CORPORATE SECURITY

UPDATED JULY 2019
GLOBAL POLICY
WHO DOES THIS APPLY TO?

• All Diageo employees.

• Joint ventures in which Diageo has a controlling interest.

• Third party contractors, agents or consultants representing or acting for or on behalf of Diageo.

• All employees are individually responsible for ensuring they comply with this policy in addition to Diageo’s Code of Business Conduct and all laws, regulations and industry standards.

• Line Managers are expected to ensure that direct reports receive the guidance, resources and training to enable them to do their jobs in compliance with this policy

OUR COMMITMENT

We are committed to protecting our people, sites, assets, brands and reputation by ensuring we have an effective and risk based approach to security. We will act to mitigate security risks by establishing and meeting minimum security standards across our business and applying more robust measures where necessary. Security will always be implemented in accordance with Diageo Values.

CONTEXT

The Corporate Security global policy supports the Diageo Performance Ambition helping the business turn risks to opportunities, increasing our resilience while at the same time ensure our reputation is protected, losses are minimised and productivity is maximised.

Security will be organised around the Diageo operating model. At a market level, overall accountability for corporate security sits with the Managing Director. Each market and each site within a market is required to nominate an individual to be responsible for Corporate Security. They will be accountable to the senior Site Manager or market Managing Director for ensuring that security risk assessments are conducted regularly and action plans to address identified risks are implemented. As outlined in the Corporate Security Blueprint in high or medium security risk market with production sites or large demand markets a fulltime Head of Security is required. In lower risk markets without production sites a Security Co-ordinator can be appointed. This is a part-time responsibility for an individual already in another role. An above market, Global Corporate Security team provides support and expertise. This includes training/capability building, technical support, governance and assurance.

All Diageo employees should play an active part in maintaining a secure workplace environment.
1. PEOPLE SECURITY

Corporate Security will get the right people in the right place to sell. Diageo will provide all staff with appropriate training and guidance for the security risks they face wherever they are based, or wherever they travel, either within their home market or overseas as part of Diageo business.

All employees are responsible for ensuring that they are aware of the security risks faced and know how to respond to security incidents including how to seek assistance in their workplace and when out and about on Diageo business. Line managers should ensure they have properly assessed the risks employees face and that appropriate training, guidance and support have been made available. The Global Corporate Security team, in-market Security Managers (where present) and nominated security co-ordinators will pro-actively identify and mitigate people security risks (incl. terrorism, civil unrest, crime, conflict) and maintain crisis plans that protect our people. If you need assistance, you should contact the global Corporate Security team.

Business Travel

As Diageo employees, we sometimes need to travel for critical business meetings. While commercial issues are important, they never take precedence over personal security.

Corporate Security is committed to ensuring that Diageo travellers receive the most comprehensive advice and training prior to travel and best possible assistance when overseas. When travelling to certain destinations training is mandatory. Global Corporate Security provides direction on extra precautions employees should take to protect highly confidential information when travelling in certain high risk countries. This may include, for example, the provision of clean devices and restricting access online.

All employees must read and comply with the Travel Security Guidelines when undertaking business travel.

In addition, as part of our business continuity global standard, businesses must ensure that no more than half of any management team ever travel on the same “vehicle” (plane, minibus, train etc.), unless approved by the Managing Director or Functional Executive. This includes Market/country management teams as well as the Global Exec.

Fire Arms

Applicable to employees, clients, contractors, vendors and visitors, to the extent permitted by law, Diageo specifically prohibits the wearing, transporting, storage or presence of firearms or other dangerous weapons while in company facilities or on company property unless expressly permitted by Diageo’s Director of Corporate Security and senior legal counsel in market. This ban includes:

- Storing or transporting a weapon in a Diageo vehicle in any vehicle in a Diageo parking area except in the countries (specific states or provinces) that specifically allow weapons storage in vehicles.
- Possessing a weapon while performing company business off the company’s property, unless expressly permitted by law and Diageo.

Any employee in the possession of a firearm or other weapon while in company facilities, on company property or while engaging in company business may face corrective action up to and including termination of employment, unless such action is prohibited by law and a Diageo exempt applies. In addition, to the extent allowed by law, the company prohibits clients, contractors, vendors or visitors from carrying weapons while in company facilities or while on company property. Exemptions to this policy apply to:

- Any law enforcement personnel engaged in official duties.
- Any person engaged in military activities sponsored by the federal or state government, while engaged in official duties.

Exemptions to this policy may apply to:

- Any security personnel engaged in official Diageo sanctioned activity.
- Personal Protection weapons issued by an official legally recognised authority to a specific individual to mitigate against a specific threat.

Evidence of sufficient training in the safe handling and discharge of the firearm would be required as part of the case put forward for consideration of exemption. Exemptions must be approved in writing via Diageo’s Director of Corporate Security and senior legal counsel in market.

Some of our facilities have areas that have an explosive risk and therefore, where Diageo has the ability to enforce a restriction, weapons should not be taken into these areas.
CORE PRINCIPLES OF THE POLICY (CONT)

2. PHYSICAL SECURITY

Physical security standards and procedures are accessible through the Corporate Security Mosaic site. These standards and procedures must be applied in all cases, incl. where site or market security is outsourced to third party contractors. In addition, all relevant local laws must be complied with.

Site Security

You must take all reasonable and practical steps to ensure that your premises and third party premises that are used to warehouse our product or house our people and other business activities are secure. All Diageo sites will meet at least the minimum standards for physical security as laid down in the Diageo Physical Security Standards. These cover alarms, perimeter security, and access control, CCTV, guarding, lighting and parking. Where appropriate, sites should conform to CTPAT, AEO or other regulatory frameworks. Each site is required to nominate an individual to be responsible for security. They will be accountable to the senior Site Manager or market Managing Director for ensuring that security risk assessments are conducted regularly and action plans to address identified risks are implemented.

Supply Chain Security

It is important that our goods are properly protected through the supply chain so that we avoid losses and damage which add cost and can undermine our ability to conduct sales and impact our reputation. Minimum standards are laid out in Diageo Global Risk Management Standards, Corporate Security’s Security Supply Chain Standards and procurement third party logistics contract templates and apply to both Diageo and third party logistics companies (3PL) operating on our behalf. 3PL companies must also ensure that these standards are met by any sub-contractor used by them.

All business with 3PL must be subject to a contract that clearly outlines the responsibilities and liabilities of all parties, including the performance of a risk assessment, the nomination of nominated persons responsible for supply chain security and insurance cover. The contract must provide provision for the following areas: specific procedures to identify and investigate all instances of interference or loss of goods under their control, specific protocols for the handling of high value items, the requirement to inform Diageo of all instances of loss/tampering, the requirement to initiate an investigation within 24 hours of theft being suspected. The cyber risk to the supply chain should be covered within the risk assessment.

3. BUSINESS CONTINUITY AND CRISIS MANAGEMENT

Business Continuity planning is critical to all parts of the business and all markets must adhere to the Business Continuity Management Global Standard (BCM) and its BCM Framework: Governance, Risk Assessment, Crisis Management, Business Continuity, Testing, Training and Awareness, Program Maintenance and Controls and Reporting. Specific guidance on each of the framework components is contained in the BCM Global Standard and complemented by the Global Risk Management Standards (GRMS). Functions, entities and businesses may apply more comprehensive policies, but the minimum requirements in this standard must be met.

Crisis Management Planning (CMP) is the stage of BCM that prepares the business to manage any type of crisis. This plan is general and is about communication and coordination. Diageo uses the FACTS process to manage crisis and all crisis should be managed using this process. If a crisis evolves and produces a business interruption, crisis management then transitions to business continuity activating the Business Continuity Plan (BCP). The minimum requirements for Crisis Management are contained with the Business Continuity Management Global Standard.
CORE PRINCIPLES OF THE POLICY (CONT)

4. INVESTIGATIONS

From time to time allegations are made, or evidence surfaces, of inappropriate behaviour by Diageo employees, contractors, suppliers or business partners. The prompt, consistent and thorough investigation of these issues is critical for achieving the Performance Ambition of most trusted. All cases should be dealt within a consistent framework across all Diageo entities.

Diageo has established the Breach Management Global Standard for investigations that ensures:

- Investigations have the right level of independence, authority and oversight.
- Diageo acts within the laws and regulations of the relevant countries.
- Proper procedures are followed in a reasonable timescale.
- The process is consistent with the Diageo values.
- Accountability for follow-on actions arising from investigations is clear.

Anyone involved in an investigation will be treated with dignity and respect, and they should be able to access support, should they require it, from local HR or their line manager.

All investigations must be conducted by a competent, suitably trained, independent investigator and overseen by an independent senior leader. Investigations should be carried out internally wherever possible, in a timely manner, and within all relevant legal frameworks.

If necessary and proportionate, and if local law permits, Diageo may seek to deploy covert methods to support an investigation. In doing so investigators will follow the procedure, and obtain the appropriate authorisation, as set out in the Diageo Investigation Guidelines. Any covert investigation will be strictly targeted at obtaining evidence within a set timeframe. Any techniques used must be compliant with local privacy laws.

If you are involved in an investigation, you must make sure that you understand and apply the Breach Management Global Standard and Diageo Investigations Guidelines. Any employee who carries out investigations on behalf of Diageo must have undertaken the Diageo Investigations training on Academy. As stated in the Code of Business Conduct, Diageo will not tolerate any reprisal for reporting a problem in good faith or assisting in an investigation.
WHERE TO GET MORE INFORMATION

For further information and support related to this policy, please contact the Global Corporate Security team at:

corporate.security@diageo.com

HOW TO REPORT A BREACH

Any breach of this Policy is also considered to be a breach of the Diageo Code of Business Conduct and should be reported promptly. Cyber investigations will be initially triaged by CSI please contact them on CSI@diageo.com

DATA PRIVACY CONSIDERATIONS

When undertaking activities under the Corporate Security global policy you may be accessing or otherwise processing personal information which is Confidential or Highly Confidential, including CCTV and access control monitoring, undertaking investigations and recording details for BCM planning. It is vital you adhere to Diageo’s Global Data Privacy Policy, our internal information handling policies and locally applicable laws seeking advice from your Diageo internal supporting lawyer as appropriate.

MONITORING & POLICY GOVERNANCE

Compliance with the Corporate Security global policy will be monitored both at the market and above market level, through security audits conducted by Corporate Security, supported by the Risk Management Community, and through existing site and business audit programmes, including the CARM process and Risk and Audit Committees. Nominated individuals responsible for security in market and at sites are required to enter all security incidents on to the Diageo security incident database.

Breaches of this policy risk the security and safety of our people, product and sites as well as Diageo’s reputation.

There may also be substantial losses incurred through failure to meet our requirements to protect our people exposing us to manslaughter legislation and failure to protect our sites and products through losing our C-TPAT license.
KEY THINGS TO REMEMBER

1. The Corporate Security global policy ensures we protect our people, sites, assets, brands and reputation by ensuring we have an effective and risk based approach to security. The policy covers the four key pillars of security: People Security, Physical Security, BCM and Crisis Management, and, Investigations. There are supporting standards and guidelines that support each of these four pillars. At a market level, overall accountability for Corporate Security sits with the Managing Directors. Each market and site is required to nominate an individual to be responsible for Corporate Security. All Diageo employees should play an active part in maintaining a secure workplace environment.
I am due to go on a business trip soon and I’ve been told to check travel security before I go. Why? Surely my manager wouldn’t be sending me somewhere unsafe!

No, your manager wouldn’t knowingly have done so – but there are some countries or locations where it is advisable to take extra security precautions and sometimes the security situation can change quickly. We are committed to ensuring that all Diageo travellers are as safe as possible, and we regularly update the list of country security travel ratings. For some countries there is a requirement to undertake Travel and Personal Security (TAPS) training available via Academy before travel. You should make sure you know how to contact Corporate Security or the local country security managers in the country to which you are travelling, and you should also know what to do in case of an emergency. Refer to the Travel Security Guidelines or the Corporate Security Mosaic Site for further information. You should also ensure you are a member of the Travel Security Yammer group to be kept up to date with the latest travel advice and restrictions.