents is lost or stolen, or an email is sent to an incorrect recipient. Instances in which personal data are lost and no back up exists also constitute a data breach.

5. Prevention and enforcement

5.1 Reliability systematically tested

Role-based screening

At the AFM, integrity never comes second. Integrity comes into play as soon as you apply for a role and begin to undertake work for the AFM. There is no question that you should be honest when providing information and ensure there are no omissions. Failure to do so could result in termination of your employment or contract in future. New employees will complete a screening that will vary according to the category of worker. A screening might also be required if you decide to apply internally for an integrity-sensitive position (see Appendix 4).

The rules after you have begun your duties

Once you take up your role or are carrying out external duties, you will still need to inform the AFM correctly and in full regarding any issues that constitute grounds for you to undergo a new reliability screening. These include criminal, tax, administrative or financial matters. If an antecedent that constitutes an integrity violation is discovered during a re-assessment of your integrity and you have failed to report it in a timely manner, this can be considered an aggravating circumstance. You can find out more about the antecedents and how they are weighed in Appendix 4.

Taking the oath or making the solemn affirmation

When you take up employment with the AFM, you will take an oath or make a solemn affirmation. This is a spoken acknowledgement that you understand what it means to be a civil servant and that you will conduct yourself accordingly. The oath or solemn affirmation confirms the standards that apply and is based on the following principle: taking the oath or swearing the solemn affirmation does not make people credible; rather, it is people who need to make the oath or solemn affirmation credible.

Confidential counsellors

The AFM has appointed a number of confidential counsellors. You can approach them if you want to ask questions about integrity, have identified an integrity risk or breach, or have another matter you wish to discuss in confidence. Confidential counsellors will listen to you in confidence and provide advice and information. They are independent, practice due care and will not take any action without your consent. The responsibility of a confidential counsellor is to advise employees on the appropriate channel for submitting a report to the compliance officer. At the employee's request and with their express consent, a confidential counsellor can pass a report to the compliance officer on the employee's behalf. When submitting a report via the confidential counsellor, reporting individuals can remain anonymous if they wish.

5.2 Suspected or actual abuses and integrity violations

Requirements to report

You have a duty to report any suspected or actual abuse (see box) or integrity violations that you come across. This will not always be easy, in particular if you have any direct or indirect involvement yourself, or if an abuse or breach concerns you. The AFM wants to promote a culture of openness around mistakes. This means we wish to take mistakes as opportunities for

learning. However, that does not mean abuses or integrity violations should remain without consequences.

What does abuse, an integrity violation or an antecedent mean?

Incidents could be of relevance for the integrity and reliability of the AFM and its employees. Incidents are subdivided into abuses and integrity violations.

Abuse is understood to mean a serious incident that puts the public at stake. This is in line with the definition of abuse in the Dutch House for Whistleblowers Act (Dutch: Wet Huis voor klokkenluiders): "abuses that violate a statutory requirement and put the interests of society at risk or pose a threat to public health, a threat to the safety of individuals, a risk of damage to the environment, or a threat to the proper functioning of the public service or a company, as a result of an improper course of conduct or failure to act".

An integrity violation refers to an incident in which the actions of employees constitute a violation of internal and/or external laws and regulations, or are otherwise contrary to the standards and values of the AFM. In these cases, the employee's integrity might be compromised. Compared with abuse, the difference is that an integrity violation does not, or has not yet; put the interests of society at stake.

Integrity violations that have resulted in sanctions might count as an antecedent for the employees involved.

Reporting

You are able to submit a report in writing or verbally, either to your line manager or the compliance officer. Your line manager will pass the report on to the compliance officer as soon as possible, and the compliance officer will then decide whether the report will be considered. If the incident involves your line manager, you can submit a report to the compliance officer or the most senior line manager. If you are unsure whether you should submit a report, you can also ask a confidential counsellor for advice (see box). If there is a reason not to submit a report to a line manager or compliance officer, the following options are open to you:

- You can ask a confidential counsellor to submit a report on your behalf.
- You can submit an anonymous report to the compliance officer through a third party. This is preferable to anonymous reports that are not submitted through an intermediary, as use of an intermediary offers the option to request additional information. Anonymous reports must be sufficiently specific and serious. If not, the compliance officer may decide not to investigate.
- You can turn to the Dutch Whistleblowers Authority (Huis voor Klokkenluiders). They not only offer advice but can also support you when submitting your report.

You should preferably submit your report internally. This is because the primary responsibility for addressing a breach or abuse rests with the AFM. However, as the previous section indicates, you can also submit a report externally. Instances in which this might be appropriate include the following: there is immediate danger, you cannot reasonably be expected to submit a report internally, and you fear retaliation might follow if you were to use internal channels or there is a clear threat of concealment or destruction of evidence.

Protection for individuals making a report in good faith
If you have reported abuse or an integrity breach, you should not be unfairly disadvantaged because of your report. However, your suspicion that an incident has occurred should be based on reasonable grounds. You do not necessarily need to have evidence but you must be able to provide some justification based on documents or observations you have made.

You can expect the AFM to treat your report with due care. Confidentiality will be our main priority. All parties involved will treat information regarding the report confidentially and with the utmost care. The compliance officer will ensure that the information can only be accessed by employees involved in the handling of the report. These employees will be duty-bound to keep the identity of the reporting individual and the accused confidential. The identity of the reporting individual cannot be disclosed unless this individual has given express written permission to do so. Further details on the legal protection of reporting individuals and other involved parties are outlined in Appendix 5 – Reporting scheme for actual and suspected abuses and integrity breaches.

5.3 Investigations and sanctions

Test
A report could prompt an investigation to establish the facts. In the course of this, all parties will be heard, careful records will be kept and proportionate investigative means will be used as relevant. An investigation may consist of an interview, conducting or ordering an examination of the operational resources used, and a body search and search of clothes. The latter will depend on the gravity of the facts and circumstances and be subject to Section 11 of the Central and Local Government Personnel Act (Ambtenarenwet).

Review of the gravity of a breach
If you are found to be in breach of an integrity rule, there might be consequences, the exact nature of which will depend on the circumstances. In addition to the gravity and duration of the breach, consideration will also be given to the level of culpability, attitude and role of the employee, and the extent to which they act as a role model. Mitigating and aggravating circumstances will also be taken into account. For example, the fact that line managers fulfil an exemplary role is considered an aggravating circumstance. This means that if a line manager committed an integrity breach, this may be given greater weight in the assessment and a more serious measure could be imposed than for a breach committed by an employee.

Following a careful assessment of the facts and circumstances, it will be determined on a case-by-case basis whether a measure will be imposed and if so, which one. A range of more or less serious measures exists, from an instructive conversation regarding standards up to and including dismissal.

Occupation
If you do not agree with a measure that has been imposed, you have the option to appeal. For less serious measures, you can direct your appeal to the Executive Board, and for measures that are more serious this is the Supervisory Board. You must set out in writing why you disagree with the measure and send your motivation to the secretary for the Executive Board or the secretary for the Supervisory Board as relevant. This officer will then ensure your appeal is reviewed. Once you have made your submission to the secretary, the chair of the Executive Board or the

Supervisory Board will issue a decision to you within four weeks. After the appeal procedure, you can also decide to launch legal proceedings in order to seek termination of the measure.

If the AFM considers there are grounds to terminate your employment contract, the AFM will request the district court to set aside the employment contract or issue a permit to give notice. If the district court grants the request, your employment contract will be terminated. In all other cases, it will be up to the chair of the Executive Board or the Supervisory Board to decide whether to impose a measure under employment law.

Appendix 6 tells you more about how the AFM deals with breaches of integrity rules, what possible consequences breaches can have and what the appeal procedure looks like.

Appendix 1: Definitions and explanations

The following definitions apply to the terms used in these regulations:

Activity:
An ancillary position or ancillary activity, which the employee currently undertakes, has undertaken or wishes to undertake during or after their duties for the AFM. Excluded from this are activities arising from the responsibilities or work of the AFM, which employees perform by virtue of their role or exclusively perform by virtue of their role with the AFM.

Antecedent:
A violation or integrity violation that has resulted in the imposition of a measure and/or sanction. In screenings for employees, a distinction is made between five categories of antecedents:

- Criminal antecedents;
- Financial antecedents;
- Fiscal and administrative antecedents;
- Other antecedents, including conflicts in the workplace or disciplinary measures.

BAS:
Bedrijfsvoering AFM Selfservice is the software used by the AFM to support and enable the digital processing of various administrative operational processes.

Accused:
The individual against whom a complaint has been made.

Conflict of interests:

- This arises when an employee has a personal interest or
- A role-based interest (conflict of duty) as a result of ancillary or other positions or duties, And should therefore be deemed incapable of safeguarding the interest of the AFM with integrity and free from prejudice.

Invest:
The execution of private investment transactions for the purpose of acquiring or disposing of financial instruments (see the definition of financial instruments), or arranging for the execution thereof.

Collective investment scheme:
An investment fund, investment firm or undertaking for collective investment in transferable securities (abbreviation: ICBE) as referred to in Section 1(1) of the Financial Supervision Act.

ICBE (Undertaking for Collective Investment in Transferable Securities):
A fund or firm as referred to in Section 1(1) of the Financial Supervision Act.

Rights issue:
A rights issue is an issue, which gives existing shareholders preferential rights over new shareholders when subscribing to the rights issue.

Compliance file:
All employees have a compliance file, which is maintained in BAS and the compliance officers' directory. The file contains all the information provided by the employee regarding ancillary activities, private investments, disclosed gifts and, where applicable, any comments made by the compliance officer. Compliance officers and the relevant employee can only access the file.

Compliance officer:
An employee in the Compliance, Integrity & Risk Management (CIR) department tasked with the internal supervision of compliance with the Code of Conduct.

Data breach:
A data breach is understood to mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data.

Dilemma:
This always means a conflict between different values. For that reason, there is no "right" answer in a dilemma. You will always go against one or more values. However, the fact that there is no "right" answer does not mean that you cannot have a discussion or that some solutions would be better than others would.

Financial instrument:
A financial instrument as referred to in Section 1(1) of the Financial Supervision Act Examples include securities, money-market instruments, rights of participation in a collective investment scheme or UCITS and similar.

Data Protection Officer:
The Data Protection Officer is responsible for independently supervising the implementation of and compliance with the GDPR, as well as monitoring the internal privacy policy.

Related third party:
- A spouse or partner;
- Relatives by blood or by marriage to the second degree in relation to the employee;
- Persons with whom the employee runs a joint household (other than those listed above).

Regulated market:
A regulated market as referred to in Section 1(1) of the Financial Supervision Act.

Closed list:
The list of undertakings and/or financial instruments in respect of which the AFM currently possesses inside information.

Insider:
An employee who has been designated an insider in BAS following registration as such by a project manager and/or compliance officer.

Integrity violation:
A breach of internal and/or external laws, regulations or core values, which could compromise the integrity of the employee. Integrity violations can take many forms, including: inappropriate conduct in matters related to the AFM, leaks of confidential information, theft, embezzlement,

corruption, manipulation or misuse of information or access to information, wastage and misuse of AFM assets, use of (physical) violence, threats, intimidation and any other misconduct, whether punishable by law or not, conflicts of interests, incompatible positions, contacts or activities, or fraud. This list is intended to give an indication of matters that could constitute an integrity violation under the Code of Conduct and is not exhaustive.

Complaints Committee:

An internal committee as referred to in Appendix 6, section 1.2, which is made up of a compliance officer, the general counsel and a confidential counsellor.

Complainant:

The individual who has approached the confidential counsellor or submitted a complaint to the Complaints Committee regarding undesirable behaviour.

Employee:

- Anyone who has an employment contract with the AFM;
- Anyone who carries out work for the AFM on a regular basis or is seconded to the AFM, such as external consultants, placement students and agency and temporary workers;
- The members of the AFM Supervisory Board;
- Anyone who does not come under any of the above categories but who, for the purpose of these Regulations, has been designated an employee by the compliance officer.

Suspected abuse:

A suspicion held by an employee that a situation of abuse exists within the AFM, whereby:

a. The suspicion is based on reasonable grounds and has arisen from knowledge that the employee has gained at the AFM;
b. A violation of a statutory requirement has occurred which puts the interests of society at risk or which poses a threat to public health, a threat to the safety of individuals, a risk of damage to the environment, or a threat to the proper functioning of the public service or a company as a result of an improper course of conduct or failure to act.

Multilateral Trading Facility (MTF):

A multilateral trading facility as referred to in Section 1(1) of the Financial Supervision Act.

Company subject to supervision:

Institutes, individuals or legal entities who are monitored by the AFM for compliance with the rules laid down by or pursuant to the Financial Supervision Act (Wft), the Money Laundering and Terrorist Financing (Prevention) Act (Wwft), the Financial Reporting (Supervision) Act (Wtfv), the Audit Firms (Supervision) Act (Wta) and the Consumer Protection (Enforcement) Act, also including the European regulations supervised by the AFM by virtue of the EU Financial Markets Regulations (Implementation) Decree.

Organised Trading Facility (OTF):

An organised trading facility as referred to in Section 1(1) of the Financial Supervision

Act.Undesirable behaviour:

- Discrimination: judging individuals based on their race, colour of their skin, descent, national or ethnic origin, gender or sexual orientation;
- Aggression and violence: mental or physical harassment, threats or attacks;
- Bullying: conduct that is perceived to be hostile, humiliating or intimidating, and which is directed at the same individual each time (mocking an individual or making it unpleasant or even impossible for an individual to carry out their work);
- Sexual harassment: unwanted sexual advances, requests for sexual favours or any other verbal, non-verbal or physical behaviour of a sexual nature.

Pre-clearance:

A request for permission from the compliance officer prior to the execution or arranging the execution of a private investment transaction.

Private investment transaction:

A transaction in a financial instrument for one's own account or for the account of a third party, either in part or in full, and which is performed other than in the execution of a role or position. The acquisition of a financial instrument by any other means, such as by way of a gift, is also deemed to constitute a private investment transaction.

Conflicting interest:

A scenario in which the personal interests of an employee could influence or appear to influence the impartial and objective execution of their duties.

Tipping off:

The disclosure of inside information to any other person, except where such a disclosure is made in the normal exercise of one's duties, profession or role.

Transaction:

An agreement for the exchange of items or rights, which involves the AFM.

Benefits:

Gifts, discounts, vouchers, hospitality (such as lunches, dinners, travel expenses and hotel accommodation) and other favours.

Inside information:

Information that is specific, has not been made public, directly or indirectly relates to one or more issuers or one or more financial instruments such as shares or bonds and which, if disclosed, could have a significant impact on the price of those financial instruments and/or the price of related derivative financial instruments.

Discretionary management agreement:

The execution or arranging of the execution of private investment transactions in financial instruments based on a written management agreement to that effect, concluded with an asset manager who has full discretionary power.

Work instructions for updating the closed list:

These work instructions describe when an institute or a financial instrument is placed on the closed list.

Appendix 2A: Private investments regulations

AFM employees are able to make private investments subject to conditions and restrictions that are aimed at preventing insider trading or the appearance of insider trading. In this regard, the AFM seeks maximum alignment with the prohibition on insider trading set out in EU Regulation no. 596/2104 (the Market Abuse Regulation or MAR). Insider trading interferes with the fair and efficient operation of capital markets, and has the potential to greatly damage the integrity and reputation of the AFM and its employees.

You are required to make an immediate disclosure to the compliance officer in the event that:

- You have failed to comply, whether in part or in full, with a provision in these Private Investments Regulations (the "Regulations") (this also applies when executing an investment transaction for the account of a third party); and/or
- A related third party has carried out private investment transactions in which you hold an interest and which relate to financial instruments admitted for trading via a regulated market, MTF or OTF active in Netherlands.

Execution of private investment transactions:

1. Prohibition

1.1. The prohibition of insider trading is applicable to all. This means AFM employees are not permitted to use inside information when carrying out private investment transactions and must avoid giving the appearance of insider trading. In addition to insider trading, the prohibition also covers tipping off and recommending or inducing others to engage in insider trading. In the event that an employee has inside information because of their professional capacity, the relevant issuer or financial instrument will need to be registered in accordance with the Work instructions for updating the closed list.

1.2. Irrespective of whether they possess actual inside information, employees are not permitted to carry out private investment transactions in relation to financial instruments admitted for trading via a regulated market, MTF or OTF active in Netherlands. The same applies to all derivative products based on these financial instruments. The market abuse and Wft supervision investigations the AFM conducts into issuers or collective investment schemes mean that inside information can be available regarding a formal measure to be taken by the AFM, which if released by the AFM, could influence the price of the associated financial instruments. The prohibition stipulated in the first full sentence only applies to financial instruments of issuers that are required to disclose inside information. This means there is an obligation on the issuer to fulfil the requirement in the MAR that inside information directly relating to the issuer must be made public as soon as possible. Not all issuers whose financial instruments have been admitted for trading or are traded via a regulated market, MTF or OTF are subject to an obligation to disclose inside information. This obligation only applies to the extent that the issuer has agreed to the admission or trading of their instruments. Use the AFM license registers to establish whether you are dealing with a regulated market, MTF or OTF.

1.3. Employees are forbidden from using a third party in order to circumvent the requirements in these Regulations and from recommending forbidden investments to third parties. Among other things, this means employees are not permitted to execute or arrange for the execution of private investment transactions in companies subject to supervision through their spouse or children, or

to issue specific instructions to asset managers to acquire or divest particular financial instruments when the regulations prohibit private investment transactions in those instruments. Nor is it permitted to make investments for the account of third parties (e.g. on behalf of a parent or sports association) or recommend specific investments in relation to financial instruments admitted for trading via a regulated market, MTF or OTF active in Netherlands.

Concerning the persons with whom the employee runs a joint household, the employee is required to use best efforts to ensure that these individuals do not execute private investment transactions in relation to financial instruments admitted for trading via a regulated market, MTF or OTF active in Netherlands. Employees will be bound by their duty of confidentiality, at all times.

2. What is permitted

2.1. Employees will be able to execute the private investment transactions listed below without requiring pre-clearance by the compliance officer:

- Acquiring or divesting bond or money-market instruments issued by central or local government bodies;
- Acquiring or divesting units in a collective investment scheme or UCITS not listed in the Netherlands or not managed by a company subject to supervision by the AFM;
- Acquiring or divesting derivative products (including derivatives and turbos) that are not listed in the Netherlands, that are not issued by a company subject to supervision by the AFM and whose underlying values consist of:
  - commodities;
  - currencies;
  - interest rates;
  - indices (with the exception of indices of companies subject to supervision).

Please visit afm.nl for a list of investment firms and UCITS's that are subject to supervision.

2.2. Employees are permitted to make investments under discretionary management agreements or in order to build up capital for a pension, mortgage or similar provision. This requires the compliance officer to review and approve the discretionary management agreement or agreement aimed at capital build-up for a pension, mortgage or similar provision in advance.

The agreement must attest to the following:

- The employee will have no influence over the underlying investment policy that is pursued or the investment choices to be made by the manager or administrator (ownership and manager must be strictly separated); There will be no prior consultation between the asset manager and the employee and/or the related third party regarding the investment transactions to be executed;
- The employee has the option to issue generally worded policy instructions to the asset manager, for example in relation to the portfolio mix policy for financial instruments to be managed by the asset manager, by type, geographic origin or industry. These general policy instructions must be included in the agreement and cannot be changed more frequently than once every six months; The employee must obtain prior approval (pre-clearance) from the compliance officer for amendment or termination of the management agreement.

2.3. Following pre-clearance, employees will be able to execute the private investment transactions listed below:

- Acquiring or divesting marketable shares, bonds or money-market instruments that are not listed on a regulated market in the Netherlands and that have not been issued by a company subject to supervision by the AFM;
- Acquiring or divesting units in a collective investment scheme or UCITS that are listed in the Netherlands or managed by a company subject to supervision by the AFM;
- Acquiring or divesting derivative products (including derivatives and turbos) that are not listed in the Netherlands, that are not issued by a company subject to supervision by the AFM and whose underlying values consist of:
  - commodities;
  - currencies;
  - interest rates;
  - indices (including indices of companies subject to supervision);
  - marketable shares, bonds or money-market instruments that are not listed in the Netherlands and that have not been issued by a company subject to supervision by the AFM.

Once they have received pre-clearance, employees are able to accept optional dividends (cash or dividends in the form of shares).

Once the compliance officer has granted clearance, the employee must issue the instruction for execution within one hour. If this cannot be achieved, for whatever reason, the employee must request prior clearance once more.

Please visit afm.nl for a list of investment firms and UCITS's that are subject to supervision.

3. Prevention of conflicts of interest for members of the Executive Board and the Supervisory Board

3.1. These Regulations apply to each member of the Executive Board and the Supervisory Board, subject to the exemptions, which have received separate, prior approval from the compliance officer.

3.2. The transitional arrangement set out in section 7 does not apply to members of the Executive Board and the Supervisory Board. Instead:

a. Proposed directors for the Executive Board or the Supervisory Board must disclose their direct or indirect private investments to the compliance officer before they are nominated, appointed or re-appointed. In these provisions, indirect private investments are understood to mean the private investments of third parties related to the member of the Executive Board or the Supervisory Board. The relevant private investments will be subject to a binding decision by the compliance officer as regards their acceptability.

   In the event that the compliance officer determines in this binding decision that certain private investments are not acceptable, the decision will in any event mean that:
   - The private investments must be divested before appointment to the Executive Board or the Supervisory Board; or

- The private investments must be placed under a discretionary management arrangement in accordance with section 2.2 for the duration of the membership of the Executive Board or the Supervisory Board; or
- During membership of the Executive Board or the Supervisory Board, it will not be permitted to execute transactions in relation to the relevant private investments;

b. Members of the Executive Board or the Supervisory Board who acquire a private investment after their appointment or re-appointment, for example by way of inheritance or as a gift, must report this to the compliance officer immediately. The compliance officer will then issue a binding decision in respect of these private investments. In this decision, the relevant member of the Executive Board or the Supervisory Board will be given a reasonable period of time to comply with the compliance officer's decision.

3.3. In order to avoid any potential or apparent conflict of interests, members of the Executive Board or the Supervisory Board cannot have any direct or indirect personal financial interests that are incompatible with membership of the AFM Executive Board or the AFM Supervisory Board. In these provisions, indirect financial interests are understood to mean the personal interests of third parties related to the member of the Executive Board or the Supervisory Board.

Direct or indirect financial interests will be incompatible with membership of the AFM Executive Board or the AFM Supervisory Board if they could result in any actual or apparent conflict of interests and/or be harmful to the integrity, performance or reputation of the current or prospective relevant member of the Executive Board or Supervisory Board, or that of the AFM.

3.4. In the event of a difference of opinion with the compliance officer regarding the interpretation and application of these Regulations, members of the Executive Board or Supervisory Board may refer the matter to the general counsel or the chair of the AFM Executive Board; see also section 9.

4. Provision of information

Employees must register any investment accounts in BAS as soon as they enter service and/or open an investment account. As part of this, employees must provide:

- An up-to-date portfolio overview of portfolios held in their own name or in the name of any under-age children, any joint and/or investment accounts with their partner, any endowment mortgages, supplementary pension schemes with an investment element, investor insurance policies and portfolio under discretionary management;
- The discretionary management agreement and a signed copy in the event of any changes to this in the interim.

At the compliance officer's request, employees are obliged to:

- Provide all information relating to private transactions executed on their behalf and for their account;
- Issue instructions to a bank, asset manager, collective investment scheme, broker or (related) third party, to provide the compliance officer with all relevant information regarding private transactions conducted by or for the employee.

5. General provisions

5.1. Compliance monitoring

The compliance officer has the authority to start an investigation concerning compliance with these provisions, and is empowered to establish and report on the findings resulting from this investigation. The compliance officer will report directly to the chair of the AFM Executive Board. If the investigation concerns a member of the Executive Board or the Supervisory Board, the compliance officer will report directly to the chair of the Supervisory Board. If the investigation concerns the chair of the Supervisory Board, the compliance officer will report directly to the vice chair of the Supervisory Board. Both when the compliance officer is required to report to the chair or vice chair of the Supervisory Board, the compliance officer will also inform the chair of the Executive Board regarding the investigation.

The employee in question will in all cases be notified of the outcome of the investigation. Before the compliance officer reports in writing about the findings of the investigation, the findings must be notified to the employee and the employee must have been given an opportunity to respond to the findings of the investigation.

5.2. Privacy

Personal data processing in connection with the provisions in these Regulations will be carried out in accordance with the guidance provided in the General Data Protection Regulation (GDPR) and other applicable laws and regulations, and will be retained in accordance with the AFM data retention policy. More information about the employee's privacy rights under the GDPR have been included in the internal privacy regulations for AFM employees.

6. Exemption authority of the compliance officer

The compliance officer may, in case of special personal or financial circumstances, or in the event of special procedures, grant exemption from specific provisions of these Regulations. This exemption may be subject to requirements and restrictions.

The exemption authority covers special circumstances, which involve financial instruments, such as:

- Entering into or dissolution of a marriage or registered partnership (division of the property);
- Inheritance or acquisition from a gift or endowment;
- Termination of a mortgage or insurance contract with an investment element.
- Employees who have served more than three years in the permanent employment of the AFM may ask the compliance officer to sell their entire investment portfolio at a time to be determined by the compliance officer.

The special procedures also cover, for example, repetitive deposits for private transactions, personnel arrangements, rights issues or public takeover bids. In specific circumstances, this could entail the execution of certain future transactions, which an employee cannot be aware of at the time the exemption is obtained.

In the cases listed above, financial instruments can come into the possession of or must be divested by an employee, for example due to marriage or divorce, or receiving an inheritance, while in principle this is not permitted under the prohibition clauses. Employees should submit these scenarios to the compliance officer in advance whenever possible.

How does it work?
The employee submits a request to the compliance officer for approval in respect of a matter eligible for exemption. This request must describe the matter for which exemption is being requested and include all information that the compliance officer requires in order to assess the request, such as an up-to-date overview of the relevant portfolio, the name of the issuer and similar. If the outcome of the assessment is positive, the employee will receive approval in an email in which the compliance officer will also outline any applicable conditions. If the employee accepts these conditions, he or she must indicate agreement in a reply to this email.

7. Transitional arrangement

New employees who possess prohibited financial instruments as referred to in section 1 before they take up employment with the AFM, have the option to sell these financial instruments within 12 months. In order to do so, the employee will need the compliance officer to grant pre-clearance.

Once the 12-month period has elapsed, the employee will no longer be permitted to reduce the positions referred to above. The employee will not be permitted to execute transactions in these financial instruments again until six months after leaving the AFM's employment.

8. Sanctions and appeal against sanctions[1]

Acting in violation of these Regulations can be deemed a serious breach of the trust that the AFM must be able to have in its employees, and on that basis can lead to one or more appropriate sanctions. Sanctions may include an entry in the employee's compliance file, reassignment, suspension and termination of service. In the event that a violation qualifies as an offence, the Executive Board or, if a member of the Executive Board is involved, the chair of the Supervisory Board may decide to notify the competent authorities in criminal matters. The nature of the offence will determine what sanction is imposed.

With regard to employees who are not members of the Executive Board, more serious sanctions such as reassignment, suspension and other disciplinary or employment measures – including summary dismissal – can only be imposed by the Executive Board and this either with or without a recommendation by the compliance officer. The authority to suspend or dismiss members of the Executive Board or Supervisory Board is vested in the Minister of Finance.

In order to establish which sanction should be taken, the nature of the violation will be assessed using a number of criteria. To determine the difference between a minor and a serious violation, consideration is given to criteria including:

- Was the violation committed knowingly or unknowingly?
- Was inside information used or not?
- Is this a repeat offence?
- Is the employee transparent and did he or she cooperate with the investigation?

If, for example, when buying a house, an employee forgot to notify the compliance officer in advance about the fact their mortgage has an investment component, this will initially be classified as a minor violation. However, if it is also found that the employee used inside information when setting up the investment component of this mortgage, or that they intentionally withheld the mortgage offer, the same offence will be classified as a serious violation

[1] Also refer to the Regulations on integrity investigations and sanctions.

by the compliance officer and will be submitted to the Executive Board or Supervisory Board. The Executive Board or the Supervisory Board will make a final decision for more serious violations, and can deviate in its decision from the recommendation made by the compliance officer. The employee will always be heard before a sanction is imposed.

In the event that the employee's compliance file contains several entries (depending the nature of the violations), the compliance officer may propose to HR that an entry about this is added to the employee's personnel file. The employee will be informed of this in advance. This may then have consequences for employees when they go for a job interview with another employer, if this employer conducts a reference check.

Every employee other than a member of the Executive Board is able to lodge an appeal against the imposed sanction with the chair of the Supervisory Board.

9. Binding ruling by the compliance officer and appeal

A decision taken by the compliance officer or a ruling made by this officer regarding a request from an employee under these provisions for pre-clearance or an exemption is binding on the employee concerned.

Employees, including members of the Executive Board, can appeal to the chair of the AFM Supervisory Board against the compliance officer's decision or ruling. Members of the Supervisory Board are entitled to lodge an appeal with the chair of the AFM Executive Board. The appeal has no suspensive effect on the decision or ruling of the compliance officer.

10. Residual powers

In all cases not provided for in these Regulations with respect to employees other than members of the Executive Board, a member of the Executive Board is empowered to adjudicate, issue instructions and, in this context, take certain measures. With respect to members of the Executive Board or Supervisory Board, this authority rests with the chair of the Supervisory Board or, if the case concerns the chair of the Supervisory Board, the vice chair of the Supervisory Board.

11. Applicability and entry into force of these regulations

These regulations were revised in a number of respects and will enter into force on 1 January 2021. These regulations apply to all employees and constitute an integral part of the employment contract or other contract between the AFM and the employee. In the event of conflicts between these regulations and the applicable employment contract or other contract, these regulations will prevail. These regulations also apply to former employees until six months after leaving the employment of the AFM.

Appendix 2B: Work instructions for updating the closed list

If you wish to carry out private investment transactions, you will in most cases need the compliance officer to provide pre-clearance. The compliance officer will check the intended transaction against a list of companies and/or financial instruments[2] in relation to which the AFM currently possesses inside information. This list is known as the closed list. To able to establish and maintain this list, the compliance officer relies on those employees who possess such information because of their supervisory activities at the AFM. The compliance officer is responsible for keeping the closed list up to date, using information provided by the departments.

This work instruction describes how to report inside information.

1. What is inside information?

Inside information is:

- non-public information
- that is specific, and
- directly or indirectly relates to one or issuers or one or more financial instruments (such as shares or bonds), and
- which, if made public, could have a significant impact on the price of those financial instruments and/or the price of related derivative financial instruments.

This could include information related to companies subject to supervision (such as changes to a board), their customers (such as issues or takeovers), business customers of the AFM (e.g. in relation to tenders) and information obtained from other supervisory authorities (such as information on developments in interest rates). See paragraph 5 for a number of examples of inside information.

2. Who should disclose inside information and when?

Any employee who possesses inside information because of their work must, either individually or collectively when working on investigations or projects as part of a team, ensure such information is promptly added and removed under the Closed List section in BAS.

Employees are not required to report any inside information that is resolved in the course of the same day because of the notification being made public by the AFM (as would be the case for material notifications, for example).

When adding or removing entries from the list, it is necessary to indicate the specific reason for doing so. It is also preferable that clear agreements are put in place at departmental, team or project level regarding the persons responsible for adding or removing entries from the list. A company may be added to and removed from the list by several departments, teams or projects in relation to different topics. When transferring a file, it will be up to the departments, teams or projects themselves to ensure proper arrangements are in place for addition to and removal from the list.

[2] This could be relevant for product interventions that entail a ban on a particular financial instrument. If this is the case, please contact the compliance officer immediately.

3. When is removal of an entry permitted?

Companies are removed from the closed list once the AFM can no longer be considered to be possession of inside information. Please also refer to the arrangements put in place within each department.

Examples:

- The undertaking has made an announcement to the market so that the AFM no longer has an informational advantage;
- The imposition of a fine has been communicated externally.

4. Roles and responsibilities

Files must always be added to or removed from the closed list using BAS. So who has responsibility for what? To identify this, the AFM distinguishes between the following scenarios:

1. New entry:
   - The responsible colleague within the department, team or project adds the company to the list using BAS. This could be the file coordinator or project manager.
2. Standard removal:
   - The colleague who added the company uses BAS to remove the company.
3. Transfer to a different department or the Penal Fines Officer:
   - The colleague who listed the company uses BAS to indicate which new colleague will take over this responsibility.
4. Removal following a transfer:
   - The newly designated responsible colleague uses BAS to remove the company.

The remaining steps in the procedure for working with the closed list are outlined in the RACI table below.

RACI for activities related to the closed list

	(transferring/ receiving) employee	(transferring/ receiving) line manager	compliance Officer	IM
Identify:				
• Keep an eye out for inside information (in daily practise)	R	A	I	
• Establish whether a specific file might contain inside information	R	A	C	
Mitigate:				
• Add institute or financial instrument to closed list	R	A	C	
• Assess entries for closed list	I		A	
• Prevent unnecessary sharing of information regarding the file	R	A	C	I
Transfer of the file:				
• Be alert when file is transferred	R	A	I	
To another colleague:				
- Indicate the name of the receiving employee BAS	R	A	I	
- Prevent unnecessary sharing of information regarding the file	R	A	C	I
Close:				
• Remove institute or financial instrument from the closed list	R	A	C	
Manage:				
• Keep the closed list up to date	R		A	
• Keep system for closed list up and running			I	A

5. Voorbeelden van voorwetenschap

In order to support you, the following contains a list of facts and circumstances that could constitute inside information. Inside information includes, among other things, full or partial knowledge of the substance of any information that has yet to made public in relation to topics such as those listed below. This list of possible inside information, which is not exhaustive, is intended as a guide to help you make your own critical assessment of whether any information constitutes inside information. The compliance officer is always available to advise you about this.

- The fact that an investigation is launched into a company subject to supervision could already be considered inside information. This is because the sensitivity of the investigation could have a significant impact on the share price of the company in question. The mere existence of a file or investigative file at the AFM can constitute sufficient reason to designate the launch (which could ultimately result in the publication of a penalty) as inside information.

- Key information on the company's performance;
  - reporting of periodic financial results in annual reports, half-yearly reports, quarterly reports or trading updates;
  - key information that could impact on the results, turnover or any forecast published previously;
  - new forecasts or material deviations from previously issued forecasts regarding the development of the operating result or turnover;
  - significant extraordinary income and expenditure, such as a book profit on assets to be sold or a write-off of goodwill paid on the acquisition of a company;
  - significant change in the regime for financial reporting;

- Key information regarding the financing of the company;
  - significant changes in loans and guarantees provided under loans;
  - breaking of a covenant
  - cancellation of key credit facilities by one or more banks;
  - negative equity;
  - suspension of own purchasing obligations by collective investment schemes;

- New information regarding capital, control or organisation
  - significant changes in the distribution of share ownership in the company, such as the acquisition of a substantial interest in the company by a competitor;
  - adoption of a decision to buy back own shares;
  - arrangement or implementation of protective measures;
  - significant changes in the legal or organisational structure, or approval of plans to that effect;
  - information on proposed takeovers, mergers, public offers and similar;
  - nationalisation;
  - issuance of shares, allocation, subscription, waiving of rights and conversion;
  - breaking of a lock-up agreement;
  - share splits or reverse share splits, including proposals to that effect;
  - changes in the rights attaching to the different categories of financial instruments;
  - dividend announcements, including the announcement of or change in the ex-dividend date, and amendments of the dividend policy. The ex-dividend date is important if there

are also options on the shares. A change in the ex-dividend date may impact on the price-setting for such options;
- notifications as provided for in Section 5:38 of the Wft, for example in the event that the percentage of a shareholder's capital is above or below the threshold value;

- Key facts pertaining to operations or strategy
  - acquisition or disposal of significant participating interests or business units;
  - entering into or breaking key alliances;
  - major reorganisations;
  - changes in strategic direction, radical changes in the company's activities;
  - acquisition or loss of key contracts, licenses, assignments, orders and similar;
  - development of significant new products;
  - dissolution of the company;
  - entry into new markets;
  - non-regular change of audit firm;
  - applying for a moratorium on payments or bankruptcy;

- Facts pertaining to board members or supervisory directors of an undertaking;
  - changes in the executive board or supervisory board of an issuer;
  - facts which could constitute grounds during an ongoing investigation for the AFM or another financial supervisory authority to replace directors of a company, proceed to the imposition of a sanction, including a warning, or report an offence committed by a director, supervisory director or the undertaking itself;
  - facts that could have a negative impact on the position of a director or supervisory director within the company, which facts do not necessarily need to be related to that officer's performance within the undertaking.

6. Arrangements for the closed list working instructions at department level

The following arrangements have been agreed with departments that may come into the possession of inside information.

6A. Audit and Reporting Quality

During the supervision of financial reporting in accordance with the Wtfv, there are two instances in which Audit and Reporting Quality (in Dutch: Kwaliteit Accountantscontrole & Verslaggeving, hereafter "KAV") may be required to disclose inside information:

1 Decision to request further clarification:
  - As soon as the KAV manager decides that a request for further clarification is to be sent, this is considered inside information.

2 A KAV employee becomes aware of inside information by another route, for example because a company:
  - provides information that will be incorporated in financial or other information that is yet to be published, as part of further clarification given verbally;
  - consults the AFM on the possible treatment of an accounting element in the annual accounts ahead of the publication of financial information.

In the context of supervising audit firms in accordance with the Wta, KAV may be required to make a disclosure in the following instances:

- Whenever an investigation is carried out into an incident, relating to an audit client (being an issuer listed on Euronext Amsterdam and/or Alternext) of the audit firm, disclosure must be considered as soon as the information is sufficiently specific. In this context, "specific" means that it is reasonable to assume that actual abuses exist (such as one or more material misstatements in the annual accounts). The disclosure does not need to wait until the draft report has been prepared or coordination with the external auditor or the audit firm has taken place.

The KAV section for Wtfv supervision will remove a company from the list when:

- A notice not containing a recommendation has been issued to the company;
- A company has given effect to a recommendation, in case a notice containing a recommendation was issued;
- The company or the AFM has announced that the AFM has taken the matter to the Netherlands Enterprise Court;
- The AFM has decided that it will not issue a notice to the company and this decision has been notified to the company by means of a final letter, whether containing agreements or not;
- The company has made an announcement to the market, because of which the AFM no longer has an informational advantage (deriving from informal discussions between the AFM and the company).

The KAV section for Wtfv supervision has the option to transfer a file previously entered onto the closed list to the Penal Fines Officer. The employee within the KAV section for Wtfv supervision, who added the file to the closed list, must specify in BAS that the Penal Fines Officer will take over responsibility.

6B. Capital Markets Integrity and Capital Markets and Data

The rules for Capital Markets and Data (in Dutch: Datagedreven Kapitaalmarkten, hereafter "DAK") are as follows:

- Circumstances, in which any intra-day inside information could be available, such as verification of a rumour with an issuer over the phone or the receipt of a transaction or material notification, will not necessarily need to be disclosed. However, disclosure will evidently need to take place if the circumstances persist for a longer period.

The rules for Capital Markets Integrity (in Dutch: Kapitaalmarktinfrastructuur en Transparantietoezicht, hereafter "KIT") are as follows:

- The receipt of prospectuses or draft prospectuses does not need to be added to the closed list as a rule. Although the announcement of the release of a prospectus could in some instances constitute inside information, for example if a potential rights issue is announced, the contents of a prospectus typically consists of public information. Prospectuses are in effect documents presenting public information in aggregated form. It cannot be ruled out here that prospectuses and supplements thereto might include elements potentially containing inside information. However, this will in the first instance be difficult to ascertain. With this in mind, issuers will be added to the closed list as soon as an application is received which includes a supplement that is known to contain information that has not been made public yet.

- All messages received with regard to a potential public offer will be entered on the closed list as a rule.

DAK and KIT will be subject to the following:

- Disclosure is required when any substantive aspects arise that could be deemed to constitute inside information.

6C. Penal Fines Officer

If a supervisory team transfers a file comprising a company appearing on the closed list to the Penal Fines Officer, the removal of this company will be the responsibility of the Penal Fines Officer.

The Penal Fines Officer will use BAS to remove the company when the imposition of the fine has been communicated externally or at the time the decision is made not to impose a fine.

6D. Account Management

The rules for Account Management (in Dutch: Accounttoezicht, hereafter "AT") are as follows:

- The AT manager responsible will use BAS to add and remove all companies included in the list which AT determines on annual basis.
- Files not appearing on the list established by AT will be added to the list as soon as the suspicion arises that inside information might exist. The company will be removed from the closed list once the relevant circumstances no longer apply. Examples include director screenings.

Appendix 3: Explanatory notes on insider files

As indicated in the table, there is a variety of reasons why an insider project with an insider file might be used. In these cases, all individuals designated as an insider by the project manager are subject to additional confidentiality measures. The compliance officer will also be involved in this and is able to designate as an insider any parties having any indirect involvement, such as individuals who are able to access the inbox of insiders or employees with access to systems used to store insider files.

Table: Phases applicable to insider files.

	Activate file	Set up file	Application in practice	Deactivate file
Who	The Executive Board, general counsel, head of department	Project Manager	Project manager and insiders	The Executive Board, general counsel, head of department
When	(1) If the continuity of the company subject to supervision is at stake and the AFM is considering drastic measures (2) If the information constitutes inside information (3) In case of a decision in relation to which the AFM, the company under supervision and/or its (co-)policymakers run a significant reputational risk if the information is made public prematurely	Immediately upon activation	Throughout the project	The envisaged situation has been achieved, the measure or inside information has been published, or there no longer is a reputational or continuity risk.
How	• appoint file coordinator (project manager) • involve compliance officer • compliance officer issues code name • register insider project in BAS	Project manager: • uses the code name in all documentation and communication regarding the file • makes insiders aware of the code name, their role and responsibilities, and the procedures for storing data, consultation and communication • ensures only the designated insiders have access to the file	• ensure all communications refer exclusively to the code name and do not name companies subject to supervision • ensure all file information is classified as secret • insiders are able to freely exchange the information among themselves • if a non-insider requires file information for work purposes, sharing is permitted after the project manager has given approval; the relevant individual must then also immediately be added to the insider list	project manager drafts a proposal • for deactivation and notifies the insiders The Executive Board, general counsel or head of department decides to proceed to the deactivation

Appendix 4: Regulations on reliability screenings

1. Introduction

Screening is one of the measures used by the AFM to ensure the reliability of its employees. Its aim in doing so is to prevent that the position of an employee is or becomes such that their reliability might be called into question. Screenings will be carried out before taking up employment (pre-employment screening) but may also be carried out in the course of an individual's employment (in-employment screening).

2. Pre-employment screening

2.1. Who will be subject to screening?

The AFM will screen all prospective employees. The screening may vary for each category of worker. The AFM has defined 5 categories of worker:

1. Individual with whom the AFM has concluded an employment agreement;
2. Individual who carries out work for the AFM on the basis of a secondment or other contract and has an AFM login account and/or has access to (highly) confidential information;
3. Individual who carries out work for the AFM on the basis of a secondment or other contract, does not have an AFM login account and has no access to (highly) confidential information and undertakes scheduled tasks for the AFM on a structural basis;
4. Individual who carries out work for or at the AFM on the basis of a secondment or other contract, does not have an AFM login account and has no access to (highly) confidential information and undertakes tasks for the AFM on an unscheduled and occasional basis;
5. Individual with whom DNB has concluded an employment agreement and who carries out work for the AFM based on a secondment or other contract.

For any employee who is assigned a different category after being screened, the screening will be restricted to those elements that did not form part of the previously conducted screening. An example could be an employee changing from category 2 to category 5.

Prospective employees who were previously screened by the AFM and have not been out of its service for more than three months, will not be screened in full again but will only be asked if there has been any change in their history. This exemption from screening will not apply (i) if the individual confirms that there has been in a change as regards their antecedents, or (ii) if a category applies that is subject to heightened scrutiny. If (i) applies, the prospective employee will be subject to screening in full and if (ii) applies, the screening of the prospective employee will be restricted to those elements that did not form part of the previously conducted screening.

Section 2.4 includes a table which sets outs the contents of the screening for each category.

2.2. Background check

Screenings may include a background check. The law authorises the AFM to access judicial records for a screening. Whether this check is carried out or not depends on the categories outlined above. For instance, a background check will not be carried out for employees who will not be given an AFM login account and carry out tasks for the AFM on an unscheduled and incidental basis.

If a prospective employee who is undergoing a background check reports an antecedent on the AFM Reliability Questionnaire and/or the check of the judicial records reveals any antecedents,

this could be a reason to exclude the prospective employee. The contact within the Human Resources & Facility Management department will inform the prospective employee of this decision. A compliance officer will provide an explanation for the reasons underlying the outcome of the screening in the Compliance, Integrity & Risk Management department. For more information on antecedents and their weighting, please see section 5.

2.3 Division of tasks

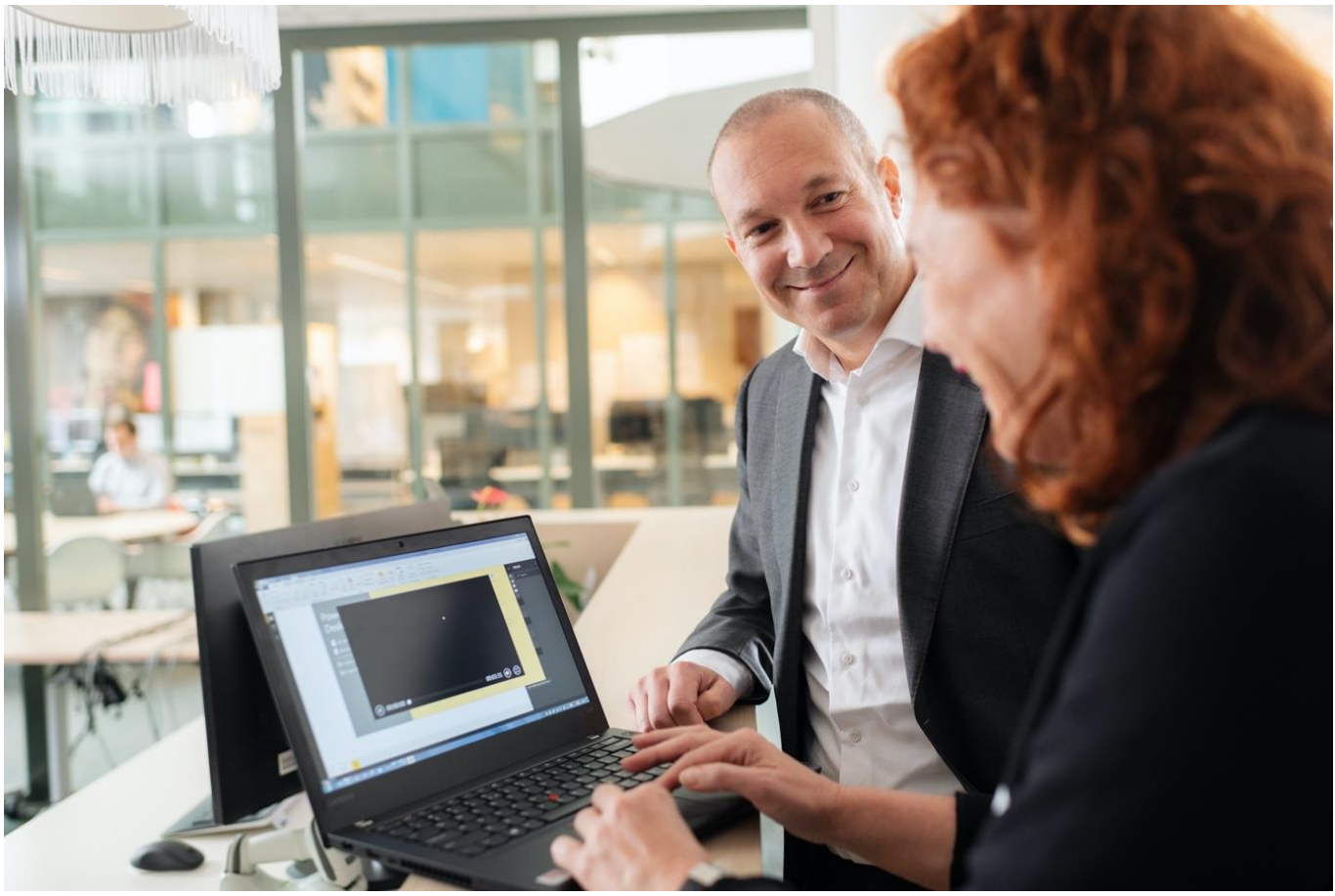
Reliability screenings will comprise various sections. Within the AFM, the following sections of the HRFB and CIR departments are involved in and responsible for the screening.

a. Human resources has responsibility for:
   - organising the screening process and executing the screening of prospective employees;

b. Facility Management has responsibility for:
   - issuing access passes and organising the associated process;

c. Compliance & Integrity has responsibility for:
   - assessing criminal and other antecedents;
   - advising Human Resources on the reliability of a current or prospective employee.

The responsibility for organising and executing screenings for prospective members of the Executive Board, or members of the Supervisory Board, rests with the secretary for the Supervisory Board. If any antecedents are identified, the secretary will request the advice of Compliance & Integrity.



2.4 Contents of the pre-employment screening for each category of worker

Reliability screenings for prospective employees will consist of the sections outlined in the following table. The responsible organisational unit is indicated alongside each section.

Sections in the reliability screening	Category of worker				
	1.	2.	3.	4.	5.
Confidentiality statement	HR	HR	HR	HR	N/A
Code of Conduct	HR	HR	N/A	N/A	N/A
Scan identity document	HR	N/A	N/A	N/A	N/A
Check references	HR	N/A	N/A	N/A	N/A
Integrity statement from previous employer	HR	N/A	N/A	N/A	N/A
Background check (judicial records)	HR/C&I	HR/C&I	HR/C&I	N/A	N/A
Reliability Questionnaire	HR/C&I	HR/C&I	HR/C&I	N/A	N/A
Private investments + automated processing form	HR/C&I	HR/C&I	N/A	N/A	HR/C&I
Declaration form regarding incompatible activities	HR	HR	N/A	N/A	N/A
Personal access card	FM	FM	FM	N/A	FM
Supplier card	N/A	N/A	N/A	Reception	N/A

3. In-employment screening

3.1 Who will be subject to screening?

Current employees of the AFM can also be subject to screening. This is referred to as an in-employment screening. This type of re-screening will take place in the event that:

- You applied internally for an integrity-sensitive position, are now the last remaining candidate for the role and the last screening by the AFM dates more than 5 years back. Please see section 4 for the definition of an integrity-sensitive position. By way of a policy decision, the Executive Board may designate further roles that must be regarded as integrity-sensitive positions.

- There is a change in relation to the employee's antecedents, which provides grounds for conducting a new reliability screening. In line with the provisions in Chapter 5.1 of the Code of Conduct, you must also notify the compliance officer of antecedents occurring in the course of your employment. Such reports may result in a new screening if the antecedent raises questions regarding your reliability. Examples include involvement with criminal antecedents such as fraud or theft. Fines for matters such as driving while under the influence or inaccuracies in a declaration

do not necessarily result in full rescreening, unless the offence is a repeat offence. More information on antecedents and their weighting is provided in Section 6.

3.2 How are screenings conducted?

In-employment screenings for the purpose of an internal application will comprise a background check. This means that the employee will be asked to complete a new AFM Reliability Questionnaire. This questionnaire asks about different types of antecedents and requests permission for obtaining a new extract from the Judicial Information Service (JustID).

If an in-employment screening is prompted by a change in their antecedents, employees will not need to complete the questionnaire. The review of the antecedent will involve a discussion between a compliance officer and the employee.

In both instances the compliance officer will also access the compliance file, including, in any event, the annual confirmation statement and any offences recorded.

If, in the course of the in-employment screening, any of the employee's antecedents raise doubts regarding their reliability, this may result in a sanction as described in Appendix 6, section 3. In the most serious cases, an antecedent may result in the employee's dismissal. To help inform its decision, the AFM has statutory powers to request judicial records from the Judicial Information Service.

3.3 Division of tasks

Screening in relation to an internal application for an integrity-sensitive position

- The responsibility for executing the screening and organising the associated process rests with HR.
- In the event that the screening reveals any antecedents, a compliance officer will be asked to assess these and advise HR on the reliability of the employee.

CIR has responsibility for:

- assessing criminal and other antecedents;
- conducting one or more interviews regarding the antecedents with the employee; and
- advising HR on the reliability of the employee.

If the assessment results in a sanction or negative recommendation regarding the employee's reliability, CIR will notify the employee of this.

Screening as a result of a change in the antecedents

- The compliance officer will review any changes in an employee's antecedents. Contrary to screenings in relation to an internal application for an integrity-sensitive position, this review will in principle be carried out without intervention from HR.
- The review of the antecedent may lead the compliance officer to conclude that a sanction is appropriate.
- The compliance officer will submit recommendations involving minor sanctions to the CIR manager, who will use the recommendation issued by the compliance officer to determine whether a minor sanction should be imposed.
- Recommendations involving a severe sanction will be coordinated with the CIR manager, the head of HR and, if appropriate, the general counsel, after which the compliance officer will

submit these to the chair of the Executive Board. Using the recommendation issued by CIR, the chair of the Executive Board will decide which sanction to impose, if any.
- CIR will communicate the outcome to the employee.

3.4 Integrity-sensitive positions

A distinction is made between three types of integrity-sensitive positions:

A. Senior positions:

- member of or secretary for the Executive Board
- general counsel
- head of department
- Commissioner for Trade Decisions

These positions are different to other positions within the AFM, given the responsibility that rests on these employees in relation to decision-making, policy setting and employee assessments. Re-assessment of any antecedents for an employee applying for a position of this nature does not only emphasise the importance of integrity to the AFM but also helps to eliminate potential risks.

B. Positions with special information privileges

- compliance officer, senior compliance officer and CIR manager
- Data Protection Officer
- auditor or senior auditor

These positions play a key role in identifying, addressing and handling signals in relation to the organisation, its employees and its/their integrity. The AFM must be able to have full confidence in the reliability of the employees tasked with this.

C. Positions with extensive information privileges

- IT Automation manager, employees in roles belonging to the IT Automation job family
- executive secretary
- member of or secretary to the Supervisory Board
- employees designated by the responsible head of department or manager
- Penal Fines Officer

Although all employees can freely access most information within the AFM, some information is blocked. There are, however, a select number of employees whose role provides them with structural access to blocked information, either for all such information or cross-file information.

3.5 Position involving confidentiality

In addition to these regulations, the minister can appoint certain positions as a 'Position involving confidentiality' (a so-called vertrouwensfunctie). Positions involving confidentiality are positions where an abuse of office could endanger national security. If you have applied for or hold a position that is designated a "position involving confidentiality" (a so-called vertrouwensfunctie), you need a "certificate of no objection" (Verklaring van geen bezwaar, VGB) issued by the AIVD. The AIVD carries out the security screening requested by the AFM.

4. Antecedents

Antecedents are a key factor in assessing the reliability of current and prospective employees. That is why it is crucial that antecedents are reported accurately, in full and immediately. The AFM will then take into account all facts and circumstances to assess the reliability of a current or

prospective employee. In this assessment, not all antecedents will be accorded the same weight. Failure to come forward about an antecedent may be factored into the assessment as an aggravating circumstance. This could raise doubts about your reliability, even if the antecedent itself does not carry great weight. This is why it is important to always be open and honest.

The following table outlines the different types of antecedents (however, the list of examples must not be considered exhaustive). For each type antecedent, you will find what things you must and need not disclose. These antecedents are the same as those listed in the AFM Reliability Questionnaire, which prospective employees must complete when they take up employment.

What antecedents should I disclose?

Type of antecedent	Things you must disclose	Things you do not need to disclose
Criminal	Crimes as provided for in the Criminal Code, the Opium Act, the Weapons and Ammunition Act, the Road Traffic Act and similar. Property crimes and serious offences involving abuse of office. Examples: - Insider trading, tax fraud, embezzlement, physical abuse, vandalism, theft, driving whilst under the influence and failure to stop after an accident.	Offences; these are generally less serious in nature than crimes and are dealt with under administrative law. Examples: Traffic offences, such as exceeding the speed limit (by up to 30 km/h), failure to wear a seat belt and public drunkenness.
Fiscal and administrative	Negligence penalties imposed by the Tax Authorities. These are imposed for the intentional submission of inaccurate or incomplete tax returns.	Default surcharges imposed by the Tax Authorities. These are imposed for failures to make payment or timely payment in respect of a tax return or tax assessment.
Financial	- A bankruptcy involving improper administration and/or fraudulent acts in respect of creditors. The individual has been held responsible. - A moratorium on payments applies or a request for debt restructuring has been filed. - Serious financial difficulties.	Payment reminders or demands due to non-payment of bills, whether unintentionally or otherwise.
Supervisory	A company where you held the position of (co-) policymaker has had a supervisory measure imposed, such as a warning or fine.	Supervisory measures do not need to be disclosed if your role did not include involvement in or responsibility for policy setting.
Other	- Conflicts in the workplace that resulted in a measure such as a reprimand, warning, deduction of wages or dismissal. - Employment, disciplinary or other similar measures imposed by a professional body, such as DSI or the Netherlands Bar Association.	If a conflict in the workplace did not result in the imposition of a measure, you are not required to disclose it.

5. Weighting factors

Antecedents will be carefully assessed using the following weighting factors: severity, culpability, time elapsed, disclosure, combination, capacity, attitude, motives and clarification.

5.1. Severity

To what extent does the antecedent impair the integrity with which the role could be fulfilled? One of the criteria used to determine the level of severity is the type of antecedent. These are classified into one of three categories[3]:

	Category I minor (less serious)*	Category II moderate (serious)	Category III severe (extremely serious)
Criminal	Maximum of 2 settlements with the Public Prosecution Service or fines for driving whilst under the influence.	Convictions for death or injury by negligence, failure to stop after an accident, theft, crimes of violence.	Convictions for economic crimes including forgery, fraud, extortion, embezzlement and convictions for offences against the Opium act and tax legislation.
Fiscal and administrative	Maximum of 2 negligence penalties of up to 25% inclusive for gross negligence.	Maximum of 2 negligence penalties of up to 50% for gross negligence.	Negligence penalty between 50% and 100% for recklessness or intent.
Financial	Financial difficulties, circumstances in which fixed outgoings or payment obligations can no longer be met.	Filing for a moratorium on payments or debt restructuring.	Culpable bankruptcy (involving improper administration/fraudulent acts towards creditors).
Supervisory	Maximum of 2 warnings/instructive meetings.	Providing incorrect or incomplete information to a supervisory authority. Measures imposed by a supervisory authority such a fine or an order subject to a penalty.	Measures imposed by a supervisory authority such as withdrawal of a license due to unethical management, report against the individual or company.
Other	Entry or warning because of a conflict in the workplace.	Dismissal because of a conflict in the workplace. Disciplinary measures due to violation of integrity requirements.	

*Although category I antecedents must still be disclosed to the compliance officer, they are in principle not considered grounds for further investigation.

5.2. Culpability

How unethical was the individual's behaviour and were they aware of the immoral or illegal act or should they have been aware of it? Among other things, the level of culpability will be determined based on attitude, capacity/position, intent (acting deliberately), intention and whether the offence is a repeat offence. If an individual has been fined multiple times for the same offence,

[3] The overview provides a number of examples but this is not an exhaustive list.

this can point to an inadequate sense of values (and ability to learn). In such cases, a category I antecedent could be given significant weight.

5.3. Time elapsed

How far back does the antecedent date? The more time has passed since an offence, the less weight will be given to it in assessing reliability. This also applies to repeat offences. In this context, the AFM applies a term ranging between 5 years for less serious antecedents and 10 years for serious antecedents. If the individual to be assessed has had an extended period without any antecedents prior to a screening or re-screening, they must be able to continue with a "clean slate".

5.4. Combination

If multiple antecedents exist, these will be assessed in relation to each other. This could mean that an antecedent that does not qualify as serious on its own merits could still give rise to doubts as regards the employee's reliability when considered in combination with other antecedents.

5.5. Capacity

Was the person acting in a professional or private capacity at the time of the antecedent? Could the antecedent be attributed to youthful indiscretion (applicable up to and including the age of 25)? Other relevant aspects for the weighting can be the individual's position, education or professional background.

5.6. Disclosure

Did the individual ensure the antecedent was reported by themselves and immediately (mitigating circumstance) or not (aggravating circumstance)? In the event an antecedent was not disclosed, it will be checked whether the information was deliberately withheld. The deliberate withholding of information will be given great weight.

5.7. Attitude, motives and clarification

Does the individual recognise how serious their action or failure to act was and that the antecedent should not have happened? Another relevant aspect is whether the individual shows themselves to be cooperative. An appropriate attitude, plausible motives and extensive clarification may count as mitigating circumstances.

6. Documentation of the assessment of antecedents

As outlined in these regulations, responsibility for assessing antecedents in the context of screenings for current or prospective employees rests with CIR.

The compliance officer will document his or her activities and manages and archives all information provided by current or prospective employees and third parties. If a screening concerns a pre-employment screening or an in-employment screening arising from a role change, the compliance officer will assess antecedents at the request of HR and notify HR of the outcome of the assessment. In the event that there is a change in antecedents, the disclosure and employee statements in respect of antecedents will be added to BAS by employees themselves. The compliance officer will assess, communicate and manage all disclosures made by employees using BAS. The compliance officer will archive the investigations conducted and actions taken in the employee's compliance file, which is kept in a secure environment in Fides.

Changes in the employee's antecedents may result in further investigation and the imposition of a sanction. Minor sanctions that are imposed will be documented in the compliance file, whereas

severe sanctions will be documented in the employee's personnel file by HR. Sanctions will be recorded in the compliance file or, the case may be, the personnel file as soon as the employee has been notified of the outcome of the screening. Only the compliance officer is able to access the compliance file. HR. maintains the personnel file. The information stored in the personnel could have consequences for employees who apply for a position with another employer, should this employer conduct a reference check and request an integrity statement from the AFM.

7. Rights of subjects

Option to appeal in relation to an in-employment screening

Following the imposition of a severe sanction, employees have 4 weeks within which to lodge a written appeal with the chair of the Supervisory Board. Appeals in respect of a minor sanction can be lodged with the chair of the Executive Board within 4 weeks. Employees must state the reasons why they disagree with the sanction that has been imposed and submit their substantiation to the compliance officer. The compliance officer will then pass this to the officer responsible for reviewing the appeal. The chair of the Supervisory Board or, as applicable, the chair of the Executive Board will issue a decision within 4 weeks of this date.

Employee privacy

The compliance officer will treat any data and information received in connection with an investigation as confidential at all times, requesting advice from the Data Protection Officer as necessary. All relevant documentation regarding the investigation and the processing of the relevant personal data will be stored in accordance with the guidance provided in the General Data Protection Regulation (GDPR) and other applicable laws and regulations, and will be retained in accordance with the AFM data retention policy. More information about the employee's privacy rights under the GDPR have been included in the internal privacy regulations for AFM employees.

8. Complaints Procedure

In the event that an employee disagrees with the manner in which the screening (investigation into the antecedent) has been carried out, he or she may submit a complaint to the AFM Complaints Committee. For further details, please refer to the AFM Complaints Procedure. 9.

9. Applicability and entry into force of these regulations

These regulations were revised in a number of respects and will enter into force on 1 January 2021. These regulations apply to all AFM employees.

Appendix 5: Reporting scheme for actual and suspected abuses and integrity breaches

Integrity has the AFM's utmost priority. For this reason, the AFM promotes a strong culture in which abuses or integrity violations have no place. This also implies that there must be a safe and quick way to report abuses or integrity violations, so that action can be taken. These regulations set out how to safely report abuses or integrity violations when there are reasonable grounds to do so.

An integrity violation is a failure of employees to conduct themselves in accordance with the AFM's standards, values and Code of Conduct. A violation that puts the interests of society at stake is considered an abuse. This relates to immoral or illegal practices taking place under the responsibility of the AFM. This has a broad scope, for example because of the severity, extent or structural nature of such practices.

The procedure is not intended for personal grievances in relation to conflicts in the workplace or similar matters. This scheme is also separate from the Complaints Procedure for Undesirable Behaviour, which specifically focuses on undesirable behaviour towards an employee, and the AFM Complaints Procedure, which may be used by anyone who wishes to submit a complaint regarding any act and/or failure to act by the AFM and its employees. This scheme applies to anyone working at or having worked at the AFM, as well as anyone who interacts or has interacted with the AFM in a work-related context. This includes all AFM employees and contractors.

Appendix 6: Regulations on investigations and sanctions explains how received reports are assessed and investigated.

1. General principles

1.1 This scheme provides employees with a possibility to report suspected abuses and integrity violations involving the AFM, including:

a. A criminal offence or imminent criminal offence;
b. A breach or imminent breach of statutory and regulatory provisions;
c. Intentional provision or imminent intentional provision of incorrect information to public bodies;
d. A breach or imminent breach of any standards and values outlined in the Code of Conduct, where such a breach could result in consequences under employment law;
e. Intentional withholding, destruction or manipulation, whether actual or imminent, of information pertaining to one of the breaches listed under a to d inclusive.
f. Direct or indirect damage, whether actual or imminent, to the AFM's reputation, in any manner whatsoever.

1.2 In light of the potential negative consequences for the employee to whom the suspicion relates, reporting must be considered a final course of action, as this leaves no other option to resolve suspected abuse or a suspected integrity violation.

1.3 If a report concerns a breach or abuse other than those listed in Section 1.1 and is insufficiently substantiated, it will not be considered. Exceptions to this are breaches of the vital interests of the AFM, the protection of the physical or moral integrity of an employee or statutory duties to report the suspected abuse or integrity violation to a public body.

In the remainder of these regulations, abuses and integrity violations will be jointly referred to as incidents.

2. Information and guidance for reporting individuals

2.1 The reporting individual has the option to discuss a suspected incident in confidence with a confidential counsellor of the AFM. Confidential counsellors are independent, and will listen and provide advice and information in confidence.

2.2 The reporting individual has the option to consult an external adviser in confidence. The external adviser is able to provide advice on the appropriate reporting channel and highlight the risks associated with making a report.

2.3 The external adviser referred to above must be bound by a duty of confidentiality based on their professional or official capacity. If this is not the case, the reporting individual may be held responsible in the event the adviser makes the incident public.

2.4 In case of potential abuse, the reporting individual is also able to obtain information, guidance and support from the advisory team at the Dutch House for Whistleblowers.

3. Internal report

3.1 In the first instance, the reporting individual must report suspected abuse internally, unless a ground for exemption as listed in Section 9.2 applies.

3.2 Suspected incidents may be reported verbally or in writing to:

a. the incident hotline managed by the compliance officer;
b. a confidential counsellor within the AFM;
c. a line manager, including the individual's own line manager;
d. the chair of the Executive Board.

3.3 Reports relating to the performance and/or conduct of the Executive Board may also be submitted to the chair of the AFM Supervisory Board.

3.4 Reports relating to the performance of the chair of the Supervisory Board may be submitted to the vice chair of the Supervisory Board.

3.5 All reports received will be passed to the compliance officer for assessment. Confidential counsellors will not pass on any reports, unless the reporting individual has given their express consent.

4. Recording of internal reports

4.1 The compliance officer will document verbal reports and the date of receipt in writing and, within 7 days of the report, provide the reporting individual with the opportunity to check, correct and sign the record of the conversation for approval. A copy of this will be sent to the reporting individual.

4.2 For reports submitted in writing, the reporting individual will receive a confirmation of receipt from the compliance officer within 7 days.

4.2 Reports of suspected abuse will be immediately notified to the chair of the Executive Board by the compliance officer or, subject to the express consent of the reporting individual, by the confidential counsellor.

4.3 In the event that Section 3.3 applies, the suspected abuse will be notified to the chair of the Supervisory Board.

4.4 In the event that Section 3.4 applies, the suspected abuse will be notified to the vice chair of the Supervisory Board.

4.5 The report will be marked as "highly confidential" and a report of suspected abuse will be marked as a "report under the Whistleblower scheme". Reports will only contain the information that is strictly and objectively necessary to verify the suspicion of abuse. In a register set up for that purpose, a note will also be made that the facts included relate to a suspicion of abuse.

5. Handling of the report

5.1 In case of a report relating to suspected abuse, the chair of the Executive Board, in consultation with the CIR manager, will decide whether one or more members of an investigation team set up for that purpose must carry out an investigation. The members of the investigation team, such as the compliance officer or senior compliance officer, will be subject to special security and confidentiality measures.

5.2 With regard to reported incidents that could involve a member of the Executive Board, the decision whether to investigate will be taken by the chair of the Supervisory Board, in consultation with the CIR manager.

5.3 With regard to reports of a potential violation of integrity by an employee, the decision whether to investigate will be taken by the CIR manager in consultation with the compliance officer or senior compliance officer. In case of a serious incident, this decision may be taken in consultation with the head of Legal Affairs and/or the chair of the Executive Board.

6. Time limits for the handling of the report and notification to the reporting individual

6.1 Within 6 weeks of the recorded date of receipt, the chair of the Executive Board or the Supervisory Board will communicate a substantive statement in respect of the reported incident, or arrange for such a statement to be communicated, to the reporting individual. This statement will outline the steps that have been taken in response to the report, such as measures taken or proposed. The reporting individual will be able to respond to this.

6.2 If it is not possible to provide the statement within the time limit indicated in Section 6.1, the reporting individual will receive a notification, including written confirmation of the timescale within which a statement will be issued to the employee. This additional period may not exceed 6 weeks.

6.3 In the event the time limit is extended, the reporting individual will receive an update on the progress made in the investigation.

6.4 By way of exception to Sections 6.2 and 6.3, the reporting individual will not be notified regarding the progress and/or the outcome of the investigation if such information could compromise the investigation or legal proceedings.

7. Confidentiality and the identity of the reporting individual

7.1 The reporting individual, members of the investigation team, confidential counsellors, the Executive Board and/or the members of the Supervisory Board and any other person involved in the reporting or investigation of a suspected integrity violation, abuse or information regarding a breach and in this context has access to data that they know or should reasonably assume to be confidential, is required to keep such information and data confidential. An exception applies in the event that law requires disclosure. In addition to the above, information regarding the report will only be made available to those parties within the AFM who need this knowledge to allow them to fulfil their responsibilities in connection with this scheme, including investigation and the follow-up of the investigation.

7.2 Whenever information is disclosed, this will be done without revealing the name of the reporting individual. Disclosures will also be made in a way that safeguards the identity of the reporting individual as much as possible. Information that could identify the reporting individual either directly or indirectly will only be shared with the reporting individual's consent or if the law requires the identity of the reporting individual to be disclosed.

8. Anonymous reports

Reports can be submitted anonymously but will only be taken into consideration if they are serious and sufficiently specific to enable further investigation without the need for additional information from the reporting individual. In view of this, the preferable approach is to submit a report via a confidential counsellor as this allows the confidential counsellor to seek further clarification that would make the case sufficiently specific. The confidential counsellor can then also act as an intermediary in answering any questions the officials dealing with the report might have.

9. Reporting suspected abuse externally

9.1 Reporting individuals who have followed the procedure for an internal report may also report suspected abuse externally if any of the following apply:

a. The reporting individual disagrees with the statement by the AFM, holds the opinion that the suspected abuse has been wrongly set aside and has made this opinion known to the AFM in accordance with Section 6.1;
b. The reporting individual disagrees with the manner in which the AFM has conducted itself in connection with the report, therefore has reason to fear retaliation as a result of making an internal report and has made the Executive Board or Supervisory Board aware of this in accordance with Section 6.1;
c. The reporting individual did not receive a statement within the time limits stipulated in Section 6.2;

9.2 Reporting individuals who cannot reasonably be expected to submit an internal report, are able to directly report suspected abuse externally. This course of action will in any event be open in the following cases:

a. If there is an immediate threat to individuals, goods or property, which, as a result of an urgent and substantial public interest, requires immediate reporting because the reporting individual is of the reasonable opinion that an internal report will not result in the necessary actions;
b. If there are reasonable grounds to assume that the suspected abuse involves a member of the Executive Board and/or the Supervisory Board;
c. If circumstances exist in which the reporting individual has reasonable grounds to fear retaliation as a result of an internal report;
d. If there is a clearly identifiable threat that evidence may be concealed or destroyed;
e. If there was a lack of action to eliminate the same situation of abuse after an earlier internal report;
f. If a statutory duty to directly make an external report applies.

9.3 The reporting individual can make an external report to an eligible external party. The reporting individual should consider the efficacy with which the external party could intervene, as well the AFM's interest in the least harmful manner of invention.

An external party is understood to mean:
a. A body responsible for the detection of criminal offences;
b. A body responsible for monitoring compliance with the provisions laid down by or under any law;
c. Any other competent body that is able to receive reports of suspected abuse, including the investigative team at the Dutch Whistleblowers Authority.

10. Notification to the accused

10.1 Following the receipt of a report, CIR will notify the individual to whom the report relates as soon as possible. However, an exception applies if such a notification would jeopardise an effective investigation into the incident by the AFM. The accused must in any event receive notification as soon as this risk no longer applies.

10.2 The accused will be informed of (i) the facts that have been alleged against them, (ii) the recipients of the report, (iii) the fact that responsibility for the scheme rests with the AFM, and (iv) the manner in which the person concerned can exercise their right of access to and right to rectification, deletion or restriction of personal data pertaining to them (refer to Chapter 6 of the Code of Conduct). The accused will not receive information with regard to the identity of the reporting individual.

11. Legal protections for reporting individuals and misuse of this scheme

11.1. Individuals reporting a suspected incident in good faith and showing due care in both formal and substantive matters, will have their legal position protected during and after the handling of an internal or external report. This means that the position of a reporting individual will not be disadvantaged in any way whatsoever because of a report having been made, including when the facts are later found to be incorrect or incomplete, or a report does not result in subsequent action.

11.2 Due care in formal matters is deemed to have been shown if:

a. The reporting individual has first reported the suspected abuse internally in the manner described in the Code of Conduct, unless this cannot be reasonably be expected as provided for under these regulations.
b. The reporting individual has disclosed the facts in an appropriate and proportionate manner when making an external report.

11.3 Due care in substantive matters is deemed to have been shown if:

a. The reporting individual has reasonable grounds to assume the facts are correct.
b. The external report serves a public interest that overrides the interest of the AFM in maintaining confidentiality.

11.4 Any misuse of these schemes, including reports made in bad faith, may result in disciplinary measures or legal proceedings. Anyone responsible for the adverse treatment of a reporting individual will be subject to the same sanctions.

12. Protection for other involved parties

12.1 Individuals who are involved with the report, such as a confidential counsellor and witnesses to incidents acting in good faith, will have their legal position protected. This means that the position of witnesses and other involved parties will not be affected in any way whatsoever because of their involvement.

12.2 Accused individuals will also have his or her legal position protected. This means the accused will be deemed innocent until proven otherwise and their position will not be affected in any way whatsoever until such proof is found.

13. Privacy

13.1 The compliance officer will treat any data and information received in connection with a report or an investigation as confidential at all times, requesting advice from the Data Protection Officer as necessary. All relevant documentation regarding the investigation and the processing of the relevant personal data will be stored in accordance with the guidance provided in the General Data Protection Regulation (GDPR) and other applicable laws and regulations, and will be retained in accordance with the AFM data retention policy. More information about the employee's privacy rights under the GDPR have been included in the internal privacy regulations for AFM employees.

13.2 The report data in the register will be destroyed when they are no longer necessary in order to comply with the requirements of the House for Whistleblowers Act or any other requirements laid by or under national or Union law.

14. Applicability and entry into force

These regulations were revised in a number of respects and will enter into force on 1 January 2021. These regulations apply to all AFM employees.

Appendix 6: Regulations on integrity investigations and sanctions

Reports regarding an integrity violation and/or abuse (incident) that may influence the integrity of an employee and/or the organisation will always be dealt with and assessed by the compliance officer with great care. The assessment could result in an investigation. This appendix explains:

- How reports will be assessed;
- When an investigation will be launched;
- If, how and what sanctions will be imposed.

1. Assessment of reports

Suspected abuse and/or suspected integrity violations may be brought to light in a number of ways (see section 5.2 of the Code of Conduct). The AFM may develop such a suspicion itself and/or an employee could report a suspicion. Reports can be made via the incident hotline, a confidential counsellor or a line manager. Antecedents can also be the subject of a report. Appendix 4: Regulations on integrity screenings explains how this type of report is assessed.

More information on the procedure for reporting suspected and actual abuse or integrity violations can be found in Appendix 5.

Assessment criteria

Following the receipt of a report, the compliance officer will always carry out an assessment based on the following criteria:

- The nature and classification of the incident (minor or severe);
- The verifiability of the incident;
- The plausibility and likelihood of the incident;
- The position or identity of the reporting individual;
- The position or identity of the individual(s) to whom the incident relates.

Examples of minor incidents	Examples of serious incidents
You have purchased a home but have forgotten to submit the offer for a mortgage with an investment component to the compliance officer for prior approval. Violations of general rules of conduct are also deemed minor antecedents.	Repeated (minor) incidents, insider trading and/or leaking confidential supervisory information, theft, abuse of powers arising from a position and/or duties, and economic crimes such as tax fraud, forgery of documents, embezzlement and bribery. Incidents that put the interests of society at stake, for example because of a threat to public health or the safety of individuals.

2. Investigation procedure

The initial assessment of the report will lead to a decision as to whether the report will be investigated. The compliance officer will make a recommendation in this regard, with the decision taken by the officer or body who has competency given the nature of the incident:

- In the case of an integrity violation by an employee, the decision is up to the CIR manager, who will consult the head HR, the head of Legal and the chair of the Executive Board as necessary in relation to serious cases. If the incident relates to the CIR manager, the decision will be made by the chair of the Executive Board.
- If abuse is suspected, it will be the responsibility of the chair of the Executive Board to decide whether an investigation will be conducted.
- If a suspicion of abuse or suspected integrity violation involves the Executive Board, the decision will be taken by the chair of the Supervisory Board.
- If an incident involves the chair of the Supervisory Board, the decision will be taken by the vice chair of the Supervisory Board.

Different actions may be taken depending on the assessment of the report:

1) No investigation
   The report will not be investigated further and the file will be closed. The incident is not sufficiently serious or the report is not sufficiently founded (insufficient evidence).
2) An investigation is launched
   The compliance officer launches an investigation. This could be an exploratory investigation, aimed at gathering additional information for a careful assessment. In the event of a serious incident, however, this can also take the form of a special investigation. In the case of a serious incident, the compliance officer may furthermore conclude that referral to the Public Prosecution Service is appropriate. The compliance officer will communicate this recommendation to the chair of the Executive Board or, in the event a member of the Executive Board is involved, the chair of Supervisory Board, either of whom will then make a decision.
3) Consideration whether to impose a suspension
   In exceptional circumstances, for example in the case of fraud, suspension of the employee for the duration of the exploratory or special investigation can be considered in case option 2) is selected. The decision to do so is taken at the level of the Executive Board, in consultation with the head of HR.

2.1 Exploratory investigation

If necessary, the compliance officer will seek further clarification from the reporting individual before launching an investigation. In addition, the employee to whom the report relates will be informed that a report has been made and asked to give a response. In exceptional cases it could be that, in the interest of the investigation, the employee will not be notified by the compliance officer until a later point in time. This will only apply in the event that announcement of the investigation could affect the outcome thereof.

Minutes will be prepared for each interview with an involved party and the employee will have the opportunity to respond to this in writing. The compliance officer will stop the investigation as soon as it becomes clear that a report is unfounded and will then notify the employee to whom the report relates accordingly. Where appropriate, a special investigation can be launched if there are sufficient grounds to believe that the employee is involved in the incident. This could be the

case if further fact finding is required. An exploratory investigation may already result in the imposition of a sanction in relation to the violation if it is confirmed that the employee was involved. In that case, no special investigation will be necessary.

To the outcome of the investigation, the compliance officer will append a written recommendation with regard to any sanctions to be taken.

2.2 Special investigation

If required, the compliance officer may conduct a (further) investigation into the facts. Once again, the investigation will not be started until the employee to whom the report relates has been notified and all parties have been heard. Special investigations may take several forms and could for example entail conducting interviews or examining the operational resources used or arranging for such an examination to be carried out. As part of this, departments such as IT Automation, TDO or IA may be called upon to provide their expertise. If the outcome of the investigation is not consistent with the response given by the employee in the interview with the compliance officer, the compliance officer will raise this with the employee and ask them to respond.

2.3 Cooperation and confidentiality

During an investigation, employees are obliged to provide information relevant for the assessment of the report as requested by the compliance officer. For example, in case of an investigation into their investment transactions, employees must provide information on private transactions executed for their own account.

The reporting individual will receive feedback on the manner in which the report was followed up, provided this does not conflict with the rights of the accused and/or third parties.

The compliance officer and all other employees and departments involved will treat any information and data received as a result of an investigation as confidential.

3. Sanctions

The compliance officer will prepare a recommendation as to whether a sanction should be imposed or not. The compliance officer will do so as soon as possible following an investigation to establish the facts and circumstances. Who will then decide whether a sanction should be imposed or not?

Recommendations involving minor sanctions will be coordinated with the CIR manager and added to the employee's compliance file.

Recommendations involving a severe sanction will be coordinated with the CIR manager, the head of HR and, if appropriate, the general counsel, after which the compliance officer will submit them to the chair of the Executive Board. Using the recommendation issued by CIR, the chair of the Executive Board will decide which sanction to impose, if any.

For cases involving a member of the Executive Board or the Supervisory Board, the recommendation will be coordinated with the chair of the Supervisory Board. In cases that involve the chair of the Supervisory Board, the vice chair of the Supervisory Board will be authorised to impose a sanction. In cases that involve the CIR manager or the head of HR, the chair of the Executive Board will be authorised to impose a sanction.

Examples of sanctions

No indication can be given as to what sanction will be attached to which incident. This must be assessed on a case-by-case basis, considering the specific circumstances that apply, such as the nature and severity of the incident, as well as the employee's personal circumstances. The next section provides a non-exhaustive overview of possible sanctions.

Minor sanctions	Severe sanctions
• Entry in the compliance file and/or an instructive conversation regarding standards • Mandatory reversal of the private transaction executed, with any additional proceeds being donated to charity	• Written reprimand or a warning • Withdrawal of facilities • Recovery of losses from the employee • Reassignment to a different department • Reassignment to a different, potentially lower position • Start-up of exit procedure • Dismissal or summary dismissal

Framework for assessing sanctions

If the investigation confirms that a violation has taken place, the compliance officer will determine whether a sanction should be imposed and if so, which one. When deciding this, the compliance officer will review whether the violation is a minor or a serious violation.

The nature and severity of the incident will be assessed using the following weighting factors:

a. Severity: Is this an incident that would impair the integrity with which the employee can fulfil and perform their role? In this regard, it is also relevant whether the incident has any impact on society or the AFM.
b. Culpability: Among other things, assessing culpability means reviewing the extent to which the person has acted illegally or was aware or should have been aware of the illegitimacy of the acts, and what their intentions were when they acted. Aspects that will be considered include the following:
    - Whether the acts were intentional or not -> Was the individual's act and/or failure to act deliberate and what intentions did they have? How was the matter viewed at the time the violation was perpetrated?
    - Capacity -> Was the individual acting in a private or work-related capacity when they committed the violation? What role or position does the individual hold?
    - Has inside information or confidential supervisory information been used?
    - Is this a repeat offence? -> Has the employee previously committed similar violations? Are there previous occasions on which an instructive interview was held or a warning was given?
    - Duration of the violation -> It is important to establish when the violation began and ended. Did the employee cease the illegal behaviour as soon as they became aware that they were committing a violation? A violation that has continued for an extended period of time will weigh more heavily than a one-off.

c. Time elapsed: An incident will carry less weight as time passes. In light of this, it is important to establish when the violation took place and when it ended.
d. Reporting, attitude and ability to learn: The extent to which the employee demonstrates transparency will carry significant weight in the assessment. Was the report made by the employee themselves or not? Consideration will also be given to the attitude adopted by the employee during the investigation. The employee's attitude, motives and clarification show whether the employee too considers their actions and/or failure to act to be serious, whether they understand the incident should not have taken place and whether they have learnt from it.
e. Combination: Has the employee been involved with incidents more frequently, whether in a culpable manner or otherwise?

Once the severity and culpability have been established, the decision as to what sanction should be imposed will also take account of the following principles:

- Proportionality: The measure must be proportionate to the violation;
- Consistency: The actions taken must be in line with those taken in similar cases in the past;
- Exceptional circumstances: All facts and circumstances must be taken into account, including both mitigating and aggravating circumstances.

Mitigating circumstances include a good record of service, approval of the action by a line manager, a long record of service, failure by a line manager to challenge or adequately challenge the employee, or inadequacies in the process and controls within the organisational unit.

Aggravating circumstances include previous warnings given by a line manager, serious loss of reputation or credibility for the AFM, exemplary role based on the position held, abuse of specific powers related to the position held, personal financial or other gain, previously imposed sanctions or repeated behaviour.

4. Compliance database

The compliance officer will document his or her activities and manages and archives all information provided by employees or third parties. Documents such as written agreements and statements provided by employees, for example with regard to private investment transactions and activities, will be recorded and managed in BAS by employees themselves. The compliance officer will assess, communicate and manage all disclosures made, sent and submitted by employees using BAS. The investigations conducted and actions will be archived in a secure environment within Fides.

Minor sanctions that are imposed will be documented in the compliance file, whereas HR. will document a severe sanction in the employee's personnel file. This will be done once the employee has been informed. Only the compliance officer is able to access the compliance file. HR. maintains the personnel file. The information stored in the personnel could have consequences for employees who apply for a position with another employer, should this employer conduct a reference check and/or request an integrity statement from the AFM.

5. Rights of subjects

Option to appeal

Following the imposition of a severe sanction, employees have 4 weeks within which to lodge a written appeal with the chair of the Supervisory Board. Appeals in respect of a minor sanction can

be lodged with the chair of the Executive Board within 4 weeks. Employees must state the reasons why they disagree with the sanction that has been imposed and submit their substantiation to the compliance officer. The compliance officer will then pass this to the officer responsible for reviewing the appeal. The chair of the Supervisory Board or, as applicable, the chair of the Executive Board will issue a decision within 4 weeks of this date.

Employee privacy
The compliance officer will treat any data and information received in connection with an investigation as confidential at all times, requesting advice from the Data Protection Officer as necessary. All relevant documentation regarding the investigation and the processing of the relevant personal data will be stored in accordance with the guidance provided in the General Data Protection Regulation (GDPR) and other applicable laws and regulations, and will be retained in accordance with the AFM data retention policy. More information about the employee's privacy rights under the GDPR have been included in the internal privacy regulations for AFM employees.

6. Complaints Procedure

If the reporting individual or another involved party disagrees with the manner in which the investigation has been conducted, they may submit a complaint to the AFM complaints committee. For further details, please refer to the AFM Complaints Procedure.

7. Applicability and entry into force of these regulations

These regulations were revised in a number of respects and will enter into force on 1 January 2021. These regulations apply to all AFM employees.

Appendix 7: Regulations on complaints of undesirable behaviour

Section 4.5 of the AFM Code of Code describes what is considered undesirable behaviour at the AFM. The AFM is committed to protecting in-house staff and contractors against undesirable behaviour. This is why these regulations have been put in place, which explain how to submit a formal complaint of undesirable behaviour. The preferred approach is that you should in the first instance attempt to address and resolve undesirable behaviour with the offending party. You can also approach your line manager or a confidential counsellor. If your attempts are unsuccessful, or if the nature of the conduct and/or relationship is such that raising the issue is not possible or uncomfortable for you, you can submit a complaint to the AFM Complaints Committee. Doing this requires great care, as the impact can be dramatic and confrontational for all parties involved.

Based on an investigation into the complaint, the Complaints Committee will issue an opinion on the plausibility of the complaint and can ultimately decide to impose an employment measure. It is both a commitment and requirement for the AFM to act as a good employer, and as such the AFM wishes to generally protect employees against unfair treatment. These regulations are a means for employees to put a stop to a situation that is undesirable for them.

The procedure is not intended for personal grievances in relation to conflicts in the workplace or similar matters. The AFM Complaints Procedure covers these matters, which is open to anyone who wishes to submit a complaint regarding any act and/or failure to act by the AFM and its employees. Nor should these regulations be used for complaints in relation to privacy. Complaints of this type can be submitted under the AFM Complaints Procedure and will be dealt with by the Data Protection Officer at the AFM. For any complaints relating to both undesirable behaviour and the complainant's privacy, the Complaints Committee will involve the Data Protection Officer at the AFM when dealing with the complaint.

1. Complaints Committee

1.1. The AFM has established a Complaints Committee that will review complaints in accordance with these regulations. The AFM will provide the Complaints Committee with the facilities it reasonably requires for the performance of the duties it has been tasked with.

1.2 The Complaints Committee consists of the general counsel, a compliance officer and a confidential counsellor. The Executive Board will appoint them committee members. The general counsel will fulfil the role of chair. In the event that one of the members is unable to participate, the chair of the Executive Board is authorised to appoint one or more other employees to the committee. The primary consideration for this appointment will be the independent position of these individuals.

1.3 Members of the Complaints Committee must withdraw in the event that they are involved in the complaint or any circumstances surrounding it, as well as in the event that an actual or apparent conflict of interests arises. In such cases, the chair of the Executive Board will appoint another employee to the committee.

1.4 The Complaints Committee will be supported by a secretary to be appointed by the Executive Board. The Complaints Committee will elaborate the remit of the secretary further.

1.5 It is the responsibility of the Complaints Committee to:

a. Record a complaint;
b. Determine whether a complaint is founded;
c. Investigate complaints submitted to the Complaints Committee;
d. Provide a written opinion stating reasons to the chair of the Executive Board on whether the allegations made by the complainant appear plausible;
e. Provide a written opinion stating reasons to the chair of the Executive Board on any measure to be imposed. If this measure is an employment measure, the advice of the head of HR must be sought.

1.6 In the course of the investigation, the chair of the Executive Board, having consulted the Complaints Committee, may decide to take temporary employment measures and/or launch a special investigation. In case of the latter, the chair of the Executive Board may decide to suspend the time limit referred to in Section 4 of these Regulations.

2. Submitting a complaint

2.1 Anyone who has been faced with undesirable behaviour is able to submit a complaint about this to the chair of the Complaints Committee.

2.2 Complaints must include:

a. The name of the complainant;
b. A description of the behaviour that is the subject of the complaint and the period over which said behaviour has taken place or is taking place;
c. The name of the accused person or persons and, if applicable, any witnesses;
d. A description of the steps the complainant has already taken and any written documents pertaining to these;
e. The date and the complainant's signature.

2.3 The Complaints Committee may ask the complainant to provide a verbal explanation to the complaint submitted.

3. Consideration of a complaint

3.1 Within 5 working days of having received a complaint, the Complaints Committee will send the complainant written confirmation of receipt and a copy of this complaints procedure. The confirmation will state the date on which the complaint was received.

3.2 The Complaints Committee must inform the complainant within 10 working days of receipt whether their complaint is admissible.

3.3 The Complaints Committee is not under any obligation to consider a complaint if:

a. The complainant has not attempted to resolve the matter through other routes;
b. The complaint does not pertain to undesirable behaviour as described in the Code of Conduct;
c. The complaint has been submitted on behalf of others;
d. The complaint has been made anonymously;
e. The Complaints Committee is of the opinion that, following a request for further information, the complainant has not adequately enabled the committee to take cognizance of relevant information necessary in order to consider the complaint;

f. The Complaints Committee has considered the complaint previously, unless there are new facts or circumstances;
g. The behaviour which is the subject of the complaint dates back more than one year, unless there are new facts or circumstances;
h. The behaviour is the subject of legal proceedings, whether ongoing or concluded;
i. The behaviour that is the subject of the complaint is being investigated or prosecuted by the police or judicial authorities.

3.4 In the event the complaint is declared admissible, a notification will be sent to the complainant, the accused and the Executive Board.

3.5 In the event the complaint is declared admissible, the accused will receive a copy of the complaint. The accused will be given the opportunity to put forward a defence to the Complaint Committee within 10 working days of receipt of the copy. The defence must be sent to the chair of the Complaints Committee.

3.6 Within 5 working days of having received the defence, the Complaints Committee will provide a copy thereof to the complainant for information.

4. Complaints handling – Investigation and hearing

4.1 If the Complaints Committee decides to declare a complaint admissible, it will begin a substantive examination.

4.2 The Complaints Committee will carefully examine whether a complaint is founded. To this end, the Complaints Committee will hear the complainant and the accused, and have the option to consult other internal or external individuals, witnesses and/or experts, whether or not based on information provided by the complainant or the accused. The Complaints Committee will be able to hear individuals on multiple occasions.

4.3 The complainant and the accused will be heard at separate hearings, unless both the complainant and the accused declare that they have no objection to a joint hearing.

4.4 The Complaints Committee will have access to documents, systems and individuals as needed in order to arrive at an opinion. The relevant individuals will be obliged to lend their cooperation and appear at any hearing that is held. The time required for this purpose will be considered working time.

4.5 Each hearing will be attended by no less than 2 members of the Complaints Committee. The Complaints Committee will prepare minutes for each hearing, which the person heard must sign for approval, with or without comments, within a reasonable time limit to be set by the committee. If the person heard refuses to sign, this will be noted in the report, stating the reason(s). If there is no response within the time limit set by the Complaints Committee, this will be taken as tacit approval.

4.6 In the interest of ensuring the records are as complete as possible, an audio recording may be made during the hearing, provided the persons to be heard have agreed to this. This audio recording is for supplementary purposes only and will not replace the written report of the hearing.

4.7 The complainant and the accused are granted privacy rights under the General Data Protection Regulation (GDPR), including a right of access to all documents pertaining to the complaint, unless a ground for exclusion as provided for in the GDPR applies.

4.8 The complainant and the accused have 5 working days within which to respond to the documents prepared for use by the Complaints Committee.

4.9 The complainant and the accused may ask an adviser internal or external to the AFM to support them during the hearings. The AFM may reimburse the cost of an adviser up to a reasonable amount.

5. Opinion by the complaints committee

5.1 No later than 6 weeks after receipt of a complaint, the Complaints Committee will communicate its opinion on the admissibility of the complaint in a written report stating reasons to the chair of the Executive Board, in accordance with the provisions of section 4.3.

5.2 In the event that it is not possible to complete the recommendation within the specified time limit, the Complaints Committee is able to extend the time limit by a maximum of 4 weeks. The Complaints Committee will communicate such extensions to the complainant, the accused and the chair of the Executive Board in writing. Further extension will be possible if the complainant agrees to this in writing.

6. Decision by the chair of the Executive Board

6.1.a Within 10 working days of receipt, the chair of the Executive Board will use the recommendation issued by the Complaints Committee to rule on the complaint. If the chair of the Executive Board deems the complaint plausible, the complaint will be upheld and the chair may then decide to impose a measure. If this measure is an employment measure, the advice of the head of HR will be sought prior to this decision.

6.1.b In the event that the chair of the Executive Board decides not to follow the recommendation of the Complaints Committee, the chair will set out the arguments for this in the decision. The intention to deviate from the recommendation must be discussed with the Complaints Committee before any decision to do so. In this event, the time limit specified under a in the first subsection will be extended by 10 working days.

6.1.c If an employment measure is imposed, the accused will be entitled to provide a response to this. The Executive Board must submit this response within 10 working days from the announcement of the intended decision. The assessment of the accused's response will include a request to the Head of HR for advice.

6.1.d The decision taken by the chair of the Executive Board, including the recommendation by the Complaints Committee and the hearing reports, will be notified to the Complaints Committee, the complainant and the accused in writing.

6.2 The chair of the Executive Board may decide to consult the other members of the Executive Board on an anonymous basis with regard to the recommendation and the measures to be taken.

6.3 At the request of the complainant and/or the Complaints Committee, the chair of the Executive Board may put in place temporary measures both before and during the handling of

the complaints, if this is necessary in the interest of the complainant's well-being and/or the circumstances are deemed untenable for one or more of the directly affected parties.

6.4 The complainant is able to withdraw the complaint up until the time the Complaints Committee issues its recommendation to the chair of the Executive Board. Withdrawal must be effected by means of a written notification to the Complaints Committee. In the event of a withdrawal, the Complaints Committee will ensure the file is destroyed.

7. Confidentiality

7.1 Anyone involved in the handling of a complaint based on this procedure will be subject to a duty of confidentiality. Disclosure of information to parties not involved in the complaint is not permitted unless this is strictly necessary for the proper handling of the complaint or disclosure is required under any statutory obligation. The privacy of the complainant and the accused will be safeguarded. This duty of confidentiality also extends to the decision-making process by the chair and involved members of the Executive Board.

7.2 The duty to maintain confidentiality does not apply to the extent that the complainant or the accused wishes to request the assistance of individuals who are subject to a duty of confidentiality by virtue of their office or position, or wish to report criminal offences in respect of the conduct to which the complaint is related.

8. Legal protection

8.1 There is no possibility to object or appeal against decisions taken by the chair of the Executive Board based on these regulations.

8.2 Unless a legal right is found to have been abused, the complainant and witnesses may not suffer any disadvantage in relation to their legal position because of the submission of a complaint or their role or actions under these Regulations.

8.3 Accused persons will also have their legal position protected. This means the accused will be deemed innocent until proven otherwise.

8.4 The members of the Complaints Committee cannot be held liable for recommendations made by the Complaints Committee or any act of failure to act in their capacity as members of the Complaints Committee.

9. Documentation and reporting

9.1 The accused will only have the measure imposed and the reasons for this recorded in their personnel file. The accused will be informed of this in writing. The Complaints Committee will provide the information required for this to the Head of HR.

9.2 The Complaints Committee will include an anonymised entry regarding the complaint in the annual report on integrity violations to the chair of the Executive Board. This report will be made available to the Works Council at the same time.

10. Supervisory Board

Where a complaint relates to conduct by a member of the Executive Board, the tasks and powers set out in these regulations for the chair of the Executive Board will be taken over by the chair of the Supervisory Board.

11. Privacy

The compliance officer will treat any data and information received in connection with a complaint or an investigation as confidential at all times, requesting advice from the Data Protection Officer (DPO) as necessary. All relevant documentation regarding the investigation and the processing of the relevant personal data will be stored in accordance with the guidance provided in the General Data Protection Regulation (GDPR) and other applicable laws and regulations, and will be retained in accordance with the AFM data retention policy. More information about the employee's privacy rights under the GDPR have been included in the internal privacy regulations for AFM employees.

12. Applicability and entry into force of these regulations

These regulations were revised in a number of respects and will enter into force on 1 January 2021. These regulations apply to all AFM employees.