Handling inside information by listed companies – Best Practices

Update May 2021 – insider lists and access to inside information

The Netherlands Authority for the Financial Markets (AFM) considers it important that companies which have issued financial instruments which are listed on an exchange continuously pay attention to the correct handling of inside information. At the end of 2015, the AFM began a market-wide review of the process of drafting, disclosure and dissemination of inside information by listed companies. The purpose of this review was to get a better idea of how press releases are drafted, how they are disseminated and how confidentiality of inside information is ensured until the moment of disclosure. Particular focus lay on the role of external organisations, such as service providers, in this process. This review resulted in the publication of best practices.
At the end of 2018, the AFM started a second review with listed companies regarding the risks of cybercrime in relation to keeping inside information confidential, both internally and by the external organisations inside information is shared with. The second review resulted in these updated best practices.

Update 2021

In 2020, the AFM conducted a review of how companies were dealing with inside information, focusing on ensuring that insider lists are complete and up to date. We also asked listed companies to state the extent to which they, and organisations that they work with, were aware of the persons who have access to inside information and at what times, and what type of access they have (reading, processing or removal of information). The AFM is now publishing an updated version of best

practices based on this most recent review. Three items have been added: compiling an insider list, access to insider information and cooperation with third parties. These items are marked as 'update 2021'. The best practices do not encompass (new) regulations in itself. Instead, the best practices provide examples and tips from daily practice that may assist organisations in the testing or refining of their relevant procedures. Lastly, the AFM wishes to note that this document also contains references to existing statutory obligations. However, this document does not provide an exhaustive list of all statutory obligations, and moreover does not take precedence over legislation and regulation. For more information on how to deal with inside information, the AFM refers to applicable legislation and regulation, and the various brochures on the website of the AFM dealing with the treatment and publication of inside information.

Confidentiality of inside information

- **Always ensure your inside information is secure.** For example, this can be achieved by drafting and storing a press release in a restricted digital environment, by encrypting the content or by protecting the document with a solid password.
- **Avoid unprotected distribution** of inside information by email**,** both internally and externally. This also applies to draft versions.
- **Keep procedures and training up to date.** Make use of written procedures and hold regular training sessions with your employees about the handling of inside information within your organisation.
- **Make adequate arrangements in order to safeguard the confidentiality of inside information and test the effectiveness of these arrangements** (e.g. with pen tests, audits, etc.). Make sufficient procedural, technical and organisational arrangements in order to safeguard the confidentiality of inside information. Let your cyber resiliency be tested regularly by cyber specialists. Make sure that you assess the effectiveness of such arrangements with external organisations. Consider whether the external organisation has made the sufficient arrangements to be allowed to process your inside information.
- **Awareness over a longer period.** In some cases, inside information may build up over a longer period or develop further (e.g. during ongoing takeover talks). Make sure that, in those situations, awareness with regard to the handling of inside information remains front-of-mind during the entire period and not only at the start or the end of the period. You may appoint a person in your organisation (e.g. your compliance officer) to monitor the confidential handling of inside information throughout the entire process. The main point is that one person is given responsibility for central coordination and for bringing

the issue of inside information to the attention of team members by, for example, sending reminders, but also by addressing the issue during meetings. Awareness can also be maintained through presentations or trainings.

- **The importance of a complete and up to date insider list.** Provide for a complete and up to date insider list by using the template which is included in the annexes of the implementing regulation (EU) 2016/347. Do not forget to register all persons who come into contact with inside information including support staff (e.g. secretary and post room employees). It is required to update the insider list continuously. The AFM may request this insider list from you. In case many external parties, such as consultants, are informed of the inside information, it is important to emphasize to these external parties that they must establish and maintain a complete picture of the total group of insiders (also when these people are not involved anymore with the inside information). This is regarded as an important part of ensuring the confidentiality of inside information by listed companies.
- **Confidentiality agreement.** Let your employees sign a confidentiality agreement and a code of conduct. If you select an external organisation to draft or review a press release (e.g. a translator or legal counsel), record confidentiality in a contract.
- **Media monitoring.** In case you have postponed disclosure of inside information, do not only monitor trading of your financial instruments on stock exchanges but also monitor news and social media reports for signals about inside information that might have leaked. Make sure that an emergency press release is always ready for disclosure.
- **Contact with the AFM.** In case of incidents, e.g. if you suspect that inside information has been leaked, immediately contact the AFM monitoring team by dialling +31 20 797 3777.

Compiling an insider list (update 2021)

- **Consciously consider who is made aware of inside information and who is not.** This also involves the decision of who should be on the insider list and who should not. The reason why a person has access to inside information and why one is included on the insider list has to be stated explicitly on the insider list, along with their job title and role. It is important that this consideration is made in a consistent manner throughout the organisation. The insider list has to provide a full account of the persons who are aware of inside information, without unnecessarily increasing the number of persons involved. Furthermore, you should also pay attention that persons participating in the decision-making organs who are accordingly aware of such information are included on the insider list.

- **Human behaviour is an important factor when dealing with inside information.** However strong the security of inside information is technically and procedurally organised, the safeguarding of confidentiality ultimately depends on human behaviour. Continuing attention to human behaviour and a good balance between hard and soft controls is therefore needed. The exemplary behaviour within a company plays an important role as well. You should also make employees aware of how they should respond to situations in which confidential information is accidentally shared.
- **An automatic link between the insider list and an authorisation, HR or billing system for example** reduces the likelihood that an insider is not included on the insider list or that an insider's personal details on the list are incorrect or incomplete. Do not allow anyone access to inside information before they are placed on the insider list. Conversely, a person can be automatically placed on the insider list at such time as they are given digital access to inside information.
- **Automation will help to reduce the administrative burden.** Ensure that all the documents related to, or qualified as, inside information are readily available at one location or in one single system. If software tools from an external party are used to log the insider list, ensure that external parties are excluded from access to inside information. If this cannot be avoided due to the need for technical assistance, ensure that the relevant persons at the external party with access to inside information are also included on the insider list.
- **Insight and awareness among insiders.** Ensuring that a notification on the insider list or signature to acknowledge that information is confidential does not consist of a simple check box or mouse click will help to raise awareness with respect to inside information. It is also helpful if the insiders at a company are aware of who else is an insider, so that they know with whom they may or may not discuss the inside information known to them.
- **Designate one person as ultimately responsible.** Experience from market participants shows that an effective approach is to make one person ultimately responsible for ensuring that the insider list is complete. This person has to have insight into who is aware of inside information and when they become aware of it, also if the persons concerned work in different departments or take part in different decision-making organs. And of course, there needs to be a back-up for this person with ultimate responsibility.
- **Knowledge of ICT is important for teams that keep insider lists up to date.** ICT processes are an integral part of the process of the management of inside information. Ensure that employees charged with monitoring the confidentiality of inside information also have adequate knowledge of ICT processes and information security.
- **Relationship between the MAR and the GDPR.** The obligations relating to insider lists in the

Market Abuse Regulation (MAR) and the General Data Protection Regulation (GDPR) co-exist and do not interfere. One practical example of compliance with both obligations is if the personal details in the insider list are kept separate, in such a way that there is a simple link to these personal details at such time that a supervisor requests to view the insider list.

Access to inside information (update 2021)

- **Ensure that there is continuous and adequate insight into who has had access to inside information, the date and time that they had such access, and the nature of the access (reading, changing or removal of information).** Manual or automated monitoring of who actually has access to inside information means that the management of inside information will include ensuring that no unauthorised persons have access. This also means that it can be checked that the right persons are included on the insider list.
- **Confirm that all users (internal, external and temporary personnel) and their activities in the ICT systems are identifiable and traceable**. Also ensure that all the activities of privileged accounts[1], such as those of system managers, are identified and monitored in relation to the treatment of inside information.
- **Grant access rights in accordance with job and process requirements.** Ensure that people only have access to the information and ICT systems necessary to perform their duties.
- **Monitor and continually improve the control framework[2] for the process of dealing with inside information in order to achieve the process objectives**. Information Security (IS) is an integral part of the process of the management of inside information. It is important that the effectiveness of the measures is tested regularly, also in combination with the other IS measures in force at the company. Findings must be communicated and followed up within the company for the control framework to be effective.
- **Regular evaluation of the process of management of inside information is important.** This ensures the possibility to assess whether there are vulnerabilities in the process and whether improvements are needed.

[1] Privileged access means all accounts with higher access rights than standard users. Examples of human privileged access accounts are super-users such as system managers, domain managers and local administrators. An application account for application management and configuration is an example of a non-human privileged user. Cyberattacks are frequently based on abuse of privileged accounts.

[2] The purpose of a control framework is to establish the minimum controls necessary at organisation level to comply with the requirements set for the various themes of access control, logging and monitoring.

Cooperation with third parties (update 2021)

- **Obligations for issuers and third parties.** If a listed company cooperates with external advisers, such as accountants, legal or financial advisers or consultants, it is important to realize that compiling an insider list and keeping it up to date is an obligation for both an issuer and the persons acting on its behalf or for its account. This is an obligation under the MAR. It is important that there is clear mutual communication of the existence of inside information and the responsibilities relating to this.
- **Agreements on information security.** Based on its insight into supply chain dependencies, a company should make efforts to conclude agreements on information security with other parties with which it cooperates. This should include agreements on mitigating the impact of incidents, such as unauthorised access to inside information, for both the company in question and the entire chain. These agreements should be established, for example by means of non-disclosure agreements (NDAs).

Drafting a press release with inside information

- **Appoint a 'disclosure committee'.** Appoint a fixed small group of employees who meet regularly to discuss the contents of press releases with inside information, to determine the moment of publication and to document potential delayed disclosure of inside information. A 'disclosure committee' meets both regularly and ad-hoc and is composed of employees (e.g. a member of the Board, legal counsel, Investor Relations, Communication department) who are each placed on the insider list of your organisation.

Disclosure and dissemination of a press release with inside information

- **You must disclose inside information as soon as possible.** You can do so during exchange trading hours, as well as before or after. The obligation to disclose inside information as soon as possible should prevail over the benefits of publishing press releases before or after exchange trading hours.
- **It is your responsibility to disclose and disseminate inside information as quickly as possible by the external organisation that you have hired.** The time between transmission of inside information to the third party which takes care of the dissemination of your press releases and the actual disclosure to press agencies or media must be kept as short as possible. You must therefore make clear arrangements with the external

organisation about this. Make sure that you can get in touch with the relevant contact person and keep in mind that they must also be available after hours.

- **Only hire specialised agencies.** In case you select a third party to handle the publication and dissemination of your press releases, be sure that this organisation is specialised in the process and that it can offer you a secure platform where you can upload your press releases and which can distribute them simultaneously to various media at the time that you have specified.
- **It is your responsibility to keep inside information confidential, including when you share the information with an external organisation.** Remember that inside information may only be shared with external organisations if it is really necessary. If so, do not only rely on the name or reputation of the external organisation, but discuss, and stipulate in a contract, how confidentiality and due diligence in the handling of inside information is safeguarded by the external organisation. Communicate about inside information only in a secure way, preferably with two factor authentication or in an encrypted environment. Keep inside information encrypted until it is published. Make arrangements about the communication of inside information within the external organisations. The group of persons within the external organisation with access to any inside information should be as small as possible. This group must also be placed on the insider list.
- **Be careful with setting up a press release.** Use codes (such as 'XXX') for sensitive information such as material numbers or company names when communicating with an external organisation about a press release and do not fill in the numbers and names until the press release is ready for publication. Do not place a press release on your website in advance of its publication. Upload the press release on your website and in the distribution system only at the very last moment. Furthermore, you may only deposit your press release into the AFM's register after it is published.

Disclaimer: these best practices are for informational purposes only. No rights can be derived from the above information. In case the wording of these best practices differs from the wording and explanation of the Regulation, the Regulation prevails.