WINNgroup

Access Control Policy

2.0

Author: David Office

Date Published: 02/09/2019

1.0 Version Control

Version:	2.0	**(Author) Issued By:**	David Office
Issued Date:	02/09/2019	**Review Date:**	19/04/2020
Document Owner:	Colette Gardner / Stuart Dent	**Document Number**	ISMS004

Approved By:	Chris Birkett	**Position:**	Chief Operating Officer
Signature:		**Approved Date:**	02/09/2019

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	01/10/2018	David Office	Initial Draft	New Policy
0.2	19/02/2019	David Office	Updated	ND Review amendments
1.0	19/02/2019	David Office	Approved	Approved by C. Birkett
1.0	19/02/2019	David Office	Released	Policy Released
1.0	19/04/2019	David Office	Review	Policy Reviewed. No Changes
1.0	19/04/2019	David Office	Released	Policy Released
1.1	02/09/2019	David Office	Updated	Updated Account deletion/retention timescales
2.0	02/09/2019	David Office	Approved	Approved by C. Birkett
2.0	02/09/2019	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

4.0 Introduction

Winn Group implements physical and logical access controls across its networks, IT Systems and service in order to provide authorised, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability in accordance with the Information Security Policy and ISO27001:2013 ISMS Standard.

5.0 Objectives, Aim & Scope

5.1 Objectives

The objective of this policy is to define how to limit access to information and information processing facilities, ensuring that only authorised users have access to information relevant to their role within Winn Group.

5.2 Aim

Access Control systems are in place to protect the interests of all authorised users of Winn Group IT systems by providing a safe, secure and accessible environment in which to work.

The aim of the Winn Group's Access Control policy is to preserve confidentiality, with access to data being confined to only those with the appropriate authority.

5.3 Scope

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

6.0 Policy Statement

6.1 Principles of Access Control

Where technically feasible, all Winn Group IT resources must be password protected.

Each IT system Winn Group utilises must have a designated system administrator(s) who is responsible for the day to day administration of the system including the creation and management of system access accounts for authorised users. Some information systems may be directly managed by the IT Department and IT Department staff may perform the role of system administrator.

The IT Department is the designated owner of all Winn Group network domains. Each Winn Group network domain must have a designated network administrator(s) who is responsible for the day to day administration of the network domain including the creation and management of network domain access accounts for authorised users.

Access to Winn Group IT Systems and networks must be strictly controlled by a formal written registration and de-registration process.

Access to Winn Group IT Systems must be controlled by the use of individual user access accounts. The use of generic or group access accounts to access Winn Group IT Systems strictly prohibited.

Maintaining Data Security Levels

Every user should understand the sensitivity of their data and treat it accordingly. Even if technical security mechanisms fail or are absent, every user should still attempt to maintain the security of data commensurate to their sensitivity. The Information Classification Policy enables users to classify data appropriately and gives guidance on how to store it, irrespective of security mechanisms that may or may not be in place.

6.2 Account Privileges

Access shall be granted using the principle of “Least Privilege”. This means establishing rules based on the premise “Everything is generally forbidden unless expressly permitted”. Authorised users will only be granted access to IT resources and network domains which are necessary for them to carry out the responsibilities of their Winn Group role or function.

Access rights and privileges to Winn Group IT resources and network domains must be allocated based on the specific requirement of a user’s role/function rather than on their status within the business.

Care must be taken to ensure that access privileges granted to users do not unknowingly or unnecessarily undermine essential segregation of duties.

Network Domain Access Accounts

Access to Winn Group network domains will be controlled using individual user access accounts. The use of generic/group access accounts is not permitted.

IT Systems Access Accounts

Access to Winn Group IT Systems will be controlled using individual user access accounts. The use of generic/group access accounts is not permitted under any circumstances on Winn Group IT Systems.

It must be noted that IT Systems may reside on-premise or a hosted service in the cloud.

Service Access Accounts

A service account is a special network domain access account that an application or service uses to interact with the operating system.

The creation of service access accounts (which in certain circumstances may include special privileges) must be rigorously restricted to the management or maintenance of the specific application.

Where there is a business requirement for the use of service accounts, these shall only be created following consultation and approval from the Winn Group Information Security Officer.

Privileged Accounts

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled and not provided by default.

Authorisation for the use of privileged accounts shall only be provided explicitly, upon written request from a Director of Winn Group, and will be documented by the system owner. System Administrators shall guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and/or integrity.

The creation of user access accounts with special privileges such as administrators must be rigorously controlled and restricted to only those users who are responsible for the management or maintenance of the information system or network.

Each administrator must have a specific admin level account, which is only used for system administrative purposes, and is kept separate from their standard user access account

Remote User Access

Access for remote users shall be subject to authorisation by a Department Head and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

7.0 Account Registration

All new requests for access to a Winn Group Network Domain and IT systems must be made in writing using the Winn Group New Starter Form and submitted to the HR Department.

System Administrators must only create new user accounts when they have received an HR department signed Winn Group New Starter form.

8.0 Account Management

Only authorised users shall have access to Networks and IT Systems. Access must be revoked when there is no longer a business reason for access.

Requests from users for password resets must only be performed once the user’s identity has been verified by the appropriate system administrator or network administrator.

Existing users who require additional access privileges on an information system must obtain the written authorisation of the designated information owner or his/her nominee. and forward this to the IT Department.

Existing users who require additional access privileges on a network domain (for example file shares etc.) must make their request in writing. Line managers must initiate the request by submitting a request to the IT helpdesk.

The access accounts of users taking career breaks, going on maternity leave or those on long term sick leave must be suspended until such a time as they return to work. Requests for account suspensions will be made from the HR Department by means of a helpdesk request.

The access accounts of users who are about to change roles or transfer to another Winn Group business or department, must be reviewed to ensure access account privileges that are no longer required by the user in their new role are removed. This will be done via a Staff Move Form, submitted by HR to the IT Helpdesk before the user changes role or transfers.

9.0 Account De-Registration

As soon as a user leaves the employment of Winn Group, all his/her information systems and network access accounts must be revoked immediately. The HR Department must request the deletion of a user's access accounts as soon as they have been informed by the user that they are leaving the employment of Winn Group. The requests must be made in writing using the Winn Group Staff Leaver Form and forwarded to the IT Department and the appropriate system administrator(s). The request should be made in advance of the users last day.

System administrators and network administrators must revoke user accounts at the requested date and time after the receipt of a properly completed Winn Group Staff Leaver Form.

10.0 Physical Access

Physical access across Winn Group buildings is controlled primarily via ID Card. Please refer to the ID Badge Policy for further information.

Physical Access shall only be granted on the authority of the Data/System Owner and shall be applied on a strict 'Required for Role' basis.

Network administrators and System administrators shall implement physical security measures in order to control Physical Access to data/systems, in addition to any physical access controls implemented for the buildings in which they are located.

Any unauthorised access must be reported to the Data Protection Team as a Security Incident.

11.0 Security

Access to all information systems and networks must be controlled via strong password authentication schemes. Further information can be found in the Winn Group Password Policy.

User access accounts must be created in such a way that the identity of each user can be established at all times during their usage. Each user access account must be unique and consist of at least a user name and password set.

Where possible Winn Group IT Systems and networks must be configured to:

- Force users to change their password at their first logon. Where this is not possible, users must be instructed to manually change their password, the first time they logon to a Winn Group IT System or network.
- Automatically lockout a user account after 5 consecutive failed login attempts.
- Automatically 'lock' or log out user accounts after 5 minutes of inactivity. Where this is not possible, users must manually log off or 'lock' their Winn Group computer device (using Ctrl+Alt+Delete keys) when they have to leave it unattended for any period of time. Computers must be logged out of and shutdown at the end of the each working day.

All passwords created must comply with the requirement of the Winn Group Password Policy.

When available audit logging and reporting must be enabled on all information systems and networks.

12.0 Monitoring & Review

Information owners or their nominees must continually monitor access to their information systems. They must perform quarterly reviews of the systems they are responsible for to ensure:

- That each user access account and the privileges assigned to that account are appropriate and relevant to that user's current role or function;
- That the information system and the information processed by the system is only accessed and used by authorised users for legitimate reasons.

System administrators and network administrators must conduct a system/network domain review at least once every quarter. User access accounts which have been inactive for 30 consecutive days or more must be suspended unless instructed otherwise by the user's line manager. Suspended user accounts which have not been reactivated within a 3 month period should be marked for deletion, unless instructed otherwise by the user's line manager.

Records of user access may be used to provide evidence for security incident investigations

13.0 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Winn Group assets, or an event which is in breach of the Group's security procedures and policies.

All employees, contractors, volunteers and vendors have a responsibility to report suspected and actual security incidents and breaches of this policy as quickly as possible through the Group's Security 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, consultants or contractors, non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Group's ICT systems or network results from the non-compliance, the Group will consider legal action against the third party. Winn Group will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an individual the matter may be dealt with under the disciplinary process.

14.0 Responsibilities

14.1 System Administrator

Each system administrator is responsible for:

- Taking appropriate and prompt action on receipt of requests for user registration, change of privileges, password resets and de-registration of users in accordance with this policy and the procedures for the information system;
- Taking appropriate and prompt action on receipt of requests for the suspension of a user account in accordance with this policy and the procedures for the information system;
- Ensuring all passwords generated for new user accounts and password resets meet the requirements of the Winn Group Password Policy;
- Notifying users of their system account details in a secure and confidential manner;
- Ensuring that appropriate records of system activity, including all authorised user registrations, change of privileges and de-registration requests are maintained and made available for review to the appropriate personnel;
- Conducting a monthly review of the information system they are responsible for, in accordance with this policy;
- Notifying the Data Protection Team if they suspect a user is responsible for misusing the information system or is in breach of this policy;
- Informing the Data Protection Team immediately in the event of a security incident involving the system;
- Complying with instructions issued by the Data Protection Team or IT Department.

14.2 Network Administrator

Each network administrator is responsible for:

- Taking appropriate and prompt action on receipt of requests for user registration, change of 'privileges', password resets and de-registration of users in accordance with this policy and the procedures for the network;
- Taking appropriate and prompt action on receipt of requests for the suspension of a user account in accordance with this policy and the procedures for the network;
- Ensuring all passwords generated for new user accounts and password resets meet the requirements of the Winn Group Password Policy;
- Notifying users of their system account details in a secure and confidential manner;
- Ensuring that appropriate records of system activity, including all authorised user registrations, change of 'privileges' and de-registration requests are maintained and made available for review to the appropriate personnel;
- Conducting a monthly review of the network they are responsible for, in accordance with this policy;
- Notifying the Data Protection Team if they suspect a user is responsible for misusing the network or is in breach of this policy;
- Informing the Data Protection Team immediately in the event of a security incident involving the system.
- Complying with instructions issued by the Data Protection Team.

14.3 IT Department

The IT Department is responsible for:

- The management, control, ownership, security and integrity of all Winn Group network domains (LAN/WAN) on behalf of the Group;
- Ensuring adequate procedures are in place to ensure compliance with this policy and all other relevant policies;
- Designating a network administrator(s) for each Winn Group network domain;
- Conducting a quarterly review of the networks in accordance with this policy;
- Providing the Data Protection Team with quarterly audit reports and user access lists for information systems which are directly managed by the IT Department.

14.4 Line Managers

Each Line Manager is responsible for:

- Ensuring complete and timely IT systems and network access requests, for both permanent and temporary staff, are forwarded to the HR Department, allowing sufficient time for the creation of the required user account prior to the users start date;
- Ensuring that each user they request access for meets all the criteria for the requested information system and/or network (principle of “least privilege”);
- Ensuring they make timely requests for the suspension of all user accounts belonging to members of their staff who are taking a career break, going on maternity leave or those on long term sick leave;
- Ensuring they make timely requests for the deletion of all user accounts belonging to members of their staff who are leaving the employment of Winn Group;
- Consulting with the Data Protection Team in relation to the appropriate procedures to follow when a breach of this policy has occurred.

14.5 All Users

Each user is responsible for:

- Respecting and protecting the privacy and confidentiality of the information systems and network they access, and the information processed by those systems or networks;
- Ensuring they only use user access accounts and passwords which have been assigned to them;
- Ensuring all passwords assigned to them are always kept confidential and not shared with others including their co-workers or third parties;
- Changing their passwords at least every 180 days or when instructed to do so by designated system administrators, network administrators or the IT Department;
- Complying with instructions issued by designated system administrators, network administrators, Data Protection Team and/or the IT Department on behalf of Winn Group;
- Reporting all misuse and suspected breaches of this policy to their line manager.

15.0 References

The following documents will provide additional information:

Doc Reference Number	Title
ISMS005	Password Policy
ISMS026	Teleworker Policy
SM041	ID Badge Policy
ISMS007	Information Classification & Handling Policy
ISMS001	Information Security Policy
ISMS002	Information Security Incident Policy

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

Standard	Control	Description