ISMS DOC 5.1 – Information Security Policy

The Board of Directors and management of GoPro Ltd., located at Tunguhals 19, which operates business activities relating to the provision of operation, maintenance and management of Software Services (Cloud / SaaS) and related Professional services and systems on a secure and hosted platform, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with GoPro Ltd.'s goals and the ISMS is intended to be an enabling mechanism for information sharing, for operations, hosting and for reducing information-related risks to acceptable levels.

GoPro Ltd.'s current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. Every year the Risk Treatment plan is made on the availability and confidentiality of the Assets (High). Head of Risk is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Information Security Manual and are supported by specific documented policies and procedures.

All employees of GoPro Ltd. and external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy. All employees, and certain external parties, will receive appropriate training. The consequences of breaching the information security policy are set out in the Organization's disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement.

GoPro Ltd. has established an Information Security Committee, chaired by Chief Financial Officer (CFO) and including the Head of IT (CIO), and Chief Information Security Officer CISO (Secretary of the Committee) and other executives to support the ISMS framework and to periodically review the security policy.

GoPro Ltd. is committed to achieving certification of its ISMS to ISO27001:2013.
This policy will be reviewed as required, for example to respond major changes in the risk assessment or risk treatment plan.

The Information Security Objectives are:

Preserve

This means that management, all full time or part time Employees/Staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy and procedures identified in Section 16 of the Manual) and to act in accordance with the requirements of the ISMS. All employees will receive information security awareness training and more specialised employees will receive appropriately specialised information security training.

Available

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and GoPro Ltd. must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans. Average uptime for GoPro system will be **98%** annually, excluding planned system downtime.

Confidential

This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to GoPro Ltd.'s information and proprietary knowledge and its systems including its network(s), website(s), extranet(s), and e-commerce systems. For any internal audit performed, a maximum of **5 minor incidents** should be detected, the objective should be reviewed annually.

Integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency including for network(s), e-commerce system(s), website(s), extranet(s) and data backup plans and security incident reporting. GoPro Ltd. must comply with all relevant data-related legislation in those jurisdictions within which it operates. For backups, no more than **5 faults** should occur each year because of lack of disc space. Data recovery from backups will also be tested **at least four times** each year. A test (of any type) shall be performed on a specific aspect of BCP/DRP at least **once a year**. Viruses and malware within GoPro system shall be kept to a minimum, with **no more than one** virus/malware detection over the year. Any incident that is detected within GoPro systems should be reported **within 24 hours** of being detected.

Physical Assets

The physical assets of GoPro Ltd. including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

Information Assets

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

GoPro Ltd. and partners that are part of our integrated network and have signed up to our security policy and have accepted our ISMS.

The ISMS is the Information Security Management System, of which this policy, the Information Security Manual ('the Manual') and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO27001:2013.

A **SECURITY BREACH** is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of GoPro Ltd.