Directive
Business Integrity and Speaking Up

April 1,2021

Requirements

Holcim conducts business across the globe. The way we conduct business is subject to the standards set in the Group Code of Business Conduct (the "Code") which apply to everyone. We conduct business with integrity.

To support transparency over our conduct and business integrity, we encourage a culture of speaking up, in which employees and others can report their concerns regarding business conduct. Concerns can be raised through the IntegrityLine website or hotline or directly to managers. Reported concerns are assessed and investigated so as to ensure that corrective action can be taken as applicable.

The purpose of this directive is to list the key requirements for ensuring business integrity through speaking up about concerns and the conduct of investigations. In respect of the conduct of investigations, the requirements include those for investigations into reported breaches of the Code and those into security incidents.

On speaking up:

- Reporting a suspected violation of the Code is an obligation for all employees and is to be encouraged and fostered by management.
- All employees are encouraged to ask questions concerning what is the right business conduct and what they should do if they encounter conduct they believe is wrong.
- Reports should be made either to a manager, to local, region or group legal and compliance, or through the IntegrityLine website or hotline; they should relate to suspected violations of the Code, state specific facts (not opinions) relevant to the allegation, and not include general employee grievances or other complaints. Reports to management shall be forwarded to the IntegrityLine.
- Reports should never be untruthful.
- Although reports may be made anonymously, reporters are encouraged to identify themselves where they feel confident to do so. The identity of the reporter and the content of the report shall be kept confidential and only disclosed to those who need to know for the purpose of the investigation or remedial action.
- Retaliation against anyone reporting in good faith is a violation of the Code and is not tolerated. Confirmed reports of retaliation shall be subject to disciplinary sanction.
- Group Compliance will maintain a global system for the purpose of facilitating reports and tracking the handling of reports and investigations through to closure and remediation.

On investigating speak up reports and security incidents:

- Reports concerning breaches of the Code are assessed and assigned for investigation under the oversight of the Group's Ethics, Integrity and Risk Committee.
- Security incidents are reported using the Security Incident Notification Tool[1] and are assessed locally. Any consequent security investigation requires the approval of the Country CEO and clearance of the Country General Counsel, who will also provide legal oversight of the investigation. If a security incident involves a suspected breach of the Code, the reporting procedure for a breach of the Code should be followed; in
- All investigations are conducted on the basis of confidentiality, objectivity, independence, and the fair treatment of all the persons involved. They are in all cases carried out in compliance with applicable laws including those relating to data protection.
- Investigations seek to establish the facts relating to the case, to facilitate a finding that the allegations are substantiated or not.
- All investigations and findings shall be subject to legal review.

[1] As per Security and Resilience Management System and People Security Directive

- Remediation of misconduct established through an investigation shall be managed by the applicable business unit, with legal and other functional advice. Group Investigations shall be involved in more serious cases.
- The investigation function shall provide periodic reporting to the applicable governance and management bodies of the group on Code investigation activities and outcomes. The security and resilience function likewise shall provide periodic reporting regarding security incidents.
- The investigation process and system from intake to closure shall be subject to independent audit and review.

CEO checklist

The Country CEO needs to:

- Periodically (and not less than annually), in communications to all employees promote a speak up culture by:
  - Pointing employees to the Code and reminding them what behaviours we value, and what behaviour should be avoided.
  - Promoting the IntegrityLine website and hotline as one of the channels employees can use to report concerns they have concerning possible breaches of the Code. Also reminding employees that they can report to their managers or to legal and compliance
  - Sounding a clear message that whilst we do not tolerate misconduct, and welcome employee reports of their concerns, if they have matters concerning general employee grievances or other complaints not related to violations of the Code, these should be directed through other channels of redress, not through the IntegrityLine.
  - Direct the country legal and compliance function, and /or other assurance functions (internal audit/controls) to supplement the CEO's communications through the year.
- Support investigations of concerns that have been reported to Group Compliance through the IntegrityLine website, hotline or other channels. This may include facilitating access to business data and personnel to assigning a local manager to conduct the investigation at the request of Group Compliance.
- Authorise and direct investigations into security incidents when assessed appropriate and cleared by the Country General Counsel. Ensure the Country General Counsel provides legal oversight of the investigation.
- Direct the Country Security Representative to provide to the Country General Counsel periodic reporting regarding security investigations and outcomes.
- Emphasise and work to ensure the confidentiality of the reporter and the subject of the report is maintained during an investigation. Enforce the principle of non-retaliation.
- Receive and act on updates of investigations in the business.
- Direct the remediation of substantiated misconduct in the business, with advice from legal and other specialist functions. Remediation may include improvements to internal controls (also in unsubstantiated cases), employee disciplinary actions, third party actions, recovery of assets or reporting to authorities.
- Seek periodic advice from Legal and Compliance on trends and other data related to investigations in the business.

Related Policy or Directive(s)	**Code of Business Conduct** **Compliance Policy** Security and Resilience Management System, People Security Directive **Minimum Control Standards Framework (MCS1, MCS7)** This directive replaces the previous **Compliance Reporting** and **Compliance Investigations Directives**.
Sponsor/Owner	Group Legal and Compliance
Date of Version/Effect	April 1, 2021, which updates the version issued on September 12, 2019
Targeted Scope of activities	Promoting a speak up culture and carrying out investigations to support business integrity
Applicability	The Directive is applicable to Holcim Ltd and its consolidated Group companies ("Holcim Group"). In associated companies or joint ventures where Holcim does not exercise equity or management control, the Holcim representative will encourage its adoption or similar rules are applied.