creative communications group

penguins GROSVENORCOMMS hlmlx FIREHOUSE a-vision

Information Security Policy Statement

ISMS DOC 5.1

The Board of Directors and Management of **DRPG**, located at 212 Ikon Estate, Droitwich Road, Hartlebury, Worcestershire, DY10 4EU, which specialises in the field of communications, including video production, event management and technical services, digital media, print, design, creative and strategic solutions are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the 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 **DRPG's** goals and the ISMS (Information Security Management System) is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

DRPG's strategic business plan and risk management framework provides the context for identifying, assessing, evaluating, and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessments, Statement of Applicability and Risk Treatment Plans identify how information-related risks are controlled.

The Head of IT / Information Security Manager 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.

Business continuity and contingency plans, data backup procedures, avoidance of viruses, hackers and emerging cyber threats, 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 Handbook and are supported by specific documented policies and work instructions.

All **DRPG's** team members and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implement's this policy and will receive appropriate training.

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

DRPG has established that the CEO, Board of Directors and Departmental Managers are committed to the ISMS framework and will ensure that all team members within the company participate.

The CISO (Chief Information Security Officer) will be responsible for managing departmental information risks; including maintaining and reviewing the information risk register and ensuring that information risks are assessed and mitigated to an acceptable level. The CISO will ensure that the policy is periodically reviewed and will lead the team to support the ISMS framework comprising:

The Head of IT / Information Security Manager will be responsible for the security of information in electronic form and cryptographic control and will be supported by the IT support team.

The Information Security Manager will be responsible for co-ordinating risk assessments with information asset owners (named individuals responsible for each identified information asset).

The departmental Manager's or Director's will be responsible for their team, and any key **DRPG** person's or **DRPG** contractor is responsible for the confidential information for either the business, a client or third party.

DRPG has a responsibility to adhere and abide to all applicable UK and EU legislation as well as a variety of regularity and contractual requirements. (See legal register LR01)

DRPG has achieved certification of its ISMS to ISO27001:2013 in August of 2016 and is committed to its continual improvement.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, 'information security' is defined as:

Preserving

This means that management, all full time or part time employees, 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 the Information Security Handbook) and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in **DRPG's** disciplinary policy. All team members will receive information security awareness training and more specialised team members will receive appropriate specialised information security training.

the availability,

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 **DRPG** 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 disaster recovery and business continuity plans.

Confidentiality

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 **DRPG's** information and its systems.

and 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 and data backup plans and security incident reporting. **DRPG** must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

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

and 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, websites, PCs, laptops, and mobile phones, as well as on CD ROMs, 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 systems how to manipulate information (i.e., the software: operating systems, applications, utilities, etc).

of DRPG

DRPG and such 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 Handbook 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 **DRPG**.