



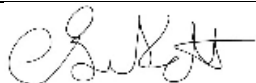
# Information Security Policy

3.0

Author: David Office  
Date Published: 01/04/2019

## 1.0 Version Control

<b>Version:</b>	3.0	<b>(Author) Issued By:</b>	David Office
<b>Issued Date:</b>	01/04/2019	<b>Review Date:</b>	01/04/2020
<b>Document Owner:</b>	David Office	<b>Document Number</b>	ISMS001

<b>Approved By:</b>	Chris Birkett	<b>Position:</b>	Chief Operating Officer
<b>Signature:</b>		<b>Approved Date:</b>	01/04/2019

## 2.0 Document Revision History

Version Control Note: All documents in development are indicated by minor versions i.e. 0.1; 0.2 etc. The first version of a document to be approved for release is given major version 1.0. Upon review the first version of a revised document is given the designation 1.1, the second 1.2 etc. until the revised version is approved, whereupon it becomes version 2.0. The system continues in numerical order each time a document is reviewed and approved.

Version Number	Date	Author Title	Status	Comment/Reason for Issue
1.1	12/03/2018	David Office	Initial Draft	Consolidation of existing policies Migrate to new template
1.2	04/04/2018	David Office	Draft	Updates from Security Governance Committee Review
2.0	19/04/2018	David Office	Released	Release Approved
2.1	19/02/2019	David Office	Updated	ND review and amendments
3.0	19/02/2019	David Office	Approved	Approved by C. Birkett
3.0	19/02/2019	David Office	Released	Policy Released
3.0	01/04/2019	David Office	Review	Policy Reviewed. No Changes
3.0	01/04/2019	David Office	Released	Policy Released

### 2.1 Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. **Any printed copies of this document are not controlled.**

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

## 3.0 Table of Contents

1.0	Version Control .....	1
2.0	Document Revision History.....	1
2.1	Document Status.....	1
3.0	Table of Contents .....	2
4.0	Introduction .....	3
5.0	Objectives, Aim & Scope .....	3
5.1	Objectives.....	3
5.2	Aim .....	3
5.3	Scope.....	4
6.0	Policy Framework.....	5
6.1	Contracts of Employment .....	5
6.2	Security Control of Assets .....	5
6.3	Access Controls .....	5
6.4	Computer Access Controls .....	5
6.5	Application Access Controls .....	5
6.6	Equipment Security .....	5
6.7	Computer and Network Procedures .....	5
6.8	Information Risk Assessment.....	5
6.9	Information Security Events and Weaknesses.....	6
6.10	Classification of Sensitive Information.....	6
6.11	Protection from Malicious Software.....	6
6.12	Removable Media .....	6
6.13	Monitoring System Access and Use .....	6
6.14	System Change Control .....	6
6.15	Business Continuity and Disaster Recovery Plans.....	7
6.16	Training & Awareness .....	7
7.0	Responsibilities .....	8
7.1	Managing Director .....	8
7.2	Data Protection Officer .....	8
7.3	Senior Managers .....	8
7.4	Information Security Officer .....	8
7.5	All Staff .....	8
7.6	External Contractors .....	9
8.0	References .....	10

## 4.0 Introduction

Winn Group has information processing as a fundamental part of the business. It is important, therefore, that the organisation has a clear and relevant Information Security Policy, allowing it to comply with information legislation.

The purpose of Winn Group's Information Security policy is to protect, to a consistently high standard, all information assets. The policy covers security which can be applied through technology but perhaps more crucially, it encompasses the behaviour of the people who manage information in the line of Winn Group business.

Information security is primarily about people but is facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and appropriate, standardised way;
- Assurance that the Winn Group is providing a secure and trusted environment for the management of information used in delivering its business;
- Clarity over the personal responsibilities around information security expected of staff when working on Winn Group business;
- Demonstration of best practice in information security;
- Assurance that information is accessible only to those authorised to have access;
- Assurance that risks are identified, and appropriate controls are implemented and documented.

## 5.0 Objectives, Aim & Scope

### 5.1 Objectives

The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Winn Group by:

- Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation. Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

### 5.2 Aim

The aim of the Winn Group's Information Security Policy is to preserve:

<b>Confidentiality</b>	Access to Data shall be confined to those with appropriate authority.
<b>Integrity</b>	Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
<b>Availability</b>	Information shall be available and delivered to the right person, at the time when it is needed.

### **5.3 Scope**

This policy applies to all employees of Winn Group and associated subsidiaries, contractors, volunteers, vendors and partners.

## **6.0 Policy Framework**

### **6.1 Contracts of Employment**

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain appropriate terms and conditions.

Information security expectations of staff shall be included within appropriate job definitions.

### **6.2 Security Control of Assets**

Winn Group's IT Department will establish an ICT asset management process and associated system, this will involve support and collaboration from vendors where applicable.

All ICT assets, (hardware, software, application or data) shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset.

### **6.3 Access Controls**

Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the relevant IAO. This includes any genuine third-party access to information. This is detailed in the Access Control Policy.

### **6.4 Computer Access Controls**

Access to ICT facilities shall be restricted to authorised users who have business need to use the facilities.

### **6.5 Application Access Controls**

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a license from the supplier.

### **6.6 Equipment Security**

In order to minimise loss of, or damage to, all assets, equipment shall be; identified, registered and physically protected from threats and environmental hazards.

### **6.7 Computer and Network Procedures**

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems and processes with third party vendors working for and on behalf of Winn Group.

### **6.8 Information Risk Assessment**

All information assets will be identified and assigned an Information Asset Owner (IAO). IAO's shall ensure that information risks assessments are performed at least annually, following guidance from the Information Security Officer. This should be increased to quarterly for all 'major' assets. IAO's shall submit the risk assessment results and associated mitigation plans to the Information Security Officer for review. Please see the Information Risk Procedures for further information.

## 6.9 Information Security Events and Weaknesses

All Winn Group information security events, near misses, and suspected weaknesses are to be reported to the Information Security Officer or designated deputy and where appropriate reported as an Adverse Incident upon identification. Please see the security incident reporting procedures for further information.

## 6.10 Classification of Sensitive Information

Winn Group shall implement appropriate information classifications controls, based upon the results of formal risk assessments, to secure their information assets. Further details of the classifications controls can be found in the Document and Records Management Policy.

## 6.11 Protection from Malicious Software

The organisation and its ICT service providers shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff are expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the IT Department or Information Security Officer. Users breaching this requirement may be subject to disciplinary action.

## 6.12 Removable Media

Removeable Media must be encrypted. Removable media that contains software require the approval of the Group Director – IT and Change Management or Information Security Officer before they may be used on Winn Group systems. Users breaching this requirement may be subject to disciplinary action. Further details can be found in the Removable Media Policy.

## 6.13 Monitoring System Access and Use

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. Winn Group will put in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Investigatory Powers Act (2016) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of a system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act and any other applicable law.

## 6.14 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Group Director – IT and Change Management. Further Information can be found in the Change Management Policy.

## **6.15 Business Continuity and Disaster Recovery Plans**

Business Impact Analysis will be undertaken in all areas of the organisation. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

The Information Security Officer has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis. Further Information can be located in the Business Continuity Management Policy.

## **6.16 Training & Awareness**

Information Governance training is mandatory and all staff are required to complete annual on-line Information Governance training.

All staff are required to read the Information Governance User Handbook and accept and sign the declaration.

## **7.0 Responsibilities**

### **7.1 Managing Director**

Information Security is everyone's business although responsibility resides ultimately with the Managing Director, but this responsibility is discharged through the designated role of Data Protection Officer and Information Security Officer.

### **7.2 Data Protection Officer**

The Data Protection Officer (DPO) is responsible for information risk within Winn Group and advises the Board on the effectiveness of information risk management across the Organisation.

### **7.3 Senior Managers**

Senior Managers shall be individually responsible for the security of their physical environments where information is processed or stored. Furthermore, they are responsible for:

- Ensuring that all staff, permanent, temporary and contractor, are aware of the information security policies, procedures and user obligations applicable to their area of work.
- Ensuring that all staff, permanent, temporary and contractor, are aware of their personal responsibilities for information security.
- Determining the level of access to be granted to specific individuals
- Ensuring staff have appropriate training for the systems they are using.
- Ensuring staff know how to access advice on information security matters

### **7.4 Information Security Officer**

The Information Security Officer will:

- Hold a relevant qualification or have relevant industry experience in Information Security.
- Have lead responsibility for information security management within Winn Group acting as a central point of contact on information security for both staff and external organisations.
- Manage and implement this policy and related procedures.
- Monitor potential and actual security breaches.
- Ensure that staff are aware of their responsibilities and accountability for information security.

In carrying out these tasks the Information Security Officer will work closely with the Information Security Governance Committee.

### **7.5 All Staff**

All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. In particular, all staff should understand:

- What information they are using, how it should be protectively handled, stored and transferred;
- What procedures, standards and protocols exist for the sharing of information with others;
- How to report a suspected breach of information security within the organisation;
- Their responsibility for raising any information security concerns with the Information Security Officer.

## **7.6 External Contractors**

Contracts with external contractors that allow access to the organisation's information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

## 8.0 References

The following documents will provide additional information:

Doc Reference Number	Title
ISMS002	Information Security Incident Policy
ISMS003	Acceptable Use Policy
ISMS004	Access Control Policy
ISMS005	Password Policy
ISMS006	Clear Desk & Desktop Policy
ISMS007	Information Classification & Handling Policy
ISMS008	Asset Management Policy
ISMS009	Documents & Records Management Policy
ISMS010	Mobile Computing Policy
ISMS011	Physical & Environmental Security Policy
ISMS012	Removeable Media Policy
ISMS013	Encryption Policy
ISMS014	Bring Your Own Device (BYOD) Policy
ISMS015	Risk Management Policy
ISMS016	Supplier Management Policy
ISMS017	Business Continuity Management Policy
ISMS018	Anti Virus Policy
ISMS019	Software Update Policy
ISMS020	Secure Development Policy
ISMS021	Systems Acquisition Policy
ISMS022	IT Sanitisation, Re-use, Disposal and Destruction Policy
ISMS023	Cryptography Policy
ISMS024	Backup & Restore Policy
ISMS025	Change Management Policy
ISMS026	Teleworker Policy
ISMS027	Secure Area Access Policy
ISMS028	Information Governance User Handbook
ISMS029	CCTV Policy
ISMS030	Project Management Policy
ISMS031	Social Media Policy
ISMS032	Clock Synchronisation Policy
ISMS033	Network Security Policy
ISMS034	Legacy IT Hardware & Software Policy
ISMS035	Outsourcing Policy
	Human Rights Act (1998)
	Data Protection Act (2018)
	General Data Protection Regulation (GDPR) (2016)
	Computer Misuse Act (1990)
	Investigatory Powers Act (2016)
	The Copyright, Designs and Patents Act (1988)
	The Health and Safety at Work Act (1974)
	Telecommunications Act 2000

This document has been prepared using the following standards and their applicable controls as reference:

Standard	Control	Description