PROPELLER

2020 Company Policy Documents

30th September 2020

Information Security Incident Management Policy

PROPELLER

Information Security Incident Management Policy

Propeller Studios Ltd is responsible for the security and integrity of all data it holds. Propeller Studios Ltd must protect this data using all means necessary by ensuring at all times that any incident which could cause damage to the Companies assets and reputation is prevented and/or minimised. There are many types of incidents which could affect security:

- A computer security incident is an event affecting adversely the processing of computer usage. This includes:
    - loss of confidentiality of information
    - compromise of integrity of information
    - denial of service
    - unauthorized access to systems
    - misuse of systems or information
    - theft and damage to systems
    - virus attacks
    - intrusion by humans

- Other incidents include:
    - Missing correspondence
    - Misplaced or missing media
    - Inadvertently relaying passwords

Ensuring efficient reporting and management of security incidents will help reduce and, in many cases, prevent incidents occurring.

1 Purpose

Management of security incidents described in this policy requires the Company to have clear guidance, policies and procedures in place. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which often go unreported and unnoticed – sometimes, over a long period of time and often without resolution.

The purpose of this policy is to:

- Outline the types of security incidents
- Detail how incidents can and will be dealt with
- Identify responsibilities for reporting and dealing with incidents
- Detail procedures in place for reporting and processing of incidents
- Provide Guidance

2 Scope

This policy applies to:

- Company employees, partner agencies, contractors and clients;
- All personnel and systems (including software) dealing with the storing, retrieval and accessing of data

3 Policy Statement

The Company has a clear incident reporting mechanism in place which details the procedures for the identifying, reporting and recording of security incidents.

All Company employees, partner agencies, contractors and clients are required to report all incidents; including potential or suspected incidents, as soon as possible to the Managing Director.

The types of Incidents which this policy addresses include but is not limited to:

Computers left unlocked when unattended
Users of Propeller Studios Ltd computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All Propeller Studios Ltd employees, partner agencies, contractors and clients need to ensure they lock their computers appropriately as described within the Clear Desk and Screen Policy. Discovery of an unlocked computer which is unattended must be reported to the Managing Director.

Password disclosures
Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedures for authorisation. If anyone suspects that their or any other user's password has been disclosed whether intentionally, inadvertently or accidentally, it should be reported as soon as possible to the Managing Director.
Under no circumstances should an employee allow another employee to use their user account details after they have logged onto a system – even under supervision.

Virus warnings/alerts
All Desktop, laptop and tablet computers in use across the Company have Antivirus (including Anti-Spyware/Malware). For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft or damage to Company data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported must be reported to the Managing Director as soon as possible.

Media loss
Use of portable media such as CD/DVD, DAT (magnetic tape), USB Flash sticks/HD drives for storing data requires the user to be fully aware of the responsibilities of using such devices. The use of PCs, laptops, tablets and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorised access. Any authorised user of a portable device who has misplaced or suspects damage, theft whether intentional or accidental of any portable media must report it immediately to the Managing Director.

Alarm Fobs
Staff must immediately report loss of their Alarm Security fob to the Managing Director.

Data loss/disclosure

The potential for data loss does not only apply to portable media it also applies to any data which is:

- Transmitted over a network and reaching an unintended, unauthorised -recipient (such as the use of e-mail to send sensitive data)
- Intercepted over the internet through non secure channels
- Posting of data on the internet whether accidental or intentional
- Published on the Company website and identified as inaccurate or inappropriate (which must be reported)
- Conversationally – information disclosed during conversation
- Press or media – unauthorised disclosure by employees or an ill advised representative to the press or media
- Data which can no longer be located and is unaccounted for on an IT system
- Unlocked and uncollected print-outs from Multi-Function Devices (MFDs)
- Paper copies of data and information which can no longer be located
- Hard copies of information and data accessible from desks and unattended areas

All Company employees, partner agencies and contractors must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of Company data at all times.

Any loss of data and/or disclosure whether intentional or accidental must be reported immediately to the Managing Director.

Personal information abuse

All person identifiable information – i.e. information which can identify an individual such as home address, bank account details etc… must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.
Any abuse/misuse of such person identifiable information must be reported to the Managing Director.

Physical Security

Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room – e.g. a combination key lock mechanism. Lower floor/level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data - concerns about any rooms/office which should be securely locked or access restricted must be reported to the Managing Director.

Logical Security / Access Controls

Controlling, managing and restricting access to the Companies Network, Databases and applications is an essential part of Information Security. It is necessary to ensure that only authorised employees can gain access to information which is processed and maintained electronically. Any incident involving the London Data Centre, or the Secondary Array must be notified to the Managing Director immediately.

Missing correspondence
Data or information which has been sent either electronically or physically which cannot be accounted for e.g. not arrived at the intended destination via physical post, sent electronically, sent for printing but no printed output retrieved etc… must be reported to the Managing Director.

Found correspondence/media
Data stored on any storage media or physically printed information which has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access e.g. unlocked printouts, discarded CD (media), must be reported through the Council's Incident Reporting procedures.

Loss or theft of IT/information
Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinet etc… or which is known/or suspected to have been stolen needs to be reported immediately to the Managing Director.

4 Responsibilities
It is the responsibility for all Company employees, partner agencies, and contractors who undertake work for the Company, on or off the premises to be proactive in the reporting of security incidents. The Companies Incident Reporting procedures are in place to prevent and minimise the risk of damage to the integrity and security of Propeller Studios Limited data and information.

It is also a responsibility of all individuals and handlers of Propeller Studios Limited data and information to ensure that all policies and procedures dealing with the security and integrity of information and data are followed.

5 Compliance with Legal and Contractual Obligations
- The Data Protection Act (1998) requires that personal data be kept secure against unauthorised access or disclosure.
- The General Data Protection Regulations require that personal data be kept secure against unauthorised access or disclosure.
- The Computer Misuse Act (1990) covers unauthorised access to computer systems.

6 Breaches of Policy
Breaches of this policy and/or security incidents are incidents which could have, or have resulted in, loss or damage to Company assets, including IT equipment and information, or conduct which is in breach of the Companies security procedures and policies.

All Company employees, partner agencies and contractors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Companies Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Company.

In the case of third party vendors, consultants or contractor's non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Companies ICT systems or network results from the non-compliance, the Company will consider legal action

against the third party. The Company will take appropriate measures to remedy any breach of the policy through the relevant contracts in place. In the case of an employee then the matter may be dealt with under the Companies disciplinary process.

Andy Hammond
Managing Director

Propeller Reference Number	P0027
Version	V7
Document Owner	A. Hammond
Date	30/09/2020
Renewal Date	30/09/2021

PROPELLER

Propeller Studios Ltd,
First Floor, Alexander House Business Centre,
40a Wilbury Way, Hitchin, Hertforshire SG4 0AP

Tel: +44 (0)1462 440077