Data and Information Security Minimum Requirements

Revision Log

Version	Date	Revision Description	Author	Reviewed	Owner
0.1	22/07/16	Draft	S Jackson	ISF	P Jackson
1.0	12/8/16	Approved by ISF for conversion to BVS and PJW format	S Jackson	ISF	P Jackson
1.1	17/02/17	Minor amend re ISO27001 and conversion to group format	S Jackson	ISF	P Jackson
1.2	03/08/18	Inclusion of Verso and small amends to text	S Jackson	PJ	P Jackson
1.3	30/07/19	Update to notification of security incident	S Jackson	PJ	P Jackson

Document review period: 1 Year

Data and Information Security Minimum Requirements

1. Introduction

1.1 The purpose of this Standard is to ensure that BVS Data (pertaining to Building Validation Solutions Ltd, PJ Web Solutions Ltd, BVS Subsidence Ltd and Verso Damage Management Solutions Ltd – hereinafter referred to as BVS) is adequately protected at all times and that security risks in relation to the Services are addressed by the Supplier to the satisfaction of BVS and without prejudice to any other Supplier obligations provided for elsewhere within this Agreement.

1.2 The provisions of this Standard set out BVS's minimum requirements for data security.

2. Supplier Obligations

2.1 The Supplier shall ensure that, in relation to the provision of the Services, BVS Data is protected so as to preserve its: `

2.1.1 confidentiality – the Supplier shall ensure that access to BVS Data is confined to those who need to know it, who have appropriate authority and who are under individual obligations of confidentiality;

2.1.2 integrity – the Supplier shall ensure that BVS Data remains complete and accurate whilst in its possession or control, accordingly the Supplier shall ensure that all systems, assets and networks that come into contact with BVS Data are operating correctly and accordingly to their specifications; and

2.1.3 availability – the Supplier shall ensure that BVS Data in its possession or under its control is available and delivered to the right person and at the time when it is needed.

2.1.4 security – the Supplier shall ensure that BVS Data is secure whilst in its possession or control.

2.2 When processing BVS Data the Supplier shall:

2.2.1 not alter, store, copy, disclose or use any BVS Data except as necessary for the performance by the Supplier of its obligations under this Agreement;

2.2.2 immediately notify BVS if any BVS Data is lost, accessed in an unauthorised way, becomes corrupted, is damaged or is deleted.

2.3 For the avoidance of doubt, to the extent that any BVS Data is held or processed by the Supplier, the Supplier shall supply such BVS Data to BVS without charge, as and when requested to do so by BVS.

2.4 The Supplier shall further ensure that appropriate facilities and procedures are available to ensure that resources are capable of sustaining the performance of the Services.

2.5 The Supplier shall take into account and comply with as appropriate, the following external factors in the provision of the Services and the protection of BVS Data:

2.5.1 legal and regulatory requirements;

2.5.2 best industry practice;

2.5.3 latest technological developments;

2.5.4 when processing BVS Data, the data security requirements as set out in this Standard; and

2.5.5 when processing BVS Data, any underlying security guidelines and/or instructions provided by BVS to the Supplier from time to time.

3. Security Incidents

3.1 In this Standard "Security Incident" means any event consisting of any:

3.1.1 unauthorised access to, disclosure, theft, loss, modification or destruction of BVS Data or any other data held, used or conveyed in connection with the provision of the Services;

3.1.2 theft of any equipment necessary to provide the Services;

3.1.3 degradation of the availability of the Services due to denial of service attacks;

3.1.4 unauthorised use of the Services;

3.1.5 failure to comply with any data security requirements as set out in this Standard; and

3.1.6 any attempt to do any of those events described in paragraphs 3.1.1 to 3.1.5 of this Standard.

3.2 When processing BVS Data, the Supplier shall immediately inform BVS of any Security Incident or suspected Security Incident. Responsibility for the management of Security Incidents lies jointly with the Supplier and BVS.

3.3 The Supplier may only disclose details of any Security Incident to its personnel and/or Subcontractors where such disclosure is necessary to comply with the Supplier's security requirements (as detailed in this Standard), or where the disclosure is necessary for the proper performance of such person's functions in providing the Services.

4. Data Security Control Requirements

In order to fully protect BVS Data, the Supplier shall ensure that when it is processing BVS Data:

4.1 It has a dedicated individual at a senior level in its organisation who has accountability for data security;

4.2 data security, policies, standards and risk analysis processes are defined and embedded across its organisation and are available for review on request;

4.3 it complies with the standards set out within this document (or is certified to ISO 27001 / PCI DSS or other equivalent data security standard) for the provision of the Services;

4.4 there is an information classification scheme in operation and BVS Data must be appropriately classified;

4.5 there are measures in place to ensure that any personnel with access to BVS Data are appropriately vetted both at the time of employment and on an on-going basis;

4.6 there are measures in place to ensure that data security and data protection responsibilities and standards of behaviour are in its personnel job descriptions and/or contracts of employment and that security breaches are subject to disciplinary action;

4.7 its personnel are provided with on-going awareness and training with regard to data security;

4.8 physical security arrangements and environmental controls are in place to protect BVS Data processing environments and that audit trails are kept for at least 6 months (including evidence of who has accessed the data processing environments);

4.9 it has control measures in place to prevent other organisations which share the Supplier's facilities from gaining access to BVS Data and/or equipment;

4.10 it has logical access controls in place to limit and protect access to BVS Data;

4.11 where BVS Data is held on your internal system, the logical access controls require user authentication using passwords which shall be a minimum length and require a combination of some or all of upper & lower-case characters, a mix of alpha-numeric characters and/or use of

special characters. Additionally the system shall enforce regular password changes (for example every 30, 60 or 90 days)

4.12 records are in place and are made available to BVS, which demonstrate the access rights which the Supplier enforces for all users of systems holding BVS Data;

4.13 it has controls in place which show which individuals shall have access to BVS Data;

4.14 it has measures in place to ensure the timely revision and/or removal of (as appropriate) physical and logical access for employee who have moved working environments or who have left the Supplier's employment;

4.15 where copies of BVS Data are permitted by BVS, it has measures in place to track and account for all copies of such BVS Data, including electronic copies and hard copies thereof. Portable media (including paper) must be secured and protected if being transported (including using a dedicated courier or registered post);

4.16 it has controls in place to protect the electronic transit of BVS Data (including email, electronic feeds and secure links);

4.17 where possible all messages to be sent are encrypted using a minimum of 128-bit encryption;

4.18 portable media devices are not used in the processing, movement or storage of BVS Data;

4.19 there are measures in place to offer adequate control where the Supplier has an authorised need to transact BVS Data with other third-party organisations. Such transactions must be secure and covered by an adequate contract with suitable information security clauses;

4.20 BVS Data is not transferred or processed outside of the EEA without the written consent of BVS;

4.21 it has controls in place to ensure that communication networks operate in a secure manner;

4.22 the retention and movement of telephony / voice data relating to BVS and/or the Services is adequately controlled;

4.23 it has controls in place over the secure storage of BVS Data (including both physical and logical security);

4.24 it has controls in place to securely dispose of BVS Data and certify secure destruction (including decommissioning of servers, desktops and laptops, as well as removable media and paper based records);

4.25 it has controls in place to ensure the rapid detection, isolation and removal of malicious code and unauthorised mobile code for example with the provision of appropriate virus scanner software that is kept up to date;

4.26 its systems which are connected to external networks are protected by firewalls and supported by Intrusion Detection & Prevention Systems which are monitored and that appropriate actions are taken where necessary;

4.27 it has controls in place to ensure that vendor supplied security updates and patches are applied to relevant software and firmware on a regular basis, e.g. Windows updates;

4.28 its assets which can hold data are subject to asset management controls and are asset register maintained;

4.29 it has controls in place to deal with and manage Security Incidents and assist BVS in investigating any Security Incidents (in accordance with paragraph 3 of this Standard);

4.30 it has controls in place to ensure continuity of service and that it has business continuity and technical recovery plans which meet the business and technical requirements of BVS. Such plans must be subject to periodic testing at least once a year and must meet recovery times proven and be successful; and

4.31 any Service level agreements which it enters into include requirements to ensure on-going data security controls, including:

4.31.1 incident reporting and subsequent management within an agreed timescale (for any business continuity event, data loss, system outage and/or failure of agreed controls and processes); and

I have read and understood this standard and confirm compliance on behalf of:

Company	
Print Name	
Signature	
Date	