



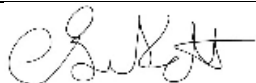
Security Incident Management Policy

1.0

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

1.0 Version Control

Version:	1.0	(Author) Issued By:	David Office
Issued Date:	04/04/2019	Review Date:	04/04/2020
Document Owner:	David Office	Document Number	ISMS002

Approved By:	Chris Birkett	Position:	Chief Operating Officer
Signature:		Approved Date:	04/04/2019

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
0.1	01/12/2017	David Office	Initial Draft	New Document
0.2	04/02/2019	David Office	Updated	Migrate to new template, Updated for DPA2018
1.0	04/02/2019	David Office	Approved	Approved by C. Birkett
1.0	04/02/2019	David Office	Released	Policy Released
1.0	04/04/2019	David Office	Review	Policy Reviewed. No Changes
1.0	04/04/2019	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 Statement	5
	Computers Left Unlocked When Unattended	5
	Password Disclosures	5
	Virus Warnings & Alerts	5
	Media Loss	5
	ID Badges.....	6
	Data Loss/Disclosure	6
	Personal Information Abuse	6
	Physical Security.....	7
	Logical Security / Access Controls	7
	Missing Correspondence.....	7
	Found Correspondence/Media	7
	Loss or theft of IT/Information	7
6.1	Compliance With Legal & Contractual Obligations.....	7
7.0	Breaches Of Policy.....	8
8.0	Responsibilities	9
8.1	All Staff	9
9.0	References	10

4.0 Introduction

Winn Group is responsible for the security and integrity of all data it holds. The business must protect this data using all means necessary in accordance with the General Data Protection Regulation (GDPR) and ISO27001:2013 ISMS, by ensuring at all times that any incident which could cause damage to the Group's assets and reputation is prevented and/or minimised.

There are many types of incidents which could affect security including (but not limited to):

- A computer security incident is an event affecting adversely the processing of computer usage. This includes:
 - Loss of confidentiality of information;
 - Compromise of integrity of information;
 - Denial of service;
 - Unauthorized access to systems;
 - Misuse of systems or information;
 - Theft and damage to systems;
 - Virus attacks;
 - Intrusion by humans.
- Other incidents include:
 - Misplaced or missing media;
 - Missing correspondence;
 - Exposure of Uncollected print-outs;
 - Inadvertently relaying passwords;
 - Loss of mobile phones and portable devices;
 - Loss of ID badge/s.

Ensuring efficient reporting and management of security incidents will help reduce and, in many cases, prevent incidents occurring.

More detailed information on the type and scope of security incidents is provided in the Policy Statement section of this policy.

5.0 Objectives, Aim & Scope

5.1 Objectives

The management of security incidents described in this policy requires Winn Group to have clear guidance, policies and procedures in place. Fostering a culture of proactive incident identification, reporting and logging will help reduce the number of potential and actual security incidents.

5.2 Aim

The aim of this Policy is to:

- Outline the types of security incidents
- Detail how incidents can and will be dealt with
- Identify responsibilities for reporting and dealing with incidents
- Detail procedures in place for reporting and processing of incidents
- Provide guidance to staff as to the correct way to report incidents

5.3 Scope

This policy applies to:

- Winn Group employees, partner agencies, contractors, volunteers, stakeholders and vendors;
- All Winn Group departments, personnel and systems (including software) dealing with the collection, storage and processing of data.

6.0 Policy Statement

Winn Group has a clear incident reporting mechanism in place which details the procedures for the identifying, reporting and recording of security incidents. By continually updating and informing Winn Group employees, partner agencies, contractors, volunteer, stakeholders and vendors of the importance of the identification, reporting and action required to address incidents, Winn Group can continue to be pro-active in addressing these incidents in accordance with the GDPR as and when they occur.

All Winn Group employees, partner agencies, contractors, volunteers, stakeholders and vendors are required to report all incidents – including potential or suspected incidents, as soon as suspected or identified via the Winn Group's Incident Reporting procedures.

The types of Incidents which this policy addresses include (but is not limited to):

Computers Left Unlocked When Unattended

Users of Winn Group computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All Winn Group employees, partner agencies, contractors, volunteers, stakeholders and vendors need to ensure they lock their computers appropriately whenever they leave their desk for any period of time.

Discovery of an unlocked computer which is unattended must be reported via the Winn Group's Incident Reporting procedures And will be managed in accordance with HR Department Disciplinary Policies.

Password Disclosures

Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedures for authorisation in accordance with the Access Management Policy.

If a member of Winn Group suspects that their or any other user's password has been compromised whether intentionally, inadvertently or accidentally, the Information Security Officer and IT Department must be notified through Winn Group's Incident Reporting procedures. Under no circumstances should an employee allow another employee to use their user account details – even under supervision.

For more information regarding Password security and management please see the Winn Group Password Policy which is available on the intranet or via the IT Department's Service Desk.

Virus Warnings & Alerts

All Desktop, laptop and tablet computers in use across the Winn Group have Antivirus (including Anti-Spyware/Malware) software installed. For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft or damage to Winn Group data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported by the user to the IT Department's Service Desk as soon as possible.

Media Loss

Use of portable media such as CD/DVD, magnetic tape, USB Flash sticks, USB Hard Disk drives for storing data requires the user to be fully aware of the responsibilities of using such devices. The use

of PCs, laptops, tablets and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorised access.

All media must be provided by Winn Group (employees MUST NOT use their own media devices), is the property of Winn Group and is encrypted in accordance with the Winn Group Encryption Policy.

Any authorised user of a portable device (including portable media) who has misplaced or suspects damage or theft, whether intentional or accidental, must report it immediately through the Winn Group Intranet Compliance Portal – Report an Information Security Incident.

ID Badges

It is essential for Winn Group to identify individuals whilst in the workplace and wearing ID badges helps the Company to do this. Any authorised employee allocated an ID Badge who has misplaced or suspects theft, whether intentional or accidental must report it immediately through the the Winn Group Intranet Compliance Portal – Report an Information Security Incident.

Data Loss/Disclosure

The potential for data loss does not only apply to portable media but also applies to any confidential data which is:

- Transmitted over a network and reaching an unintended, unauthorised recipient (such as the use of E-mail to send sensitive data)
- Intercepted over the internet through non-secure channels
- Posting of data on the internet whether accidental or intentional
- Published on the Winn Group's website and identified as inaccurate or inappropriate
- Conversationally – confidential information disclosed during conversation
- Press or media – unauthorised disclosure by employees or an ill-advised representative to the press or media
- Data which can no longer be located and is unaccounted for on an IT or manual system
- Unlocked and uncollected print-outs from Multi-Function Devices (MFDs)
- Paper copies of data and information which can no longer be located
- Hard copies of information and data accessible from desks and unattended areas
- Posting paper copies of data and information to unintended, unauthorised recipients internal to Winn Group or external to the business.

All Winn Group employees, partner agencies, contractors, volunteers, stakeholders and vendors must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of Winn Group data at all times.

Any loss of data and/or disclosure whether intentional or accidental must be reported immediately using Winn Group's Incident Reporting procedures.

Winn Group have a duty to report certain types of personal data breach to the relevant supervisory authority. This must be done by Winn Group within 72 hours of becoming aware of the breach.

Personal Information Abuse

All Person Identifiable Information (i.e. information which can identify an individual such as home address, bank account details etc.) must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.

Any abuse/misuse of such Person Identifiable Information must be reported through Winn Group's Incident Reporting procedures.

Physical Security

Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room (e.g. a combination key lock mechanism). Lower / floor level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data - concerns about any rooms/office which should be securely locked or access restricted must be reported to the IT Department Service Desk via Winn Group's Incident Reporting procedures.

Continuing emphasis and re-enforcement of the Winn Group's Clear Desk & Desktop Policy will further help to reduce the number of security incidents.

Logical Security / Access Controls

Controlling, managing and restricting access to the Group's Network, Databases and applications is an essential part of Information Security. It is necessary to ensure that only authorised employees can gain access to information which is processed and maintained electronically. For more information on Logical Security and Access Management please see the Winn Group Access Management Policy.

Missing Correspondence

Data or information which has been sent either electronically or physically which cannot be accounted for e.g. not arrived at the intended destination via physical post, sent electronically, sent for printing but no printed output retrieved etc. must be reported through Winn Group's Incident Reporting procedures.

Found Correspondence/Media

Data stored on any storage media or physically printed information which has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access (e.g. unlocked printouts, discarded CD (media)), must be reported through Winn Group's Incident Reporting procedures.

Loss or theft of IT/Information

Data or information which can no longer be located or accounted for (e.g. cannot be found in a location where it is expected to be, filing cabinet etc. or which is known/or suspected to have been stolen) needs to be reported immediately through Winn Group's Incident Reporting procedures.

6.1 Compliance With Legal & Contractual Obligations

GDPR & The Data Protection Act (2018) requires that personal data be kept secure against unauthorised access or disclosure.

Winn Group have a duty to report certain types of personal data breach to the relevant supervisory authority. This must be done by Winn Group within 72 hours of becoming aware of the breach.

The Computer Misuse Act (1990) covers unauthorised access to computer systems.

7.0 Breaches Of Policy

Breaches of this policy and/or security incidents are incidents which could result in an information security incident that cause loss or damage to Winn Group assets and confidential data or conduct which is in breach of the Group's security procedures and policies.

All Group employees, partner agencies, contractors, volunteers, stakeholders and vendors have a responsibility to report security incidents and breaches of this policy upon identification or if suspected by following the Group's Incident Reporting Procedure.

This obligation also extends to any external organisation contracted to support or access the Information Systems of the Group.

In the case of third-party vendors, volunteers, consultants or contractors, non-compliance could result in the immediate removal of access to the system or data. If damage or compromise of the Group's ICT systems, networks or data results from non-compliance with Winn Group policies and/ or procedures, the Group will consider legal action against the third party.

The Group will take appropriate measures to remedy any breach of this Policy through the relevant frameworks in place (including Risk Management and ISO27001:2013 ISMS). In the case of an employee, infringements will be investigated under the disciplinary procedure and progressed as appropriate.

This Policy is referenced by other Group policies and guidelines. Copies of these policy statements are obtainable via the Group's Intranet.

This Policy is maintained and reviewed by Winn Group's Information Security Officer and ratified by the Group's Information Governance Committee.

8.0 Responsibilities

8.1 All Staff

It is the responsibility for all Winn Group employees, partner agencies, contractors, volunteers, stakeholders and vendors who undertake work for the Group, on or off the premises, to be proactive in the reporting of security incidents. The Group's Incident Reporting procedures are in place to prevent and minimise the risk of damage to the integrity and security of Group data and information.

It is also a responsibility of all individuals and handlers of Group data and information to ensure that all policies and procedures dealing with the security and integrity of information and data are followed.

9.0 References

The following documents will provide additional information:

Doc Reference Number	Title
ISMS013	Encryption Policy
ISMS006	Clear Desk & Desktop Policy

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

Standard	Control	Description