Westerly Owners' Association

WESTERLY OWNERS' ASSOCIATION INFORMATION SECURITY POLICY

By
Robert Walker CEng, MIET, Rear Commodore WOA

PUBLICATION REFERENCE:	WOA POL_2301 Version: 01
DOCUMENT NAME:	Information Security Policy
AUTHOR:	Robert Walker CEng MIET
PUBLICATION DATE:	29 March 2023
TARGET AUDIENCE:	All Westerly Association Members
ADDITIONAL CIRCULATION LIST:	Nil
DESCRIPTION:	Policy and high-level procedures for information security
SUPERSEDED DOCUMENTS:	Draft A
CONTACT DETAILS:	admin@westerly-owners.co.uk

DOCUMENT RELEASE:

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.

DOCUMENT STATUS:

Document Number: WOA POL_2301	Issue Date: 29 March 2023	Version Number: v01
Status: Approved	Next Review Date: 29 March 2024	Approved By: Gill Clare Commodore Westerly Owners Association
Approval Date:		Signature:

TABLE OF AMENDMENTS

Version	Date	Amendment	Originator	Approved By
Draft A	29 Mar 2023	Original	R Walker	G Clare, Commodore
V01	25 Jul 2023	Final – Roles & Responsibility updated	R Walker	G Clare, Commodore
V02	30 Jul 2023	SIAO, SIRO update	R Walker	
V02.1	30 Aug 2023	SIAO Responsibilities	R Walker	G Clare, Commodore

TABLE OF CONTENTS

List of Figures

List of Annexes

Annex C: *List of Acronyms*

1. INTRODUCTION

1.1 Background

1.1.1 The Westerly Owners Association (WOA) hereafter referred to as the Association, is an organisation with information processing as a fundamental part of its purpose and is bound by the Data Protection Act 2018. This is the UK's implementation of the General Data Protection Regulation (GDPR) and everyone responsible for using personal data must follow strict rules called 'data protection principles.'

1.1.2 It is important, therefore, that the Association has a clear and relevant Information Security Policy to establish and maintain its data protection principle. This is essential to our compliance with data protection and other legislation and to ensuring that confidentiality is respected.

1.1.3 The purpose of the Association'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 more crucially it encompasses the behaviour of the people who manage information in the line of Association business.

1.1.4 Information security is about peoples' behaviour in relation to the information they are responsible for, 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 corporate way.
- Assurance that the Association 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 Association business.
- A strengthened position in the event of any legal action that is taken against the Association (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security cognisant with a small non-profit organisation.
- Assurance that information is accessible only to those authorised to have access. Assurance that risks are identified, and appropriate controls are implemented and documented.

1.1.5 An *Information Security Risk Assessment* was completed in February 2023 [Ref: 1] spanning the Association's Information Assets. The results were published in a white paper, *Westerly Owners Association Information Assurance* [Ref:2].

1.1.6 This policy has been developed in response to a key recommendation detailed in Ref 2.

1.2 Objective

1.2.1 The objective of the Association's Information Security Policy is to preserve:

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

1.3 Aims

1.3.1 The aims of this policy are to establish and maintain the security and confidentiality of information, information systems, applications, and networks by:

- Ensuring that all members 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 are implemented in the Association. Introducing a consistent approach to security, ensuring that all members fully understand their own responsibilities.
- Creating and maintaining within the Association 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.
- Provide members with IA awareness and guidance to secure data where the use of Portable Electronic Devices (PEDs) are used, sometimes referred to as 'Bring Your Own Device' (BYOD) [Ref 3].

2 SCOPE

2.1 Users

2.1.1 The following users of personal data are within scope of this document:

- All Association committee members including the Flag Officers.
- All Area Group (AG) committee members and associated clusters.
- Any member entrusted by an Association committee member or AG committee member to hold or process such data to complete a task on behalf of the Association.

2.2 IT Infrastructure

2.2.1 The scope shall cover the whole of the IT infrastructure used to perform the association's business. The boundary of the scope is defined in terms of the business needs and being able to manage it. Figure 1 below illustrates a typical scope and its boundary which is akin to the association.

3 ROLES & RESPONSIBILITIES

3.1 Commodore

3.1.1 Responsibility for information security resides with the Commodore. This responsibility is discharged through the designated roles of Senior Information Risk Owner (SIRO) and Senior Information Asset Owner (SIAO).

3.2 Senior Information Risk Owner (SIRO)

3.2.1 The Senior Information Risk Owner (SIRO) is responsible for information risk within the Association and advises the Commodore and Association committee on the effectiveness of information risk management across the organisation.

3.2.2 The SIRO shall report directly to the Commodore (See Figure 2) and advise upon:

- Information Security matters.
- Resilience (Disaster Recovery).
- Training.
- National Cyber Security Measures.
- Strategic Planning.

3.2.3 The SIRO is responsible for the long-term strategy to ensure security of their physical environments where information is processed or stored. Furthermore, they are responsible for:

- Ensuring that all users are aware of the information security policies, procedures, and user obligations applicable to their area of work.
- Ensuring that all users are aware of their personal responsibilities for information security.

3.2.4 Cyber Security; the SIRO is responsible for developing, implementing, and enforcing suitable and relevant information security procedures and protocols to ensure the Association information assets remain compliant with the Data Protection Act 2018.

3.2.5 The role of the SIRO should be appointed to the Association committee.

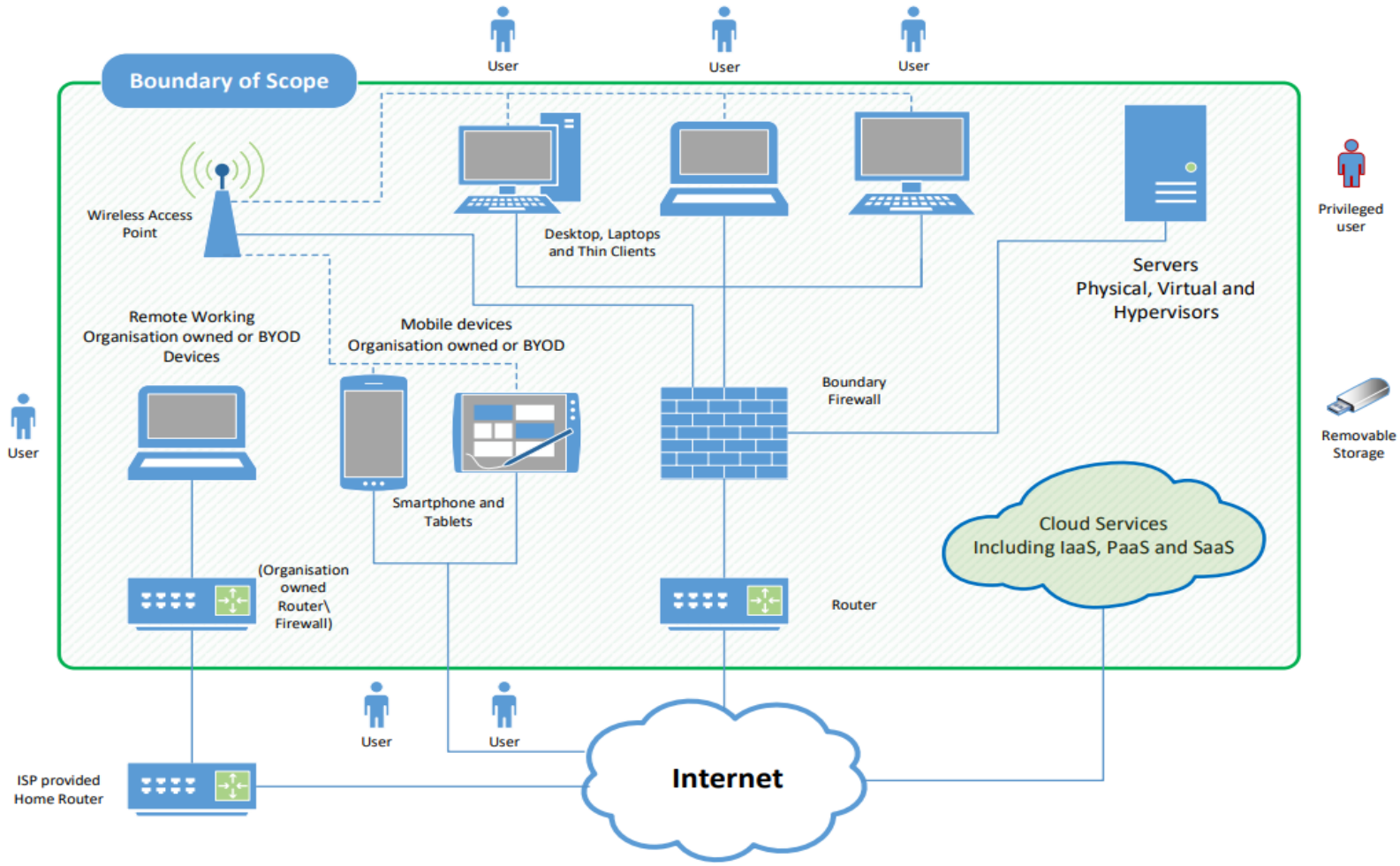

Figure 1: *IT Infrastructure Boundary (Courtesy of the National Cyber Security Centre)*

3.3 Senior Information Asset Owner (SIAO)

3.3.1 The SIAO is responsible for:

- The day-to-day information security, providing advice, monitoring compliance, and is the first point of contact in the organisation for data protection matters. The SIAO reports to the Commodore and works with the SIRO to deliver the strategy, policies, and procedures. See Figure 2.
- The SIAO will liaise directly with Information Asset Owners in each AG and they shall report directly to the SIAO.
- The SIAO is responsible for ensuring that third party data processors have appropriate ISO and/ or Cyber Essentials accreditation where appropriate for assets stored electronically with third parties.
- In collaboration with the SIRO, determine the level of access to be granted to specific individuals/users and thereafter to manage and control access permissions.
- Ensuring staff have appropriate training for the systems they are using.
- Ensuring staff know how to access advice on information security matters.

3.4 Information Asset Owner (IAO)

3.4.1 Each AG committee will appoint a member within their respective AG to take on the role and responsibility of an IAO.

3.4.2 Each IAO will report to their respective committees and the SIAO. See Figure 2.

3.4.3 Each IAO is also responsible for ensuring appropriate data protection assurance from all users processing personal data. This is specific to PEDS/BYOD.

3.5 All Users (Members)

3.5.1 All users are responsible for information security and therefore must understand and comply with this policy and associated guidance. All users should undertake an annual Data Security Awareness workshop provided by the SIRO and understand:

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

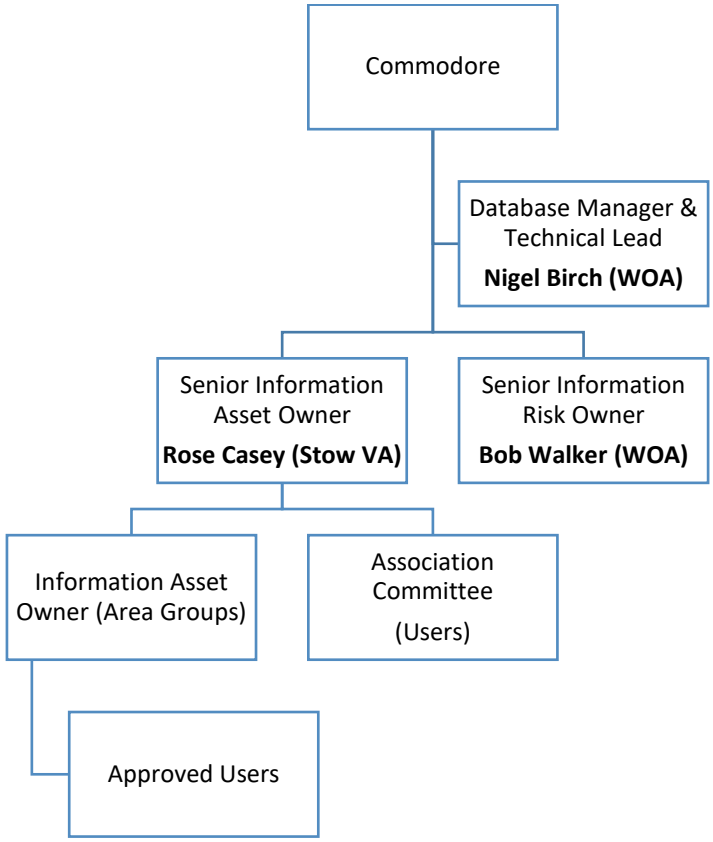

Figure 2: *WOA Information Security Hierarchy*

4 POLICY FRAMEWORK

4.1 Access Controls

4.1.1 Access to personal information shall be restricted to users who have an authorised need to access the information and as approved by the relevant IAO.

4.2 IT Network Controls

4.2.1 Access to data, systems utilities and programme source libraries including plugins shall be controlled and restricted to those with a higher level of legitimate requirements e.g., systems or database administrators and database managers. Authorisation to use an application shall be strictly approved and controlled by the SIAO.

4.3 IT Equipment Security

4.3.1 In order to minimise loss of, or damage to all assets which will be those categorised as PEDs and BYOD, asset owners/users will be reminded during the annual Data Security Awareness workshop of their obligation to physically protect their devices from damage, threats, and environmental hazards.

4.3.2 Users will also be made aware of the potential damage which malware can cause which threatens the information security of not just their own device but also the central database through the transfer of the virus across the network.

4.3.3 To preserve network security, the SIAO will be responsible for controlling access and ensuring the cloud-based platform provider is maintaining the appropriate levels of security protocols.

4.3.4 The Data Security Awareness workshops shall be used to remind users of their obligation to minimise the risk from malicious software by ensuring that their devices are kept up to date with operating systems software patches when they become available for download, and they also operate a suitable anti-virus software application on their device.

4.4 Information Risk Assessment

4.4.1 IAO's shall ensure that information risk assessments are performed at least annually, following guidance from the Senior Information Risk Owner (SIRO). IAO's shall submit the risk assessment results and associated mitigation plans to the SIRO for review.

4.5 Business Continuity and Disaster Recovery Plans

4.5.1 The Association will implement a business continuity management system (BCMS) that will be aligned to the international standard of best practice (ISO 22301:2012 – Societal security – Business continuity management systems - Requirements).

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

4.5.3 The SIRO 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 evaluated on a regular basis.

4.6 Information Security Awareness

4.6.1 The SIRO assisted by the SIAO shall annually hold a Working Group to appraise all users of:

- The latest changes to the Information Security Strategy.
- Current threats.
- Rollout of new applications.
- Best practice for BYOD.
- Cyber Essentials.

4.7 Communication

4.7.1 Breaches or known potential breaches to Information Security shall be reported immediately via the IAO's to the SIAO. The SIAO will take immediate action to mitigate the risk and inform the SIRO and Commodore of the event.

4.8 Classification of Information

4.8.1 Information classification is not always obvious, but this is key to determining the sensitivity of the information and therefore, where it is kept and who has access to it. It can also be the case that two separate pieces of information may be regarded as non-sensitive but the aggregation of information by combining them could make it sensitive.

4.8.2 A flowchart to help decide on the classification or sensitivity of information is at ANNEX A to this policy document.

Information Classification Flowchart

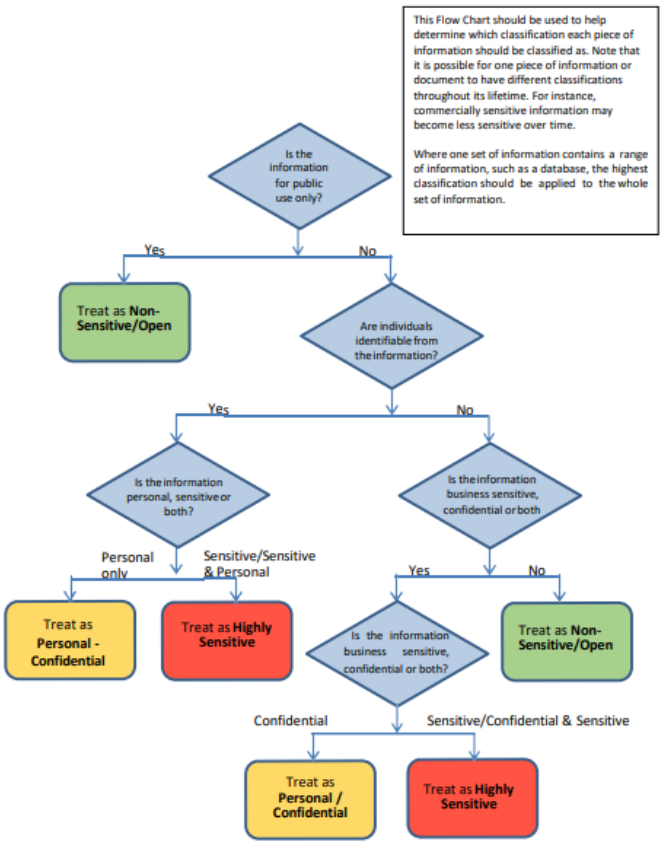

Figure 3: *Information Classification Flow Chart*

ANNEX B TO
INFORMATION SECURITY POL_2301
DATED 29 MARCH 2023

List of References

1. WOA Information Security Risk Assessment by Robert Walker dated February 2023.
2. Westerly Owners Association Information Assurance by Robert Walker dated 27 February 2023.
3. Cyber Essentials: Requirements for IT Infrastructures Version 3 – National Cyber Security Centre Dated Nov 2021.

ANNEX C TO
INFORMATION SECURITY POL_2301
DATED 29 MARCH 2023

List of Acronyms

AG	Area Group
BCMS	Business Continuity Management System
BS	British Standard
BYOD	Bring Your Own Device
GDPR	General Data Protection Regulation
IAO	Information Asset Owner
IaaS	Infrastructure as a Service
IS	Information Security
ISO	International Standards Organisation
IT	Information Technology
NCSC	National Cyber Security Centre
PEDs	Portable Electronic Devices
PaaS	Platform as a Service
SaaS	Software as a Service
SIAO	Senior Information Asset Owner
SIRO	Senior Information Risk Owner
WOA	Westerly Owners Association