 RBLI	Royal British Legion Industries Information Security Policy	Effective Date	1st October 2010
Policy Title		Review Date	Aug 2020
Information Security Incident Management		Authored by	Mike Smith
		Reviewed By	Kate Porter
Purpose			
<p>The purpose of this document is to specify the policy that regulates how RBLI shall respond to information security incidents, and how the organisation shall learn from these and design and implement improvements.</p>			
Scope			
<p>This policy is applicable to all aspects of RBLI’s operations, whether electronic, hard-copy documentation or reports, personnel, premises or infrastructure. It also includes landline and mobile telecommunications, Web-based activity, social media and any medium by which RBLI and its employees use, present, publish, modify and store data and information that relates to the organisation’s business activities whether past, present or future.</p>			

Breaches or Suspected information security incidents

Breaches of information security or suspected breaches of information shall be reported without delay to the Head of Business Systems to speed the identification of any damage caused, any restoration and repair actions required, and to facilitate the gathering of associated evidence.

Reporting to outside authorities

Procedures and guidelines shall be implemented that specify when, and by whom, the authorities, regulatory and enforcement agencies are to be notified of serious information security incidents. Notification at this level shall be a matter to be considered and actioned by the Executive Team. Information security incidents shall be reported to outside authorities whenever this is required to comply with legal requirements or regulations. This may only be done by authorised persons. Refer to Data Breach Procedure document which defines how breaches should be reported.

Notifying information security weaknesses

All identified or suspected information security weaknesses shall be notified immediately to the Head of Business Systems.

Being alert for fraudulent activities

Employees shall be expected to remain vigilant for possible fraudulent activities.

Software errors and weaknesses

Any discovered or perceived software errors or suspected systems weaknesses shall be reported immediately to the system owner and to the Head of Business Systems.

Detecting electronic eavesdropping and espionage activities

Where a risk assessment has identified an abnormally high risk from the threat of electronic eavesdropping and/or espionage activities, all employees shall be alerted and reminded of the specific threats and the specific safeguards to be employed.

Recording information security breaches

Evidence relating to a suspected information security breach shall be formally recorded and processed.

Responsibilities for managing information security incidents

Information security incidents shall be properly investigated by suitably trained and qualified personnel. Where necessary, the Executive Team will assign one or more managers or staff to assist the Head of Business Systems in arranging and/or carrying out the investigation. Should external expertise and resources be required to carry out a full investigation, the Executive Team shall assess this based on recommendation from the Head of Business Systems.

Segregation of duties when investigating information security incidents

During the investigation of information security incidents, the segregation of duties shall be addressed in the procedures to strengthen the integrity of information and data, and to ensure that a cohesive approach to the investigation takes place.

Responding to information security incidents

The Head of Business Systems shall respond rapidly but calmly to all information security incidents, liaising and coordinating with colleagues to both gather information and offer advice.

Monitoring confidentiality of information security incidents

Information relating to information security incidents shall only be released by authorised persons.

Using information security incident checklists

Staff shall be supported by management in any reasonable request for assistance, together with practical tools, such as security incident checklists etc., in order to respond promptly and effectively to an information security incident.

Maintaining a register of information security breaches




A register of information security breaches and remedial actions shall be created and maintained. This shall be regularly reviewed, together with any anecdotal evidence used, to help reduce the risk and frequency of information security incidents within RBLI.

Analysing information security incidents resulting from system failures

Information security incidents arising from system failures shall be investigated by appropriately qualified and skilled persons. The outcomes will be reported to the relevant vendors or developers, and explanations obtained together with confirmation of any further preventative actions that RBLI’s technical team may need to put in place.

Ensuring the integrity of information security incident investigations

The use of information systems shall be monitored regularly with all unexpected events recorded and investigated. Such systems shall also be periodically audited and the results recorded in such a way that future investigations can be cross-referenced to similar events.

Approved by :		
Head of Business Systems 	Director of Corporate Services 	Chief Executive 
Date: 1 st Nov 2016	Date: 1 st Nov 2016	Date: 1 st Nov 2016