Information Security Policy

Policy Objectives

This policy is intended to establish the necessary policies, procedures and an organisational structure that will protect Cleanbrite's information assets and critical activities from all appropriate threats and to ensure regulatory, statutory, contractual, and legislative requirements are met.

Compliance with this policy is necessary to ensure business continuity, and to minimise business damage by preventing and minimising the impact of security incidents.

Scope

This policy applies to:-

1. All departments and the information processed by those departments;
2. All company operations run out of all offices;
3. All information processed by Cleanbrite in pursuit of its operational activities, regardless of whether it is processed electronically or in paper form; and
4. All information transferred or exchanged with third parties, or held by third parties on behalf of Cleanbrite, regardless of whether it is process electronically or in paper form.

Communication

This policy will be made available to all those working for or on behalf of Cleanbrite and made available on the company website to our suppliers, customers, and stakeholders.

Policy Statement

It is company policy to ensure that:-

1. Information assets and information processing facilities shall be protected against unauthorised access;
2. Information shall be protected from unauthorised disclosure;
3. Confidentiality of information assets shall be a high priority;
4. Integrity of information will be maintained;
5. Cleanbrite's requirements, as identified by information asset owners, for the availability of assets and information processing facilities required for operational activities shall be met;
6. The management of the supply chain requires those negotiating contracts to ensure appropriate information security and business continuity measures are included in contracts, where possible, so that the service provider is able to deliver acceptable levels of service;
7. Any supplier engaged by the company to handle payment card data will comply with the Payment Card Industry Data Security Standard (PCI);
8. Business continuity plans shall be produced, maintained and tested; and
9. Unauthorised use of information assets and information processing facilities shall be prohibited; the use of obscene or otherwise offensive statements shall be dealt with in accordance with other policies published by the company.

All breaches of information security, actual or suspected, shall be reported and investigated in line with company policies.

Controls shall be commensurate to with the risks faced by the company. In support of this information security policy, more detailed security policies and possesses shall be developed for those working for or on behalf of the company, information assets and information processing facilities.

Information Security Objectives

The Objectives of the Information Security Management System are:-

1. To provide the necessary policies, procedures and an organisational structure that will protect company information assets and critical activities from all appropriate threats and to ensure regulatory, statutory, contractual and legislative requirements are met;
2. To ensure business continuity, and to minimise business damage by preventing and minimising the impact of security incidents; and
3. To preserve the appropriate level of confidentiality, integrity and availability of company information assets and critical activities.

Definitions

Please refer to Appendix 1.

Responsibilities

Directors

The Directors shall be accountable for ensuring that appropriate and effective information security controls are implemented, monitored, and reviewed to ensure compliance with Cleanbrite's legal, regulatory or contractual obligations.

The Directors will be responsible for:-

- Ensuring that the information security objectives are aligned with the organisations objectives;
- Shall be accountable for ensuring that appropriate security, legal and regulatory controls are identified, implemented, and maintained by information owners; and
- Shall ensure that continuous compliance monitoring within their area of jurisdiction.

The Directors shall be supported by all Colleagues.

Information Asset Owners (IAO)

The IAO shall be responsible for the identification, implementation, and maintenance of controls for the information assets they own and the risks to which they are exposed.

A list of information assets and their owners is set out in the Information Asset Register.

Information Governance and Security Board (IGSB)

The IGSB is responsible for setting the priorities for the information security work programme. A programme of reviews and assessments of security effectiveness will form part of this programme and will establish an agenda for security improvements.

Compliance will be periodically reviewed by the IGSB.

Head of Information Compliance and Data Protection Officer (ICDPO)

The ICDPO is responsible for facilitating information at an operational level including convening with the IGSB.

Managers

The Managers within every business area are responsible for implementing security policies and procedures including with third parties that they manage.

As part of the formal assessment of security effectiveness, Managers will be required to account for security problems, breaches and the security performance of their areas of control.

All Colleagues

All Colleagues, including permanent and temporary, are responsible for the protection of the company information assets, ensuring the confidentiality, integrity and availability of these assets are maintained and must adhere to all policies relating to information Security.

Third Party Suppliers

All third-party suppliers must conform to this policy.

Non-Compliance

Non-compliance will be subject to investigation and may result in:-

- Disciplinary action in accordance with company procedures that may result in termination of employment.
- Legal prosecution.
- Loss of access privileges to information assets or information processing facilities.
- Other actions deemed appropriate by the Directors and our legal advisors.

Governance

Information Security will be governed and the effectiveness measured by the following methods:-

1. Internal audit
2. External audit e.g. Regulators such as Information Commissioners Office and The Professional Standards Authority
3. Business continuity and disaster recovery through testing and actual scenario bases
4. Management Review e.g. risk assessments, lessons learnt from security incidents and identified improvements
5. The results of these processes will enable the business to review the effectiveness of the controls and continually develop the Management System

The IGSB will review and approve the prioritisation of information security aspects of the internal audit schedule at least on an annual basis, ensuring that every business process is audited at least once in a 3-year period.

The Information Security Policy will be reviewed every 12 months or when there are significant changes to ensure it is being implemented correctly and consistently whilst quality is maintained.

Security Awareness and Training

Colleagues with access to information assets and information processing facilities shall be educated on their information security responsibilities. Education shall be provided as part of the induction process

so that new Colleague completely understands their responsibilities in the protection of information assets and information processing facilities.

Colleagues shall be provided with on-going security education and supporting reference materials. Refresher courses will be scheduled within each Colleagues training matrix to regularly remind everyone of their obligations.

The security responsibilities of third parties shall be made clear prior to the award of contract.

Risk Management

A systematic approach to information security risk management has been adopted to identify business needs regarding information security, including legal, contractual, and regulatory, and to create an effective operational information security framework.

Information security risk management is not a one-off exercise with a single set of control recommendations which remain static in time but a continual process.

The implementation of the information risk strategy shall be based on formal methods for risk assessment, risk management and risk acceptance and independent of technology or software.

Continual Improvement

The Board of Directors and Senior Management shall ensure continual improvement of the information security management system.

Legislation and Standards

The list below contains some the legislative and regulatory requirements the Company must comply with:-

- Data Protection Act 2018
- UK General Data Protection Regulation
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Computer Misuse Act 1990
- Companies Act 2006
- Health & Safety at Work Act 1974
- Equality Act 2010
- Bribery Act 2010
- Fraud Act 2006
- Regulation of Investigatory Powers Act 2000

Name: **Senior Management Team**
Position: **Company Directors**
Review Date: **1st August 2021**

Appendix 1
Definitions

Definitions

Asset	Anything of value to the organisation. There are many types of assets including information, software, hardware, and intangible assets such as reputation.
Availability	The property of being accessible and usable upon demand by an authorised entity.
Business Continuity Management	A process that identifies potential threats to an organisation and the impacts to operations that those threats, if realised, might cause. It provides a framework for building the capability for an effective response that safeguards the interests of its key stakeholders and the organisation's reputation.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Information Security	Information security is the protection of information from a wide range of threats to minimise business risk, preserve confidentiality, integrity and availability of information.
Information Security Management System	Part of the overall management system based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve the organisation's information security.
Integrity	The property of protecting the accuracy and completeness of assets.
Physical Security	This covers the assets and way those assets are used to restrict physical access and the presence of people in certain locations to stop theft of, or damage to, assets and property. This may include guards, locked doors, identity checks and movement controls.