# SECURITY POLICY

# INTRODUCTION AND PURPOSE

Security is the degree of resistance to or protection from harm. It applies to any vulnerable and valuable asset, such as a person, site, community, IT network, nation or organization. As a responsible company, Carlsberg India Private Limited (“CIPL”/”Company”) together with any subsidiary of CIPL from time to time (“CIPL Group”) is committed to protecting vulnerable and valuable assets from harm. This requires the establishment and maintenance of security programmes, without which the CIPL Group could be exposed to serious risks, damages and losses. This policy defines the framework for managing security within the CIPL Group.

# SCOPE

This policy applies to the management, employees and contract workers of all entities in the CIPL Group. The policy is supplemented by manuals as well as any guidelines and instructions issued by each CIPL Group entity.

# REQUIREMENTS

## 1. GENERAL

1.1. You must adhere to the CIPL Group's Security Policy and manuals. Additionally, you must familiarize yourself and comply with local regulations, rules and procedures.

1.2. You must be vigilant about security and challenge people appropriately if you believe they are contravening company security requirements or posing a threat to the security of the CIPL Group.

1.3. You must familiarize yourself with security risks to reduce the likelihood and impact of any such risks to yourself and your colleagues.

1.4. You must report security incidents or concerns to your manager, the CIPL CFO or Group Security, and assist with any investigations into such incidents.

1.5. You must support those specifically engaged in security duties.

## 2. PERSONAL SECURITY

2.1. The CIPL Group will provide employees with appropriate information and guidance on the security risks they face wherever they are based or wherever they travel.

2.2. 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 you have provided appropriate training, guidance and support.

2.3. If you need assistance, you should contact the CIPL CFO or Group Security, who can help you identify risks, provide security updates and advise on appropriate security measures.

## 3. PHYSICAL AND SITE SECURITY

3.1. We must all play our part by taking reasonable and practical steps to ensure that our premises are secure, and we must all observe site security requirements. All CIPL Group sites must meet the requirements set out in the Physical and Site Security Manual. These cover site surveillance, site access control, perimeter security and monitoring.

## 4. EVENT SECURITY

4.1. In order to protect our employees, assets and reputation from harm during internal and external events, security measures must be implemented in accordance with the outcome of a security risk assessment of the event location. Detailed requirements on event security can be found in the Event Security Manual.

## 5. BUSINESS TRAVEL

5.1. As a responsible employer, the CIPL Group will ensure that business travellers receive advice and training prior to travel, and the best possible assistance while they are travelling.

5.2. All CIPL Group business travellers must observe the requirements set out in the Travel Security Manual.

## 6. IT ACCEPTABLE USE & INFORMATION SECURITY

6.1. You must use CIPL Group systems and IT equipment with due care and primarily for business purposes.

6.2. You must not use CIPL Group systems and IT equipment in a way that is a source of discomfort to CIPL Group employees or other third parties.

6.3. You must not use CIPL Group systems and IT equipment in a way that is in conflict with local or international law, or damages the reputation of the CIPL Group.

6.4. You must not use CIPL Group systems and IT equipment in a way that adversely affects the availability of CIPL Group systems or the confidentiality or integrity of CIPL Group data.

6.5. Further detailed requirements can be found in both the IT Acceptable Use Policy and the Information Security Policy.

# ROLES AND RESPONSIBILITIES

| Body/function/individuals | Roles and responsibilities |
|---|---|
| CIPL Board of Directors (BoDs) | Responsible for policy approval. |
| CIPL CFO (in consultation with Group Security) | Policy owner with overall responsibility to BoDs for security issues in the CIPL Group and for ensuring that material security risks in the Group are duly attended to and communicated to CIPL BoDs/ Audit Committee as relevant. |
| CIPL IT | Responsible to CIPL BoDs for information and IT security issues in the CIPL Group and for ensuring that material information and IT security risks in the Group are duly attended to and communicated to CIPL BoDs/the Audit Committee/. |
| CIPL CFO | Responsible for ensuring that this policy and associated manuals are implemented and adhered to, and that all relevant employees are made aware of the policy and its requirements. |
| Management, employees and contract workers of all entities in the CIPL Group | Responsible for adhering to this policy and associated manuals. |
| Managing Director, CIPL Functional Heads at Corporate Office, Local Management | To the extent this policy requires notification and/or escalation to a representative of the Carlsberg Group, outside of the CIPL Group, a representative nominated by CSAPL (Singapore) Holdings Pte. Ltd. shall be copied in such notification and/or escalation. |

For a detailed overview of roles and responsibilities, see Appendix A.

## DEVIATIONS

No exemptions from this policy can be granted unless there are exceptional circumstances or the policy is obviously not applicable. All requests for exemptions must be made in writing to the policy owner. The policy owner must assess and decide on each request individually. Exemptions must be duly logged and documented.

## POLICY REVISION

This policy will be revised every two years or whenever a major breach or incident makes it relevant to review and revise it. It may be amended at any time with the approval of CIPL BoDs. In the event of any discrepancies between the English version of this policy and a translated version, the English version will be binding.

## ASSOCIATED POLICIES AND MANUALS

- Employee Security Manual
- Physical & Site Security Manual
- Event Security Manual
- Travel Security Manual
- ELUD, Assignees & Transferes Manual
- Security Risk Assessment Manual
- Information Security & Acceptable Use Policy

## CONTACT

CIPL CFO and Group Security & Crisis management.

## GOVERNING LAWS

This Policy shall be subject to applicable Indian Law(s).

## Appendix A

| Body/function/individuals | Roles and responsibilities |
|---|---|
| CIPL CFO | • At least once a year provides strategic direction for security management and the risk appetite of the CIPL Group.<br>• Ensures that a system and organisation is in place to effectively manage security across the CIPL Group.<br>• Actively supports and promotes a positive security culture within the scope of this policy. |
| CIPL CFO (in consultation with Group Security) | • Establishes a security strategy and roadmap for security in the CIPL Group.<br>• Establishes, maintains and operates a risk-based security programme in order to effectively and efficiently implement the security strategy in all CIPL Group entities.<br>• Ensures that geopolitical and security risk assessments are conducted, updated and communicated across the business.<br>• Helps ensure that physical and site security programmes are implemented.<br>• Ensures that a travel security programme, including training, notification and response, is in place globally for CIPL Group business travellers.<br>• Ensures that a security response system is in place to minimise the impact of security incidents.<br>• Supports criminal investigations for the CIPL Group globally.<br>• Helps ensure that security services providers are managed efficiently in order to minimise costs and improve efficiency and quality.<br>• Provides support with screening of new partners/big suppliers/key personnel.<br>• Provides security advice and analysis on strategic security issues to CIPL management.<br>• Annually reports to CIPL BoDs on the status and effectiveness of the CIPL Group's security programme as well as any risks or incidents that have impacted on the Group.<br>• Provides an annual overview of the CIPL Group security budget and manages related costs. |
| CIPL IT | • Establishes an information security strategy and roadmap for information security in the CIPL Group.<br>• Establishes, maintains and operates a risk-based information security programme in order to effectively and efficiently implement the information security strategy in all Group entities.<br>• Delivers reporting on the status of the information security strategy, the progress of information security programme activities, and the identification of new or unrealised initiatives for achieving the strategy.<br>• Provides information security services to the CIPL Group that enable employees and business functions to work securely and take informed, risk-based decisions.<br>• Ensures that information security requirements and controls are embedded in all Group IT activities; security by design, security by default.<br>• Supports the “nine-layer” model for IT and security in the supply chain.<br>• Ensures adequate risk assessment and security compliance in sourcing and vendor management activities in relation to IT services.<br>• Manages cyber security incidents and disaster recovery processes relating to IT services provided to CIPL Group.<br>• Provides ongoing awareness and training for employees and third parties on relevant information security issues.<br>• Manages investments and operating budgets for the information security programme, including security technologies, processes and resources. |
| CIPL Head of Corporate Affairs (with support of Finance Controller) | • Actively assumes full ownership of the security of his/her operations and ensures implementation of and compliance with the Group Security Policy and associated manuals.<br>• Ensures that, from a security perspective, the business complies with relevant local and international law.<br>• Serves as the point of contact with Group Security on security issues in the given Group entity.<br>• Keeps abreast of and reports to Group Security/local management on any factors of Group interest.<br>• Develops, maintains and coordinates a local security programme for the relevant Group entity and maintains local networks for use in connection with security issues.<br>• Provides an annual overview of the local security budget (including fixed yearly charges and projects) and manages related costs<br>• At least once a year reports to local management and Group Security on the implementation and effectiveness of the local security programme as well as risks or incidents that have impacted on the given Group entity.<br>• Ensures that local security services are managed efficiently in order to minimise costs and improve efficiency and quality accordingly.<br>• Ensure that security awareness activities and campaigns are conducted<br>• Ensures security assessments are conducted and follow-up on implementation of agreed recommendations |
| Management, employees and contract workers of all entities in the CIPL Group | •Adhere to the requirements set out in this policy and associated manuals. |

ENGLISH

LIVE BY OUR COMPASS

June 2018

Carlsberg India Private Limited
Regd. Office : 04th Floor, Rectangle No.1, Commercial Complex D4, Saket, New Delhi-110017, India
Corporate Office : 3rd Floor, Tower-A, Paras Twin Towers, Sector-54, Gurugram, Haryana-122002, India