Speaking Up and Protection of Disclosures.

Introduction

Exicon, formerly KBC Bank Ireland, is strongly committed to supporting a responsible and ethical organisational culture. We pride ourselves on the integrity that we bring to our daily work and recognise the importance of that integrity being at the core of how we operate for the benefit of our customers.
From time to time, however, things can go wrong and when that happens Exicon should be informed so we can take action to remedy matters. We aim to foster a working environment where employees feel comfortable in raising concerns relating to potential wrongdoing within Exicon and to provide the necessary supports for those who raise genuine concerns. This sort of working environment reflects our core values especially those of "empowerment" and "accountability". A commitment to integrity, professionalism, openness, and transparency are also a key part of these values.

Protection of the Discloser

Exicon guarantees that a Discloser who speaks up or makes a Protected Disclosure under the Policy on *Speaking up and the Protection of Disclosures* will be protected from penalisation as a result of raising their concerns.

A report made under this Policy is:

1) A report of information which in the reasonable belief of the discloser tends to show wrongdoing has occurred, is occurring or is likely to occur; and
2) A report made either internally or externally (to competent authorities such as the Central Bank of Ireland "CBI") in accordance with this Policy.

Any instruction or contractual term which would prevent a worker from disclosing concerns in accordance with this policy is wholly inappropriate and will be void. Furthermore, Exicon will not permit any other person to penalise or threaten penalisation against a worker who makes a disclosure pursuant to these standards. A complaint that a worker has been penalised following a disclosure can be made directly to the Chair of the Executive Committee, Chair of the Audit Committee or Chair of the Board of Directors.

It would also be a breach of this policy to:

• Attempt to quash/divert/mischaracterise a disclosure; and / or
• Attempt to penalise the discloser by any member of staff (either to whom a disclosure has been made or who has become aware of same and negative behaviour is related to that disclosure).

Where, following investigation, it is deemed that there is no case to answer, but the person who made the report reasonably believed that there was wrongdoing, the person will suffer no adverse consequences for making the report.

Exicon must not disclose the identity of the discloser unless permitted or required to by law. The discloser shall be informed before their identity is disclosed unless such information would jeopardise the related investigations or judicial proceedings. Any report made pursuant to The Policy on Speaking Up and Protection of Disclosers in relation to wrongdoing as defined in the policy will be considered to be a protected disclosure within the meaning of the Protected Disclosures Act 2014. Disclosers who report concerns anonymously, but who are subsequently identified and suffer retaliation, will qualify for protection.

How to make a Protected Disclosure

Concerns about wrongdoing should be reported through any possible channel of communication. Internally this can be done by letter, e-mail, phone, personal discussion, online reporting tool etc or to an appropriate

external third party. Reports may also be made to the CBI and relevant contact details can be found at **Protected Disclosures & Whistleblowing | Central Bank of Ireland.** External reports can be made using the **Secured Reporting Channel for Protected Disclosures in Exicon which is the EQS Integrity Line reporting tool.**

We will acknowledge concerns reported within seven days of Exicon being in receipt of the disclosure.
In order to support a thorough investigation, disclosures should, insofar as possible, provide the following information in their reports:

- Name and contact details of the discloser;
- Description of the concern with all relevant facts known to the discloser (what happened, where, what specific behaviour gave rise to the concerns being reported, who is involved, etc.);
- The period of time during which the discloser observed the matter or irregularity giving rise to the concern;
- How the concern came to the attention of the discloser;
- An indication of why the matter is being reported;
- An indication of whether the matter has already happened or may happen in the future;
- An indication of how the discloser obtained his/her knowledge of the incident or situation;
- Whether there are other persons involved or other potential witnesses; and
- Any supporting information available to the discloser.

It is important to note that any relevant concerns can still be raised, even if the concrete facts are not known in detail. Where the discloser has a "reasonable belief" that information obtained in the course of their employment indicates wrongdoing, the protections guaranteed by the Protected Disclosure Act 2014 will apply. When obtaining the information, the discloser is required to respect all legal and regulatory rules and internal guidelines.

For the sake of the thoroughness of investigations, and with a view to protecting all those concerned and avoiding a culture of anonymous reporting, preference is given to confidential reporting by identified individuals. If circumstances demand, concerns may be reported anonymously. Anonymous reports will also be investigated within the framework of these standards.

Follow up

Exicon will provide a 7-day acknowledgement to the discloser and also provide updates to the discloser every 3 months. From time to time, Exicon will be required to contact the discloser to obtain additional information prior to escalation for investigation. The communication with the Discloser should be held mainly within secured inbox in EQS Integrity Line the third-party reporting tool used by Exicon.

Record Keeping

Exicon must keep records of every disclosure received, in accordance with the confidentiality requirements. Disclosures shall be stored for no longer than it is necessary and proportionate in order to comply with the requirements imposed by European Union or national law. For cases reported through the EQS Integrity Line, records can be downloaded and saved locally as required.
Where a recorded telephone line or another recorded voice messaging system is used for reporting, subject to the consent of the discloser, Exicon has the right to document the oral reporting by making a recording of the conversation or through a complete and accurate transcript. Exicon will offer the discloser the opportunity to check, rectify and agree the transcript of the call by signing it.
Where an unrecorded telephone line or another unrecorded voice messaging system is used for reporting, Exicon has the right to document the oral reporting in the form of accurate minutes of the conversation written by the person managing the case. Exicon will offer the discloser the opportunity to check, rectify and agree the minutes.

Data Retention

Personal Data not related or irrelevant to the investigated case will be deleted immediately once the investigation has formally finished and notification has been sent to the Discloser. Personal Data related to Disclosures where it has been confirmed Exicon rules and policies were violated (but not a violation of legislation) will be deleted after 2 years once the investigation is formally finished and notification sent to the Discloser. Personal Data related to the reported Breach where the legislation was violated, and such an act can be labelled as a crime will be deleted after 10 years once the investigation has formally finished and notification sent to the Discloser.

Information on Protected Disclosures

What is a Discloser?

A person who reports/discloses concern(s) regarding potential or actual wrongdoing. Based on the definition of "worker" provided by the Protected Disclosure Act 2014, this includes: all directors, all employees and ex-employees of Exicon and all persons who work or worked for Exicon, in circumstances in which they were introduced or supplied to Exicon to work by a third person and the terms under which they are or were engaged to do the work are or were in practice substantially determined, not by them, but by Exicon and/or the third person. It also includes persons whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other precontractual negotiations and persons whose work-based relationship has ended.

What is wrongdoing?

Wrongdoing, regardless of where in the world the suspected wrongdoing has taken place, can be the subject of a protected disclosure, in accordance with the Protected Disclosures Act 2014. 'Wrongdoing' for the purposes of this policy includes a breach or, likely breach, of law, regulations, codes. Wrongdoing would also include the breach or, likely breach, of Exicon internal Codes, mandates and frameworks, or unethical behaviour or conduct. Examples of wrongdoing include but not limited to the following; that a miscarriage of justice has occurred, is occurring or is likely to occur, that a breach of any regulation or code issued by a relevant authority (e.g. the Consumer Protection Code (CPC)) or policy published by Exicon has been committed, is being committed or is likely to be committed or that a miscarriage of justice has occurred, is occurring or is likely to occur.