1. Introduction

This document defines the information security policy of IMPULSE B2B SOLUTIONS.

As a modern, forward-looking business, IMPULSE B2B SOLUTIONS recognizes at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, IMPULSE B2B SOLUTIONS has implemented anInformation Security Management System (ISMS) in line with the International Standard for Information Security, 1S0/IEC 27001. This standard defines the requirements for an ISMS based oninternationally recognised best practice.

The operation of the ISMS has many benefits for the business, including:

- Protection of revenue streams and company profitability;
- Ensuring the supply of goods and services to customers;
- Maintenance and enhancement of shareholder value; and
- Compliance with legal and regulatory requirements

IMPULSE B2B SOLUTIONS has decided to maintain full certification to ISO/IEC 27001 in order that the effective adoption of information security best practices may be validated by an independent third-party,a Registered Certification Body. In addition, the guidance contained in the ISO/IEC 27017 and 27018 codes of practice has been adopted as these have particular relevance for Cloud Service Providers.

This policy applies to all systems, people and processes that constitute the organization's informationsystems, including board members, directors, employees, suppliers and other third parties who have access to IMPULSE B2B SOLUTIONS systems.

The following supporting documents are relevant to this information security policy and provide additional information about how it is applied:

- Risk Assessment and Treatment Process
- Statement of Applicability
- Supplier Information Security Evaluation Process
- Internet Acceptable Use Policy
- Mobile Device Policy
- Teleworking Policy
- Access Control Policy
- User Access Management Process
- Cryptographic Policy
- Physical Security Policy
- Anti-Ma/ware Policy
- Backup Policy
- Logging and Monitoring Policy

- Software Policy
- Technical Vulnerability Management Policy
- Network Security Policy
- Electronic Messaging Policy
- Information Security Policy for Supplier Relationships
- Availability Management Policy
- IP and Copyright Compliance Policy
- Records Retention and Protection Policy
- Privacy and Personal Data Protection Policy
- Clear Desk and Clear Screen Policy
- Social Media Policy
- HR Security Policy

2. Information Security Policy

2.1 Information Security Requirements

A clear definition of the requirements for information security within Impulse B2B Solution will be agreed and maintained with the internal business and subsequently all ISMS activity is focused on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements about the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the Impulse B2B Solutions Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

2.2 Framework for Setting Objectives

A regular cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, informed by the management review process during which the views of relevant interested parties may be obtained.

Information security objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001 the reference controls detailed in Annex A of the standard will be adopted where appropriate by Impulse B2B Solutions. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with information security risk treatment plans. For details of which Annex, A controls have been implemented and which have been excluded please see the Statement of Applicability.

In addition, enhanced and additional controls from the following codes of practice will be adopted

and implemented where appropriate:

- ✓ ISO/IEC 27002 - Code of practice for information security controls
- ✓ ISO/IEC 27017 – Code of practice for information security controls base on ISO/IEC 27002 for cloud services
- ✓ ISO/IEC 27018 – Code of practice for the protection of personally identifiable information (PII) inpublic clouds acting as PII

The adoption of these codes of practice will provide additional assurance to our customers and help further with our compliance with international data protection legislation.

2.3 Continual Improvement of the ISMS

Impulse B2B Solutions policy regarding continual improvement is to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards
- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to information security
- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties including cloud service customer
- Review ideas for improvement at regular management meetings in order to priorities and assess timescales and benefits

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

2.4 Information Security Policy Areas

Impulse B2B Solutions defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both within and external to, the organization.

The table below shows the individual policies within the documentation set and summarises each policy's content and the target audience of interested parties.

Policy Title	Areas Addressed	Target Audience
Internet Acceptable Use Policy	Business use of the Internet, personal use of the Internet, Internet account management, security, monitoring, and prohibited uses of the Internet service.	Users of the Internet service
Mobile Device Policy	Care and security of mobile devices such as laptops, tablets and smartphones, whether provided by the organization or the individual for business use.	Users of company-equipment and BYOD (Bring Your Own Device) mobile devices
Teleworking Policy	Information security considerations in establishing and running a teleworking site and arrangement e.g. physical security, insurance and equipment	Management and employees involved in setting up and maintaining a teleworking site
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities andsystem and application access control	Employees involved in setting up and managing access control
Cryptographic Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management	Employees involved in setting up and managing the use of cryptographic technology and techniques
Physical Security Policy	Secure areas, paper and equipment security and equipment lifecycle management	All employees
Anti-Malware Policy	Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring and alerts, technical reviews and malware incident management	Employees responsible for protecting the organization' s infrastructure from malware

Backup Policy	Backup cycles, cloud backups, off-site storage, documentation, recovery testing and protection of storage media	Employees responsible for designing and implementingbackup regimes