Bit10 IT Security Policy

www.bit10.net

1. Introduction

Bit10 develops web and mobile applications and provides hosting services for websites and servers.

The importance of the data on these systems is of paramount importance to Bit10 and its customers and as such access to this data must be restricted to authorised personnel only.

Corruption or illegal access to client data could affect both Bit10's reputation and that of its clients.

2. Objective

This Policy addresses the security of the Bit10's IT systems and the information stored on them. The Policy's objective is to protect Bit10 from security problems that might have an adverse impact on its operations and that of its clients.

Security problems include, but are not necessarily confined to, confidentiality (the wrong people obtaining information), integrity (information being altered without permission, whether deliberate or accidental) and availability (information not being available when it is required).

The widest possible definition of security will be used to include all types of incident that impact the effective use of information. This includes the performance, consistency, reliability, accuracy and timeliness of equipment, systems, and data.

3. Principles

3.1 Approach

- Use all reasonable, appropriate, practical and effective security measures to protect important processes and assets in order to achieve the security objective.
- Use ISO 27001: Code of Practice for Information Security Management as a framework for guiding the approach to managing security.
- Continually examine ways in which security measures to protect and enhance our business can be improved.
- As a responsible organisation Bit10 shall protect and manage its information assets to enable it to meet its contractual, legislative, privacy and ethical responsibilities.

3.2 Responsibilities

NetPlan (ISO 27001, 9001, PCI DSS registered) are responsible for overseeing the security of Bit10's client facing servers hosted with them and our internal IT department are responsible for our internal servers and providing client access to client servers.

Everyone granted access to client systems shall be responsible for protecting its information assets, systems and infrastructure and shall protect likewise the information assets of third parties.

All members of Bit10 shall be responsible for reporting shortfalls in existing security practices and/or improvements that could be made to Information Services.

3.3 Practices

- Risk analysis techniques will be used to identify security risks and their relative priorities. Identified risks will be responded to promptly, implementing safeguards that are appropriate, effective, culturally acceptable and practical.
- Information shall be shared as appropriate within and outside Bit10 in order to facilitate business in an efficient and effective manner. Information may be designated as, or otherwise considered to be, confidential, and Bit10 has obligations under the Data Protection Act 1998 to that effect.
- Where practicable all actions shall be attributable to an identified individual.
- All use of computer and information systems and information (including third party information) shall be attributable, protected by safeguards and handling rules in accordance with current legislation requirements.
- Subject to the requirements of current legislation Bit10's hosting provider, NetPlan shall monitor routinely network traffic to assure the continued integrity and security of Bit10 and client systems. Bit10 shall ensure that its activities can continue with minimal disruption, or other adverse impact, should it suffer any security incident to it as an organisation or to any of its locations or services.
- Actual or suspected security incidents will be reported promptly to the CEO, who will manage the incident to closure, and analyse it for lessons to be learnt.
- Documented Regulations, Procedures and Standards, education and training, will supplement these Principles.

The CEO will monitor compliance with, and the effectiveness of the Policy on a regular basis. The CEO will review and bring forward for approval revisions to the Policy as appropriate.

4. Policy Awareness

The CEO shall publicise this Security Policy to all members of Bit10. All members are expected to be familiar with, and to comply with, the Security Policy. The CEO shall, in the first instance, be responsible for interpretation and clarification of the Security Policy.

5. Applicability and Enforcement

This Policy and compliance with it applies to all members of Bit10 and those who use its computer and information systems.

The CEO is responsible for ensuring that suitable regulations, policies and procedures are in place to enforce the principles addressed in this policy.

Bit10 will require the adoption and use of this Security Policy in all joint ventures.

Date: 1 March 2012
Revision: 1.0