Information Security Policy

Document Ref.	**:**	**Information Security Policy**
Date Created	**:**	**03/06/2016**
Issue Number	**:**	**4.0**
Issue Created	**:**	**10/05/2019**
Classification	**:**	**Public**
Last Reviewed	**:**	**10/05/2019**

	Signed	**Print**	**Date**
Prepared By		David Carroll	03/06/2016
Authorised By		Martyn Lawson	22/06/2016
Relevant Parties			

AMENDMENT RECORD

Amendment List			Incorporated By	
Issue	**Date**	**Reason for Change**	**Signed**	**Date**
2	06/07/16	Added review frequency to document.	D.Carroll	06/07/16
3	13/06/18	Updated DPA to GDPR	M.Lawson	13/06/18
4	10/05/19	Update GDPR to DPA 2018, Replace management team references with Board of Directors	M Lawson	10/05/19

REVIEW RECORD

Review History			Reviewed By	
Date	**Issue**	**Comments**	**Signed**	**Date**
31/01/18	2.0	Reviewed with no action required	M Lawson	31/01/18
12/06/18	2.0	Reviewed during bi-annual Management Review meeting. Change required to update DPA to GDPR.	M Lawson	12/06/18
10/05/19	3.0	Updates required resulting in v4.0	M Lawson	10/05/19

SUPPORTING DOCUMENTS

Document Title	Reference	Issue	Date

Contents

+44(0)1332 781 882 warwickicsystems.com enquiries@warwickicsystems.com

1. Policy

It is the Company's policy to develop, implement and maintain an Information Security Management System (ISMS) that:

- Provides assurance within the company and to our clients, partners and interested parties that the availability, integrity and confidentiality of their information will be maintained appropriately
- Manages information security risks to all company and customer assets
- Protects the company's ongoing ability to meet contracted commitments through appropriate Business Continuity
- Bases information security decisions and investments on risk assessment of relevant assets considering; Integrity, Availability and Confidentiality
- Takes into account business and legal or regulatory requirements and contractual security obligations
- Maintains awareness of all employees so they can identify and fulfil contractual, legislative and company specific security management responsibilities
- Minimises the business impact and deals effectively with security incidents

This Policy is supported by the following high-level objectives:

- Implementation of a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001 Standard for Information Security Management Systems
- Implementation of a sensitive information control policy including compliance with regulations under the Data Protection Act 2018 to protect client, partner, supplier, our own and personal employee information which is not in the public domain
- Implementation of an Information Security Risk Assessment Process that assesses the business harm likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and controls currently implemented
- Development and implementation of a Business Continuity Plan to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters
- Defined security controlled perimeters and access to controlled offices and facilities to prevent unauthorised access, damage and interference to business premises and information
- Information security awareness guidance for all company employees
- A Board of Directors that supports the continuous review and improvement of the company ISMS
- Implementation of incident management and escalation procedures for reporting and investigation of security incidents for ISMS management review and action

The company information security policy is reviewed by the Board of Directors every 6 months as part of the management review, who recommend amendments and updates to the policy as part of the continuous service improvement process.

This policy will be made available to Interested Parties, where required.