IT Security:

Information Security Policy Statement

Document Approval Table

Role	Approval Date	Release Date
Chief Operating Officer	29/08/19	29/08/19
Information Security Manager	29/08/19	29/08/19

Version Control Table

Version	Amended by	Amendment date	History of changes
1.0	Information Security Manager	21/03/10	1st Draft
1.1	Information Security Manager	06/04/10	Final
1.2	Information Security Manager	21/04/10	Document approver added. (ISM)
1.3	Information Security Manager	03/08/10	Internal classification added
1.4	Information Security Manager	18/02/11	SecurStore added to Scope
1.5	Information Security Manager	23/03/11	Managing Director changed to Chief Executive
1.6	Information Security Manager	21/12/11	SunGard removed and Interactive added to the scope.
1.7	Information Security Manager	28/02/12	Extra blank page removed
1.8	Information Security Manager	07/03/14	Bicester reception removed from scope
1.9	Information Security	17/09/14	Scope changed to reflect the

	Manager		new ISO27001:2013 standard
2.0	Information Security Manager	29/01/15	SecurStore changed to KeepItSafe
2.1	Information Security Manager	08/08/16	Charles changed to Ian as approver
2.2	Information Security Manager	09/08/16	Footnote about Scope added.
2.3	Information Security Manager	24/01/17	Contractual added to "Legislative, regulatory and contractual requirements will be met"
2.4	Information Security Manager	04/08/17	Scope updated
2.5	Information Security Manager	18/08/17	Scope updated, "RackSpace hosting service" to "hosting services provided by RackSpace" for clarity
2.6	Information Security Manager	24/01/18	Changed Data Protection Act to General Data Protection Regulation
2.7	Information Security Manager	10/09/18	"Interactive hosting" removed from the scope
2.8	Information Security Manager	13/08/19	Changed Bis-Web Group to Bis-Web
2.9	Information Security Manager	29/08/19	Scope updated after external audit.

Information Security Policy Statement

Objective

To establish the basic policy of the Bis-Web for the use, protection, and preservation of information generated by, owned by or otherwise in the possession of Bis-Web.

The objective of information security is to facilitate business development and maximize stakeholder benefit whilst protecting the company's information assets from all relevant threats

Primary principles: -

Confidentiality	Protecting information assets from unauthorized disclosure;
Integrity	Safeguarding the accuracy and completeness of information and software;
Availability	Ensuring that information and vital services are available when required;

Scope[1] and Applicability

"Bis-Web Limited, trading as ClearView Continuity, based in Bicester, Oxfordshire, covers the business activities relating to the provision; design; development; maintenance and management of Internet and Web services and systems, in accordance with the latest Statement of Applicability"

Information exists in many forms and includes (but is not limited to):

- Hardcopy documents
- Electronic data
- Software
- Hardware
- Storage media
- Communications networks
- Telephone or face-to-face discussions

[1] *The Scope is also defined within "Information Security Manual 27001-2013"*

Policy

- The full ISO 27001 policy can be accessed on Bis-Web's Intranet.
- The policy's goal is to protect Bis-Web's and its clients informational assets[1] against all internal, external, deliberate or accidental threats.
- The Chief Operating Officer has approved the information security policy.
- The security policy ensures that:
    - Information will be protected against **unauthorised access**;
    - **Confidentiality:** protecting information from unauthorised access and disclosure;
    - **Integrity:** safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion;
    - **Availability:** ensuring that information and associated services are available to authorised users whenever and wherever required;
    - **Legislative, regulatory and contractual** requirements will be met;
    - **Business continuity plans** will be developed, maintained and tested[2];
    - **Information security training** will be available for all employees;
    - **All actual or suspected information security breaches** will be reported to the Information Security Manager and will be thoroughly investigated;
- Procedures exist to support the policy, including virus control measures, passwords and continuity plans.
- Bis-Web's information processing facilities may only be used for authorised purposes.
- All use of proprietary software must be in accordance with the licence terms and conditions.
- Business requirements for availability of information and systems will be met.
- The Information Security Manager is responsible for maintaining the policy and providing support and advice during its implementation.

Information security is *everyone's* responsibility.

[1]See scope.

[2]This plan allows users and clients to access information and essential services when needed.

Legal Requirements

Effective information security controls are essential for compliance with U.K. law. Legislation that places specific record keeping and information security obligations on organisations includes:

Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
General Data Protection Regulation
Freedom of Information Act 2000
Privacy and electronic communications Regulations
Telecommunications Act (Lawful Business Practice regulations 2000)
Fire detection and fire alarm systems for buildings

The Bis-Web Board