SUGAR BUTTONS CREATIVE

Information Security Policy

INFORMATION SECURITY POLICY

1 Table of Contents:

1. Document Control

Document owner	Imogen Davison, Director, Sugar Buttons Creative
Prepared by	Glow Virtual Assistants
Reviewed by	Imogen Davison, Director, Sugar Buttons Creative
Approved by	Imogen Davison, Director, Sugar Buttons Creative
Approved on	1st May 2018
Next review date	1st April 2019
Reference	ISP_001
Version	1.0
Classification	Public

Distribution list	
Imogen Davison	To approve and authorise

Communication	The Information Security Policy is published on public facing websites.

2. Introduction

Sugar Buttons Creative is registered with the Information Commissioners Office (ICO).

Sugar Buttons Creative has an ethical, legal and professional duty to ensure the information he holds conforms to the principles of confidentiality, integrity and availability. In other words, the information Sugar Buttons Creative is responsible for is safeguarded where necessary against inappropriate disclosure, is accurate, timely and attributable, and is available to those who should be able to access it.

This Information Security Policy outlines Sugar Buttons Creatives approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of data and information systems.

Sugar Buttons Creative considers information to be a strategic asset that is essential to his core business and objectives. He has a responsibility to manage effectively the risks around protecting the confidentiality, integrity and availability of data and in complying with all statutory, regulatory and legal requirements.

Sugar Buttons Creative recognises the General Data Protection Regulation (GDPR) and will endeavour to ensure that all personal data is stored and processed in compliance with this regulation from 25 May 2018, the date the regulation comes into force.

3. Statement of Intent

The main purpose of this Policy is to describe the minimum level of protection that Sugar Buttons Creative expects of all Sugar Buttons Creative information systems to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

A secondary but very relevant purpose of this Policy is to ensure that all users understand their responsibilities for protecting the confidentiality and integrity of the data that they handle, including making users aware of relevant legislation.

The overarching objectives set out in the Policy are:

- To support the business objectives in a flexible and effective way
- To maintain adequate regulatory compliance
- To protect Sugar Buttons Creative information assets
- To maintain business continuity

The policy of Sugar Buttons Creative is to protect information systems from unauthorised access, use, disclosure, destruction, modification, disruption or distribution.

Sugar Buttons Creative will ensure business, legal, regulatory requirements and contractual information security obligations are met.

Information security management system will be monitored regularly with reporting of the status and effectiveness at all levels.

4. General Statement of Scope

This Policy is applicable and will be communicated to all relevant client 3rd parties who interact with information held by Sugar Buttons Creative and the information systems used to store and process it.

This Policy applies to Sugar Buttons Creative.

5. Roles and Responsibilities

5.1 Responsibilities of every user of Sugar Buttons Creative IT resources

5.1.1 Appropriate use of IT resources

Sugar Buttons Creative and any other authorised users of Sugar Buttons Creative IT resources are expected to meet the acceptable usage policies and related terms and conditions of the services provided by Sugar Buttons Creative and by any 3rd party on our behalf under licensing agreements.

5.1.2 Confidentiality of passwords

Users must manage passwords with care and processes should be in place to ensure confidentiality from the initial creation, storage in applications, communication and day to day usage.

5.2 Responsibilities specific to Sugar Buttons Creative

5.2.1 Appropriate use of IT resources

Sugar Buttons Creative and any third parties authorised to use Sugar Buttons Creative systems are accountable for understanding and following Sugar Buttons Creative information security policies, as well as promoting safe practices within their teams and monitor compliance.

5.2.2 Asking for help, reporting a concern

Sugar Buttons Creative and authorised third parties are responsible for asking for assistance when in doubt about how to proceed or interpret a policy and also to report any concern or suspect activity encountered.

5.3 Responsibilities of senior management

5.3.1 Risk ownership

Sugar Buttons Creative owns the overall risk management process, and the prioritisation and acceptance of risks.

5.3.2 Risk Acceptance

Sugar Buttons Creative has the accountability for taking a stance on risks ensuring the business operates in line with his expectations and within regulation.

5.3.3 Risk Treatment

Sugar Buttons Creative will identify and mitigate risks taking advice from other sources in assessing and managing risk. Ultimately, the responsibility for risk lies with Sugar Buttons Creative.

5.3.4 Policies and education

Sugar Buttons Creative is responsible for communicating acceptable levels of risk and mitigation practices to any authorised 3rd parties via policy, standards and awareness programs.

5.3.5 Incident response

Sugar Buttons Creative is responsible for effectively responding to significant information security related incidents.

5.4 Responsibilities specific to 3rd party providers

5.4.1 Meeting terms of service/contract agreements, right to audit.

3rd party shall adhere to the IT acceptable usage policy as well as any other requirements specified in the service contract.

6. Policy

6.1 Organisation of information security

6.1.1 Ultimate accountability for security

Sugar Buttons Creative has the ultimate accountability for implementing information security in his businesses.

6.1.2 Information security reviews

A regular review of information security shall be established and led by Sugar Buttons Creative. The review will be completed annually.

Sugar Buttons Creative will review and discuss information security issues regularly, including delivering policy and awareness training / updates as required.

6.1.3 Information Security Manager

It is not currently appropriate for Sugar Buttons Creative to have the role of Information Security Manager due to the small scale of the business.

6.1.4 Segregation of duties

Conflicting duties and areas of responsibility are unlikely to arise given the current scope and scale of Sugar Buttons Creative. However, it is recognised by Sugar Buttons Creative that segregation of duties is good business practice to reduce opportunities for unauthorized or unintentional modification or misuse of the business assets.

6.2 Policy management, education and awareness

6.2.1 Policies as minimum expectation, need for risk management

Managing risks is an essential part of the business activity at all levels of management. The information security policies are the minimum expectation to address information security risks according to well established practice.

Sugar Buttons Creative should assess the business, legal, contractual and corporate social responsibility risks and requirements in each relevant jurisdiction to decide on the need for additional controls or exceptions and be able to justify and be accountable for these decisions.

6.2.2 Policy issuing, communication and updating

Policies and procedures for information security and data protection will be maintained, approved by management, published and communicated to relevant authorised external parties. These Policies should be reviewed and updated at least annually.

6.2.3 Trust, but verify

The Policy statements are necessary but not sufficient on their own. Sugar Buttons Creative should demonstrate the application of the controls and best practice.

6.2.4 Awareness and education on policies and procedures

Sugar Buttons Creative should ensure external authorised parties working with Sugar Buttons Creative systems and data are formally aware of and educated on the policies and procedures they must be compliant with. This is a fundamental step to establishing any individual's accountability.

6.3 Human Resource Security

Sugar Buttons Creative does not currently have any employees.

6.4 Data / assets management

6.4.1 Data classification

Sugar Buttons Creative must identify the data being used for fulfilling tasks and adopt processes appropriate to protect the information according to its risk. It should be assumed that all information is critical.

6.4.2 Retention of information

Sugar Buttons Creative will have processes in place to safely dispose of information as required by law or, within legal compliance, when it is no longer necessary to retain.

Data stored by Sugar Buttons Creative electronically, is stored on local laptops, or stored with 3rd party software providers. When electronic data is required to be deleted, this is completed locally from laptops ensuring that all relevant data is removed or is completed via the 3rd party software following their standard deletion routines.

Generally, retention periods are defined by Sugar Buttons Creative and by the clients of Sugar Buttons Creative, but always in accordance with the relevant regulation.

Hard copies of data stored by Sugar Buttons Creative may be retained and stored in a locked filing cabinet within a locked office.

6.4.3 Safe storage, use and disposal of electronic media and surplus hardware

Sugar Buttons Creative has the responsibility to securely store and dispose of media and hardware using best practice, such as:

Storage, use:

- Devices to be password protected.
- Individual files to be password protected.
- Devices to be stored securely when not in use, out of direct sight of windows etc.
- Operating system to be kept updated with manufacturer recommended updates.
- Only manufacturer approved and recommended software updates to be applied.
- Operating system firewall to be turned on.
- Anti-virus protection to be installed.
- Regular sweeps for virus and malware to be conducted.

Disposal:

- Device to be reset to factory settings to eliminate all traces of data.
- Where possible, hard drive to be removed for destruction.

Sugar Buttons Creative recognises the environmental impacts of the disposal of media and hardware and would employ best practice at the time of disposal to limit the impact. Arrangements need to be dealt with on a case by case basis.

6.4.4 Use of removable media

Sugar Buttons Creative accepts that in certain circumstances the use of removable media is necessary. Where this use is defined as being required, the media device should be rest to factory settings before and after use (to remove all traces of previous / current data). The use of encryption will be considered on a case by case basis. The removable media is to be securely stored.

6.4.5 Physical security, controlled areas

Sugar Buttons Creative is responsible for ensuring the security of it's hardware, systems and media, protecting them against intentional or accidental physical damage.

6.5 Security by design, secure architecture, acquisition and development

6.5.1 Governance on approved technology and security design principles

Should the use of new technology be required in a specific project or assignment, generally Sugar Buttons Creative will determine if the suggested approach and technologies are acceptable.

6.5.2 Information security in new projects

Information security shall be considered for any new project which falls outside of the standard processing techniques or systems.

6.5.3 Separation of Environments

Due to the nature of the current Sugar Buttons Creative business model, system environments, for example test and production, are not required.

6.5.4 Protection from malware

As referred to in 6.4.3 the default approach is that all Sugar Buttons Creative hardware should have detection, prevention and recovery controls to protect against malware combined with appropriate user awareness. Exceptions need to be formally approved on a case by case basis by Sugar Buttons Creative.

6.5.5 Minimum security features in systems

Systems should be developed/acquired and configured with the security features necessary to enable enforcement of the following:

- Authorised users can only access data and functionality for which they are authorised.
- Accountability for usage is maintained via appropriate audit trails.

6.5.6 Installation of software, patching

As referred to in 6.4.3 manufacturer approved / recommended software updates should be kept current. To facilitate this, ‘updates’ should always be set to auto-update.

6.5.7 Testing of security

Whilst Sugar Buttons Creative has no formal security testing procedure, periodically testing of security may be undertaken as part of the regular business as usual.

6.6 Technical and operational security

6.6.1 Control requirements for remote and mobile access / working

Due to the nature and scale of Sugar Buttons Creative there are no additional control requirements for remote access.

With regards to mobile access and working, Sugar Buttons Creative will be aware of surroundings and take any appropriate measures to ensure security, including but not limited to, the physical security of the hardware and data.

6.6.2 Encryption of data

Sugar Buttons Creative does not currently regularly encrypt data unless it is required for specific projects. Data is generally transferred electronically through known channels / systems. Where there are exceptions to this, the circumstances and need for encryption will be determined on a case by case basis.

6.6.3 Logging and auditing

As such, Sugar Buttons Creative does not actively log or audit systems use due to the nature of the business model as previously described. Therefore, only manufacturer, software or 3rd party logging is completed. For example, website hosting provided by third parties maintains an audit of changes to pages and content.

6.6.4 Physical and environmental security

As previously described in this Policy, it is the responsibility of Sugar Buttons Creative to provide physical and environmental security for devices, hardware and hard copies of data. Exceptions to this are considered on a case by case basis.

6.6.5 Data backup and restore procedures

Currently, third party storage providers are used by Sugar Buttons Creative for the storage of some client data. 3rd party systems maintain their own backups.

System backups and restore procedures are not performed explicitly by Sugar Buttons Creative, rather, these are inherent in the operating systems and software employed by the business.

6.7 Access management

6.7.1 Due diligence before granting access

Access to systems and information, including setting up permanent network connectivity solutions, will be granted to third parties/service providers only after a due diligence assessment has been performed and after the employment or service contracts, including confidentiality and accountability clauses has been agreed in writing.

6.7.2 User accountability for security

All third parties using Sugar Buttons Creative systems are accountable for understanding and following Sugar Buttons Creative security policies, in particular on how to protect their accounts and passwords from misuse.

6.7.3 Privileged access to systems

All privileged/administrator activity (e.g., providing access to data, maintenance, and support) will be traceable to the individuals through the 3rd party software / system providers routines.

6.8 Incident management

6.8.1 Incident response

Sugar Buttons Creative incident management will be maintained by Sugar Buttons Creative. The incident response will be determined on a case by case basis.

6.8.2 Contact with authorities

Appropriate contacts with relevant authorities and external parties shall be maintained. In case of an incident, contacts will be nominated who are authorised to liaise with authorities and external parties.

6.9 Continuity management

6.9.1 Secure operations in contingency

People, assets and information services need to be protected in a disaster situation. Should such situations arise, each will be treated on a case by case basis.

6.9.2 Business management responsibility for security

Sugar Buttons Creative is responsible for security and, where appropriate, the availability of systems/data.

6.10 Compliance, validation and certification

6.10.1 Compliance with the law

Sugar Buttons Creative are accountable for operating within the law, and it is their responsibility to be aware of legal and contractual requirements and implement the controls within their remits to comply.

6.10.2 Information security in contracts with 3rd parties

Sugar Buttons Creative contracts with 3rd parties, including contracts with Sugar Buttons Creative clients, will contain appropriate security and regulatory or contractual obligations. Where Sugar Buttons Creative has no powers to set or amend the contractual wording of 3rd party providers, the appropriateness of each contract will be considered on a case by case basis.

6.10.3 Supplier service delivery management

Sugar Buttons Creative assume responsibility for monitoring and reviewing supplier service delivery where this is appropriate.

6.10.4 Management controls

When appropriate, Sugar Buttons Creative should review the compliance of information processing and procedures against this security policy.

6.10.5 Internal and independent security reviews

Internal security reviews may be undertaken at the instruction of Sugar Buttons Creative. Independent security reviews are considered unlikely to be required given the current Sugar

Buttons Creative business model, however they remain an option should an appropriate situation arise.