BADDINOSAUR

Information Security Policy

June 2017

Version 1.0

Contents

1. Introduction and Policy Objectives

For Bad Dinosaur the security of our and our clients data and systems is of utmost importance and in fact underpins the value that we offer to clients. As such, we must protect against loss, corruption, misuse and theft.

The object of this policy is to ensure that our information, and that of our clients, remains protected whilst under our control from all types of Information Security and Cyber threats, both internal and external.

The aim of this policy is to ensure that Bad Dinosaur has well-documented parameters for the assessment and management of information security risks, with clear responsibilities understood by clients, potential clients and those within the business.

2. Policy Ownership

The Information Security Policy is a Board matter, which is sponsored, reviewed and approved by the Board of Directors.

Due to the structure of the company at present the policy ownership, and those responsible for the currency of the policy and its application, sits with the Directors.

3. Applicability and Scope

This policy applies to the whole of Bad Dinosaur's business and to all systems and information assets.

For the purposes of this policy, information includes verbal, electronic, paper, or any other media formats. Systems can include business processes and workflows, physical computer equipment, mobile devices, networks, permanent and removable media and most pertinently cloud-based environments and solutions that Bad Dinosaur or their clients make use of.

This policy applies equally to all Bad Dinosaur employees, both permanent and temporary.

4. Risk Management and Appetite

At present, Bad Dinosaur does not have the scale for the operation of a Risk Management Framework. Instead a set of guiding principles is to be adhered to until the business is of a scale to warrant the use of a Framework. Supporting this position is the fact that all

Directors are employees and intimately invested in the protection of Bad Dinosaur and it's clients from harm.

Bad Dinosaur has zero appetite for Security related incidents, which affect clients or their customers, caused by an omission or lack of care by Bad Dinosaur. The following Risk Management principles will therefore be adhered to:

- Risk is to be considered at all stages of engagement with clients, from service design to change and secure removal of data.
- Identified risks should be recorded in a risk register.
- Mitigation must be considered and recorded in the risk register.
- The risk register must be reviewed bi-monthly in order to identify relevant changes including level of risk in light of the moving landscape of Information and Cyber Security Threats.

5. Policy Statements

The following minimum standards apply.

1.1 Organisational Principles

- The Information Security Policy is a Board approved policy and is communicated to all employees and relevant external parties.
- Risks to Bad Dinosaur and its clients will be managed according to the Risk Management Principles stated in the Information Security Policy.
- All employees are responsible for the identification of risks and their management.
- All Security Breaches and incidents (both actual and suspected) must be reported to affected clients in line with the contractual agreements.
- All Security Breaches and incidents (both actual and suspected) must addressed continuously until any affected client is satisfied that the incident is at an end.

1.2 People Principles

- Before employment both temporary and permanent staff must undergo background checks in the form of Disclosure Scotland check and following up of references stated on CVs.
- All staff must undergo Security Awareness Training.
- All staff must maintain an appropriate level of knowledge of Information Security good practices.
- Malicious security breaches and data theft will be dealt with via termination of employment and the commencement of legal avenues as applicable.

1.3 Systems Principles

- Bad Dinosaur will not provide services to client environments which do not take appropriate consideration of security in their design.

1.4 Data Retention and Destruction

- Client confidential data stored on media (any) must be securely destroyed when requested by clients; for computer systems where data is feasible this should be through total destruction of storage devices such as hard disks or USB drives; and for paper by shredding or fire.

6. Version History

Version	Date	Status	Comments
1.0	June 2017	Board Approved	