	Royal British Legion Industries Information Security Policy	Effective Date	30 April 2010
	Policy Title	Review Date	Aug 2020
	Clear Desk Policy	Review by	Kate Porter

1. Purpose

The purpose of this document is to describe the Company's requirements for a "clear desk" policy that will support and strengthen RBLI's overall data security procedures. Anyone with access to RBLI's information must be made aware of the expectations about the use and care of that information.

2. Scope

- 2.1. All staff, employees and entities working on behalf of RBLI are subject to this policy, regardless of location.
- 2.2. When third party organizations are contracted to undertake work for or on behalf of RBLI, care should be taken to ensure that the requirements for confidentiality and data security are embodied in any documentation, whether formal or informal, that relates to the working arrangement.
- 2.3. An effective clear desk effort involving the participation and support of **ALL** RBLI's employees and appointed agents can protect paper documents and electronic media that contain sensitive information about customers, clients, vendors and business operations.

3. Overview

- 3.1. All staff are responsible for the security of information in their control. During absences from the work place, no matter where it is located, staff must ensure that information is secured appropriately. This is known as the "clear desk" policy.
- 3.2. At the close of business each day, staff must take precautions to ensure that information, particularly if subject to a security classification, is protected from unauthorized access.

4. General guidelines

The following principles should be observed by all staff as part of an effective lock-up procedure that underpins this clean desk policy.

- 4.1. Log off all computer systems in the correct manner, preferably with a complete shutdown of workstations where practicable.
- 4.2. If you leave your workstation unattended you must lock it.

- 4.3. Ensure that there are no security-classified documents left in the workplace, paying particular attention to shared network printers, documents that may be in a print queue awaiting printing and output as a hard-copy document.
- 4.4. Ensure that no classified information has been placed in waste paper bins.
- 4.5. Shred all unwanted work-related papers.
- 4.6. Ensure that all white boards, flip charts and other displays do not show any confidential information. Special care must be taken with electronic whiteboards due to the number of panels that can be used and the ease with which these can be copied.
- 4.7. Ensure that all cabinets, safes and containers that house confidential information are locked and that keys to these are not left where they may be misappropriated.
- 4.8. Ensure that all doors that can be secured are properly locked.
- 4.9. The codes to doors that are secured through access controls must not be written down and left where they are accessible. Such codes are not to be revealed to unauthorized persons.
- 4.10. Keys to key safes must be securely stored in designated places, and released only to authorized persons. Under no circumstances are duplicate keys to be made without the written authority of an RBLI director.
- 4.11. If in doubt – throw it out! If unsure as to whether a duplicate piece of sensitive documentation should be kept it should be shredded.
- 4.12. The use of scanning paper items for storage in an electronic system should be considered.

5. Specific guidelines for IT users

- 5.1. The clear desk policy also relates to absences from computer workstations, whether desktop or laptop. It is mandatory that all IT users ensure their workstations are protected from unauthorized access to any electronic system or network to which they have been connected. For extended periods, this would entail logging off. For shorter periods, locking the workstation requiring the user to enter a password for reconnection would be adequate.
- 5.2. A “lock workstation” feature is employed on all of RBLI’s equipment whether it is linked to the organization’s networks or standalone. This will ensure that individual computers will automatically go into “locked” mode after 5 minutes of idle time. However, this is not fail safe as unauthorized access could occur between the start of a period of inactivity and the point at which the lock-out commences.
- 5.3. Users are advised that they **MUST** lock their workstations using the CTRL+ALT+DELETE keys and selecting the “Lock Workstation” option when leaving the workstation for any reason. This is mandatory where the user is working on security classified information which otherwise might remain displayed on the computer’s screen in the user’s absence.
- 5.4. RBLI may provide laptop computers for some staff on a permanent basis. Other users may access laptop computers for work purposes from a loan pool. The standard user configuration for laptop

computers includes the automatic “Lock Workstation” feature which activates after 5 minutes of idle time. It is expressly forbidden for any staff member to alter this or any other laptop default settings that have been incorporated to provide security for such equipment.

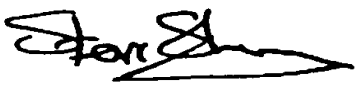


- 5.5. Users are responsible for ensuring that laptop computers used to create, process or store security classified information are afforded the level of protection commensurate with the highest level of security classification for information stored on the equipment. This is particularly important for laptops used away from RBLI’s secured premises.
- 5.6. Individual business units should establish appropriate close-of-business procedures for the checking of workstations and work areas to ensure that all confidential information, whether paper or electronic-based, is secured at the end of each working day.
- 5.7. The above guidelines also apply to portable data storage devices, such as CDs, DVDs, USB memory sticks, portable hard drives. Because of their small size and ease of transport, they should be locked away securely when not in use.
- 5.8. All portable computing devices should be locked away when not in use.

6. General Responsibilities

- 6.1. In the event of any loss or suspected loss of confidential information or data, it is the user’s responsibility to report the breach or suspected breach as laid down in RBLI’s Security Incident Reporting policy and procedure.
- 6.2. Similarly, should unauthorized access to a workstation be evident or suspected, it is the authorized user’s responsibility to report this as laid down in RBLI’s Information Security Incident Management policy and procedure.

7. Enforcement

- 7.1. Regular spot checks are to be carried out by Heads of Departments to ensure that this policy is adhered to. Breaches or suspected breaches must be recorded and reported to the Head of Business Systems.
- 7.2. Failure to adhere to this policy will be considered a breach of RBLI’s security policies and may be subject to appropriate disciplinary action & access to systems may be withdrawn.

Approved by :		
 Steve Sherry – Chief Executive	 Philip Defraigne – Director of Finance & Corporate Services	 Kate Porter – Head of Business Systems