

Group Security Policy

Introduction

The objective of this Policy is to set the framework by which the Group can ensure a level of security and resilience commensurate with its regulatory and legal obligations, while meeting the demands of a competitive commercial organisation. The principles set out in this document are, therefore, designed to enhance commercial opportunity, while minimising corporate risk.

The Policy

The policy has eight subject areas:

- 1) Framework and Governance: outlines requirements for the reporting of security incidents, security management structure, accountabilities, controls and oversight framework.
- 2) Physical Security: outlines requirements for establishing, implementing and maintaining a physical security programme to ensure the safety and security of staff, contractors, buildings and property at all times, using a risk-based approach to manage identified and foreseeable risks.
- 3) Business Travel Security: outlines the requirements to maintain the safety and welfare of staff who undertake business travel on behalf of the Group, including approval processes, risk assessing and tracking of travel.
- 4) Health and Safety: provides the minimum requirements for LBUs to provide a safe and healthy working environment and the prevention of injury and ill-health to employees, contractors, visitors and those affected by Prudential operations. This include the establishment of a Healthy and Safety management system defining governance, roles and responsibilities; the requirement to risk assess, identify hazards and mitigate identified risks to tolerable levels.
- 5) Business Continuity Management: provides the framework to establish, implement and maintain a comprehensive BCM programme using nine key integrated component controls, thereby ensuring our business can withstand, absorb and recover from operational and business disruptions.
- 6) Counter Fraud: requires LBUs to develop and maintain a fraud risk management framework to prevent, detect and respond to fraud events. This framework includes requirements for fraud risk assessments, investigation and quality assurance.
- 7) Speak Out: mandates the Confidential Reporting system implemented to receive Concerns raised by staff, contractors, vendors, agents and customers. LBUs are required to promote the existence of the Speak Out programme, record all reported concerns, strictly control access to related Speak Out information and maintain the confidentiality and the protection of parties lawfully raising concerns in good faith. The policy further mandates investigation and oversight requirements and staff training and awareness.
- 8) Investigations: requires LBUs to implement policies and procedures to ensure investigations are conducted by appropriately trained and experienced investigators, proportionate to the complexity, scale and seriousness of the investigation; the requirement to plan and record key actions, activities and decisions during investigations; and the recording, reporting and tracking of investigation outcomes.