stun

Stun Creative Ltd

www.stuncreative.net

Information Security / GDPR Policy

1. Purpose

1.1 This policy provides a framework for the management of information security throughout Stun Creative Ltd. It applies to:

- all those with access to Stun Creative Ltd information systems, including staff, visitors and contractors
- any systems attached to the Stun Creative Ltd computer or telephone networks and any systems supplied by Stun Creative Ltd
- all information (data) processed by Stun Creative Ltd pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form, any communications sent to or from Stun Creative Ltd and any information (data) held on systems external to the network
- all services provided by Stun Creative Ltd to third parties where information is exchanged
- principal information assets including the physical locations from which Stun Creative Ltd operates.

2. Aims and Commitments

2.1 Stun Creative Ltd recognises the role of information security in ensuring that users have access to the information they require in order to carry out their work. Computer and information systems underpin all Stun Creative Ltd' activities, and are essential to its administrative functions.

2.2 Any reduction in the confidentiality, integrity or availability of information could prevent Stun Creative Ltd from functioning effectively and efficiently. In addition, the loss or unauthorised disclosure of information has the potential to damage Stun Creative Ltd' reputation and cause financial loss.

2.3 To mitigate these risks, information security must be an integral part of information management, whether the information is held in electronic or hard-copy form.

2.4 Stun Creative Ltd is committed to protecting the security of its information and information systems in order to ensure that:

- the integrity of information is maintained so that it is accurate, up to date and 'fit for purpose'
- information is always available to those who need it and there is no disruption to the business
- confidentiality is not breached so that information is accessed only by those authorised to do so (the "need to know" principle)
- Stun Creative Ltd meets its legal requirements, including those applicable to personal data under the General Data Protection Regulation (GDPR) and Data Protection Act 2018
- the reputation of Stun Creative Ltd is safeguarded.

2.5 Information security risk assessments should be performed for all information systems on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limits.

2.6 Stun Creative Ltd is committed to providing sufficient education and training to its staff to ensure they understand the importance of information security and, in particular, exercising appropriate care when handling confidential/personal information and understanding the requirements of the GDPR as it applies to Stun Creative Ltd business operations.

2.7 Stun Creative Ltd will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies and network and telecommunications operators in respect of its information security policy.

2.8 Breaches of information security must be recorded and reported to appropriate bodies in Stun Creative Ltd who will take action and inform the relevant authorities

2.9 This Policy and all other supporting policy documents shall be communicated as necessary throughout Stun Creative Ltd to meet its objectives and requirements.

3. Responsibilities

3.1 The Stun Creative Ltd Board has ultimate responsibility for information security within the organisation. More specifically, it is responsible for ensuring that Stun Creative Ltd complies with relevant external requirements, including legislation.

3.2 The Stun Creative Ltd Directors are responsible for:

- ensuring that staff are aware of this policy
- seeking adequate resources for its implementation
- monitoring compliance
- conducting regular reviews of the policy, having regard to any relevant changes in legislation, organisational policies and contractual obligations

- ensuring there are clear direction and visible management support for security initiatives.

3.3 Agreements with third parties involving accessing, processing, communicating or managing information or information systems should cover all relevant security requirements and be covered in contractual arrangements.

4. Risk Assessment and the Classification of Information

4.1 The degree of security control required depends on the sensitivity or criticality of the information. The first step in determining the appropriate level of security therefore is a process of risk assessment in order to identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring.

4.2 The risk assessment will identify Stun Creative Ltd information assets; define the ownership of those assets and classify them, according to their sensitivity and/or criticality to the department or Stun Creative Ltd as a whole. In assessing risk, we will consider the value of the asset, the threats to that asset and its vulnerability.

4.3 Where appropriate, information assets will be labelled and handled in accordance with their criticality and sensitivity.

4.4 Information security risk assessments will be repeated periodically and carried out as required during the operational delivery and maintenance of Stun Creative Ltd' infrastructure, systems and processes.

5. Personal Data – GDPR Policy.

5.1 As an organisation Stun Creative Ltd processes personal data in relation to its employees (including temporary staff), directors, volunteers and users of our services.

5.2 Stun Creative Ltd is registered under the Data Protection Act 2018 and has an entry in the Data Protection Register. This Register is maintained by the UK Information Commissioner.

5.3 Stun Creative Ltd commits to:

- Comply with all GDPR requirements and also industry good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held

- Provide training and support for staff who handle personal data, so that they can act confidently and consistently
- Notify the Information Commissioner voluntarily.

5.4 Stun Creative Ltd holds data on individuals for the following general purposes:

- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- Statistical information
- Monitoring, evaluation and providing best possible service to those who use our services.

5.5 All staff and volunteers are responsible for ensuring that all personal data received by them is handled in accordance with the Stun Creative Ltd Data Protection Policy, which is a linked policy to this Information Security Policy, and in accordance with the Data Protection Act 2018 and subsequent updates to this regulation.

6. Protection of Confidential Information

6.1 Stun Creative Ltd respects the privacy of our paid employees, volunteers and work placements and also ensures that they all understand the importance of confidentiality for client information.

6.2 Storage of information

6.2.1 Confidential information should be kept secure using, where practicable, dedicated storage (e.g. file servers) rather than local hard disks, and an appropriate level of physical security.

6.2.2 File or disk encryption should be deployed as an additional layer of defence, where physical security is considered insufficient.

6.2.3 Personal confidential information must never be stored on memory sticks or laptops unless encrypted.

6.3 Access to information

6.3.1 Confidential information must be stored in such a way as to ensure that only authorised persons can access it on a "need to know" basis.

6.3.2 All Stun Creative Ltd users must be authenticated in line with our Password Issue Procedure. This policy is linked to this Information Security Policy.

6.3.3 Users with access to confidential information will be security vetted, as appropriate, in accordance with existing policies.

6.3.4 Physical access should be monitored and access records maintained.

6.3.5 If a situation of potential abuse is suspected based on confidential information passed on to them, staff may ask permission from the service user to pass on information to an appropriate authority

6.4 Remote access of information

6.4.1 Where remote access is required, this must be controlled via a well-defined access control policy and tight access controls provided to allow the minimum access necessary.

6.4.2 Any remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication.

6.5 Copying of information

6.5.1 The number of copies made of confidential information, whether on portable devices or media or in hard copy, should be the minimum required and, where necessary, a record kept of their distribution. When no longer needed, the copy should be deleted or, in the case of hard copies, destroyed.

6.5.2 All copies should be physically secured e.g. stored in a locked cupboard drawer or filing cabinet.

6.6 Use of portable devices or media

6.6.1 Procedures should be in place for the management of removable media in order to ensure that they are appropriately protected from unauthorised access.

6.6.2 The permission of the information owner should be sought before confidential information is taken off site. The owner must be satisfied that the removal is necessary and that appropriate safeguards are in place e.g. encryption.

6.6.3 The password of an encrypted device must not be stored with the device

6.7 Hard Copies

6.7.1 Protective marking: Documents containing confidential information should be marked as 'Confidential' or with another appropriate designation e.g. 'sensitive', etc, depending on the classification system adopted by the department.

6.7.2 Storage: Wherever practicable, documents with confidential information should be stored in locked cupboards, drawers or cabinets. Where this is not practicable and the information is kept on open shelving, the room should be locked when unoccupied for any significant length of time.

Keys to cupboards, drawers or cabinets should not be left on open display when the room is unoccupied.

6.7.3 Removal: Confidential information should not be removed from Stun Creative Ltd unless it can be returned on the same day or stored securely overnight.

6.7.4 Transmission: If confidential documents are sent by fax, the sender should ensure they use the correct number and that the recipient is near to the machine at the other end ready to collect the information immediately it is printed.

If confidential documents are sent by external post, they should ideally be sent by a form of recorded delivery. The sender must ensure that the envelope is properly secured.

If confidential documents are sent by internal post the documents should be placed in an envelope marked 'Confidential' with the addressee's name clearly written on it.

6.7.5 Disposal: Confidential documents must be shredded in a confidential manner prior to disposal.

6.8 Enforcement of the Information Security Policy

6.8.1 Any failure to comply with the Stun Creative Ltd Information Security Policy may result in disciplinary action.

6.8.2 Any loss or unauthorised disclosure must be promptly reported to the Stun Creative Ltd Managing Director in line with our Data Security Breach Policy which is a policy linked to this Information Security Policy.

6.8.3 Computer security incidents involving the loss or unauthorised disclosure of confidential information held in electronic form must be reported to the Stun Creative Ltd Managing Director and investigated immediately.

6.8.4 If the loss or unauthorised disclosure involves personal data, whether electronic or hard copy, Stun Creative Ltd' Data Protection Officer must also be informed, either by e-mail or phone.

7. Compliance

7.1 Stun Creative Ltd has established this policy to promote information security and compliance with relevant legislation, including the Data Protection Act. Stun Creative Ltd regards any breach of information security requirements as a serious matter, which may result in disciplinary action.

7.2 Compliance with this policy should form part of any contract with a third party that may involve access to network or computer systems or data.

7.3 Relevant legislation includes, but is not limited to:

- The Computer Misuse Act (1990)
- The Data Protection Act (1998) – replaced by Data Protection Act 2018 and General Data Protection Regulation (GDPR) in May 2018
- The Regulation of Investigatory Powers Act (2000)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000)
- The Freedom of Information Act (2000)
- The Special Educational Needs and Disability Act (2001).

Signed by: **David McKenna**
Director

Last Review Date 1 March 2021