Whistleblower Protection Policy

Governance Policy | Global

Version 2.0 · July 2026 · Confidential — Internal Use

This document is a template intended to be reviewed, tailored and approved by your organisation before use.
Replace all references to "the Company" with your organisation's name.

Document Control

Document name	Whistleblower Protection Policy
Document type	Governance Policy
Jurisdiction	Global
Owner	Company Secretary
Approved by	Board of Directors
Version	2.0
Effective date	July 2026
Review cycle	Annual
Next review due	July 2027
Classification	Confidential — Internal Use

Contents

1. Purpose

This Policy sets out how the Company receives, protects and handles disclosures of misconduct or an improper state of affairs. It exists to encourage the reporting of wrongdoing by making it safe to speak up: a person who makes a Protected Disclosure must not suffer Detriment for doing so, and the Company must keep their identity confidential except in the narrow circumstances permitted by this Policy and applicable law.

The Policy implements international good practice for whistleblowing management systems. It is designed around ISO 37002, which structures a whistleblowing programme on the principles of trust, impartiality and protection across the full lifecycle of receiving, assessing, addressing and concluding reports; it supports the speak-up obligations of the Company's compliance management system under ISO 37301; and it gives effect to the expectation in the G20/OECD Principles of Corporate Governance and the BCBS Corporate Governance Principles for Banks that boards ensure staff and other stakeholders can raise concerns about illegal or unethical conduct without their rights being compromised. Where a statutory protected-disclosure regime applies in a jurisdiction in which the Company operates, this Policy operates alongside, and never below, that regime.

Beyond compliance, the Policy is an integral part of the Company's risk management and governance framework. Disclosures are frequently the earliest signal of fraud, regulatory breach, or conduct and culture failures, and the Board regards an effective, trusted whistleblowing programme as a core detective control and as a measure of the health of the Company's culture.

This Policy is approved by the Board of Directors and owned by the Company Secretary.

2. Scope

This Policy applies to the Company and to all of its subsidiaries and controlled entities, across all business lines, products, channels and locations. Where the Company operates through branches or joint ventures, the Company must apply this Policy to the fullest extent it is able to under the relevant governance arrangements.

The Policy applies to every person who may make a disclosure as described in the Who Can Make a Disclosure section, whether or not they currently work for the Company, and to every officer, employee, contractor and secondee of the Company in their capacity as potential recipients or handlers of disclosures.

The Policy governs disclosures of Reportable Wrongdoing. It does not apply to Personal Work-related Grievances, which should be raised through the Company's grievance and human resources procedures (see the Matters outside this Policy sub-section of the How and to Whom to Make a Disclosure section); however, a matter that is partly a grievance and partly Reportable Wrongdoing is covered by this Policy, as is any grievance that concerns Detriment for making a disclosure.

Nothing in this Policy limits, and no agreement (including any employment contract, settlement deed or confidentiality agreement) may be applied by the Company to exclude or reduce, any protection available to a Discloser under applicable law. Where applicable law confers protections broader than this Policy, those protections apply in full.

Jurisdictional application. This Policy states international best practice for whistleblower protection. The Company must map the requirements of this Policy to the law of each jurisdiction in which it operates — including any statutory protected-disclosure regime, employment law, data protection law and mandatory reporting obligations — and document that mapping. Where local law imposes a stricter or additional requirement, local law prevails and must be complied with.

The mapping must record, for each jurisdiction and legal entity, whether applicable law requires a reporting channel, a designated recipient or a policy to be established at entity level rather than group level, and any local acknowledgement or feedback deadlines. Where entity-level arrangements are required, the Company Secretary must ensure that a local Designated Recipient is appointed and recorded in the mapping, trained to the standard in the Training and Awareness section, and required to notify the WPO of each disclosure within [X] business days on a de-identified basis unless local law prevents it, in which case the mapping must record how group oversight is achieved. Any gap in required entity-level arrangements must be reported to the [Audit / Board Audit and Risk] Committee within [X] business days of identification.

3. Definitions

Term	Definition
Reportable Wrongdoing	Conduct, or an improper state of affairs or circumstances, in relation to the Company or a member of its group that a Discloser has reasonable grounds to suspect involves a breach of law or regulation, fraud, corruption, danger to persons, the environment or the financial system, or other misconduct described in the What Can Be Disclosed section of this Policy. A suspicion may be reasonable even if it later proves to be incorrect.
Discloser	A person who reports, or is believed or suspected to have reported or to be about to report, Reportable Wrongdoing under this Policy. The term corresponds to the "reporting person" concept in ISO 37002 and includes current and former workers and the other categories set out in the

	Who Can Make a Disclosure section.
Detriment	Any disadvantage caused, or threatened, to a person because of an actual, suspected or anticipated disclosure, including dismissal; demotion or withheld promotion; alteration of duties, hours or location to the person's disadvantage; discrimination, harassment, intimidation or ostracism; harm or injury, including psychological harm; damage to property, reputation, business or financial position; blacklisting; and any other damage to a person.
Eligible Recipient	A person or body designated under the How and to Whom to Make a Disclosure section of this Policy as authorised to receive disclosures of Reportable Wrongdoing, including the WPO, officers and senior managers of the Company, the external auditor, and the independent external reporting channel.
Anonymous Disclosure	A disclosure made without the Discloser revealing their identity to the Company or to the external reporting channel. Anonymous Disclosures are accepted and handled under this Policy on the same basis as named disclosures, so far as investigation is practicable.
External Disclosure	A disclosure of Reportable Wrongdoing made to a Competent Authority, or (where and to the extent permitted by applicable law) to another external party such as a member of the legislature or a journalist, as described in the Competent Authorities and legal advisers sub-section and the Wider public disclosures sub-section of this Policy.
Competent Authority	A regulator, supervisor, law enforcement body or other public authority empowered under applicable law in the Company's operating jurisdiction(s) to receive, and where applicable to act on, reports of wrongdoing — for example the Company's prudential regulator, the conduct regulator, the financial intelligence unit (FIU), the tax authority, an anti-corruption agency or the police.
Personal Work-related Grievance	A grievance about a matter relating to the Discloser's current or former employment or engagement that has implications for the Discloser personally (such as an

	interpersonal conflict or a decision about promotion, transfer, discipline or termination), that does not concern Detriment for making a disclosure and does not otherwise involve Reportable Wrongdoing.
Protected Disclosure	A report of suspected wrongdoing made through a channel described in the Company's whistleblowing arrangements, or otherwise qualifying for protection under applicable local law, which attracts the confidentiality, non-retaliation and support commitments of those arrangements or of the law, whichever affords the greater protection.
Senior Manager	A person, other than a director, who holds senior executive responsibility for the Company or for a significant business unit or control function, including any person designated, registered or approved as such under the senior manager accountability regime applicable in the Company's operating jurisdiction(s) or, where no such regime applies, under the Company's own accountability arrangements.
Whistleblowing Investigation Register	The restricted-access register maintained by the WPO recording all disclosures received under this Policy, their assessment, investigation status, outcomes and remediation actions.
Whistleblower Protection Officer (WPO)	The senior officer appointed by the Board as the Company's central authorised recipient of disclosures, responsible for triage, protection of Discloser identity, oversight of investigations and reporting under this Policy. The WPO performs the whistleblowing management function contemplated by ISO 37002.
Whistleblower Support Officer (WSO)	An officer appointed by the WPO, independent of the investigation, responsible for the welfare and support of a Discloser and, where appropriate, of persons mentioned in a disclosure.
Conflict of Interest	A situation in which a person's private interests, relationships, financial or family interests, or duties owed to another person or entity, could improperly influence, or could reasonably be perceived to influence, the performance of their duties to the Company or its

End of preview

This is a preview extract. The complete document continues beyond the pages shown here.

The full document is supplied as a single, fully editable Microsoft Word (.docx) file immediately after purchase — including every remaining section, the definitions, the regulatory framework references and all appendices and templates.

Bracketed prompts such as [30 days] mark the points where your own thresholds, committee names and local regulatory references are inserted.