DIAGEO

CORPORATE SECURITY

Global Policy

CODE OF BUSINESS CONDUCT

All Diageo employees should feel secure in their place of work and all Diageo sites should meet our standards

Our commitment

We are committed to protecting our people, assets, brands and reputation by ensuring we have an effective and robust approach to the management of security risks. 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 our Diageo Values.

Scope of this policy

The Corporate Security global policy applies to all employees of Diageo entities at global and market levels and to Diageo managed joint ventures. We require our business partners, suppliers and contractors to adopt a similar approach.

This policy covers all aspects of Diageo's activities and must be considered at all stages of the business process, from the initial feasibility study through development to operational use and finally to de-commissioning, as well as for particular projects such as brand sponsorship and other public events at which our employees, customers, suppliers, or other Diageo guests are in attendance.

Context

All Diageo employees should play an active part in maintaining a safe and secure workplace environment.

Security will be organised around the Diageo operating model maximising local knowledge and expertise and forming a Diageo network to share best practice. 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. They will be accountable to the senior Site Manager or market General Manager for ensuring that security risk assessments are conducted regularly and action plans to address identified risks are implemented. A small, above market, Corporate Security team provides support and expertise, including training / capability building, technical support, and monitoring of best practice.

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

You must act to mitigate risks which arise from deliberate or accidental breaches in your site security or threats to your people.

Q&A

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 lists of country security travel ratings. 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.

Principles

Personal security

Diageo will provide all staff with appropriate training and guidance for the security risks they face wherever they are based, or wherever they travel.

We are all responsible for making sure that we are aware of the security risks we face and that we know how to respond to security incidents and how to seek assistance should an incident occur. If you are a manager, you should ensure that you have properly assessed the risks your staff face and that appropriate training, guidance and support have been made available.
If you need assistance, you should contact the global Corporate Security team or the appropriate Country Security Manager: these are a centre of excellence to support you in identifying risks, providing security updates and providing appropriate security measures.

Business travel

As Diageo employees, we sometimes need to travel for critical business meetings where a telephone or video conference would not be effective. While commercial issues are important, they never take precedence over personal safety and security.

Corporate Security is committed to ensuring that Diageo travellers receive the most comprehensive advice prior to travel and best possible assistance when overseas, including directions on extra precautions you should take to protect highly confidential information when traveling in certain high risk countries This may include, for example, the provision of clean devices and restricting access online.

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

In addition, as part of our business continuity standards, 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 General Manager or Functional Executive. Market/country management teams should follow the Exec travel policy.

Site and asset security

You must take all reasonable and practical steps to ensure that your premises are secure and you must follow site security procedures.
All Diageo sites will meet at least the minimum standards for physical security as laid down in the Diageo 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 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.

Business Continuity 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 in particular the key non-negotiables set out in that standard:

- Each market and site must be covered by a Crisis Management and Business Continuity plan.
- A BCM risk assessment must be performed annually.
- Crisis Management and Business Continuity Plans should be tested annually.
- The control design of key CARM control [C0017] should stipulate when the annual review takes place, who leads the review and who, overall, signs off on the updated BCM plans. The updated documents [risk assessments, plans, and evidence of trainings) must be shared with Global BCM Manager.
- Each market and site must have a Crisis Management Team (CMT) trained in the FACTS process.
- The FACTS process should be used to manage all crisis events.
- Any activation of a country or market CMT should be notified immediately to the Regional President and Corporate Security (corporate.security@diageo.com) who will help coordinate central functions support.

Specific guidance on each of these statements is contained in the BCM Global Standard and complemented by the BCM Global Risk Management Standards. Functions, entities and businesses may apply more comprehensive policies, but the minimum requirements in this standard must be met.

Investigations

From time to time allegations are made, or evidence surfaces, of inappropriate behaviour by Diageo employees, contractors, suppliers or business partners. The prompt and thorough investigation of these issues is critical for maintaining the company's reputation and standing and for ensuring that cases are dealt with appropriately and 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.

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

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

Occasionally, in the most serious allegations and if local law permits, Diageo may seek to deploy covert methods to support an investigation. In doing so, Diageo investigators will follow the procedure, and obtain the appropriate authorisation, as set out in the Diageo Investigation Guidelines. Contact Corporate Security for further information.

Any covert investigation will be strictly targeted at obtaining evidence within a set timeframe and if such techniques are used, it 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, as far as it is appropriate for the particular investigation. Any employee who carries out investigations on behalf of Diageo must have undertaken the Diageo Investigations Guidelines training. This training is available via 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.

How does this apply to me?

- We are all responsible for helping to protect against security risks.
- We should make sure that we are aware of and that we follow our local security guidelines, including restriction on what we can do in high risk countries
- We must make sure we know what to do if an emergency occurs at our place of work.
- We should make sure we understand about all potential security risks before we undertake any business activity, including travelling on business or organising an event, and that we know how to obtain advice and assistance a.
- We must read and comply with any travel security advice before travelling.
- We must ensure that if we are involved in an investigation, it is conducted fairly, in line with all relevant legal frameworks and with the appropriate

Responsibility

We are all individually responsible for making sure that we comply with this policy in addition to Diageo's Code of Business Conduct and all laws, regulations and industry standards.
If you manage people, you are expected to ensure that the individuals who report to you receive the guidance, resources and training they need to enable them to do their jobs in compliance with this policy.

Monitoring

Compliance with the Corporate Security global policy will be monitored through security audits conducted by Corporate Security, supported by the Risk Management Community, through existing site and business audit programmes.

Any breach of this policy is also considered to be a breach of the Diageo Code of Business Conduct and should be reported promptly through one of the routes described in the Code. You can also discuss concerns or make a confidential report using SpeakUp.

Breaches of this policy will be dealt with in accordance with the Breach Management Global Standard, Diageo Investigations Guidelines and local disciplinary policies, as permitted by law.

Contacts and further information

For further information and support related to this policy, please contact the Global Corporate Security team on corporate.security@diageo.com. The Global Risk & Compliance team are available to provide help and guidance on all issues relating to the Code and Diageo policies. Global Risk & Compliance can be contacted on: global.compliance.programme@diageo.com.

Extraordinary security information, such as in the event of a natural disaster or outbreak of war, will be posted on Mosaic.

This policy was last reviewed and updated in July 2016.