| | | | |
|---|---|---|---|
| RBLI | Royal British Legion Industries<br>Information Security Policy | Authored By | Michael J Smith |
| | | Effective date | 1st January 2010 |
| | | Version date | Aug 2020 |
| Information Classification | | To review by | Aug 2021 |
| | | Reviewed By | Kate Porter |

## Purpose

This policy describes RBLI's policy on the classification of information assets held and maintained across the company. It is part of the overall policies, procedures and guidelines that document RBLI's Information Security Management Systems (ISMS) and related matters.

## Scope

- All staff, employees and entities working on behalf of RBLI are subject to these guidelines, regardless of location, if they have a username and password to at least one RBLI system or application, regardless of whether an end user or a system administrator for that system or application.
- When third party organisations are contracted to undertake work for or on behalf of RBLI, they shall be required to adhere to these guidelines.

## Consequences of non-compliance

- Failure to comply with this Policy will significantly increase the risk of confidential, personal and sensitive data being exposed to unauthorised access, theft and malicious damage.
- If information is not properly classified and protected, there is a risk of RBLI breaching the requirements of the General Data Protection Regulation and the Data Protection Act 2018
- Staff failing to adhere to these guidelines could be liable to disciplinary procedures or other sanctions, in accordance with RBLI's various HR policies and Terms and Conditions of Employment.

## Additional background

- Information of different types need to be secured in different ways. Therefore, a classification system is required that categorises information according to its value and sensitivity, allowing security mechanisms to be devised and applied based on the classification given to individual information assets.
- The General Data Protection Regulation sets out how organisations may use personal data.

## Procedural guidelines

1. There are several concepts that characterise the classification of information. These are –
   - All data and information has an owner

   The data, information or process owner must -

- Classify the information into one of the security categories adopted, depending on legal obligations, costs, corporate information policy and business needs.
- The owner should determine who is allowed access to the data.
- The owner is responsible for the data and must ensure that it is secured according to its classification.
- All documents should be classified and the classification level should be marked on at least the title page.

2. Once data on a system has been classified into one of the following four levels, that system should be configured to conform to all security requirements for that classification, and those classifications below it. For example, if a system is classified as Class 3 then the systems must follow the directives of Class 1, Class 2 and Class 3.

3. If a system contains data of more than one sensitivity class, it must be classified according to that needed for the most confidential data held on the system

4. The following are the classifications to be used –

- **Class 1 – Public and non-classified information**
  Data at this level could be made public without any implications for RBLI – i.e. the data is not confidential. Data integrity is not vital and loss of service due to malicious attacks on the system is an acceptable risk.
  ***Examples*** *are test services without confidential data, certain public information services, product brochures that might normally be widely distributed and data that is generally in the public domain anyway.*

- **Class 2 – Internal information**
  External access to this classification of data is to be prevented, but the consequences of this data becoming public would not be considered as critical – e.g. RBLI could be embarrassed but business would not suffer unduly. Data integrity is important but not vital.
  ***Examples*** *of this type of data could be data used in development environments where no "live" data is present, some customer data, telephone lists, day-to-day working documents, project meeting minutes and associated papers.*

- **Class 3 – Confidential information**
  Data in this category is confidential within RBLI and is to be protected from external access. If such data were to be accessed by unauthorised persons it could influence RBLI's operational effectiveness, lead to financial loss, provide a significant gain to a competitor or cause a loss of customer confidence. Data integrity is vital.
  ***Examples*** *are data held at datacentres (e.g. Sota), salaries, personnel data, accounting data and reports, information on systems configuration, details of security weaknesses, very confidential customer data and confidential contracts.*

- **Class 4 – Restricted information**
  Unauthorised external OR internal access to this data would be critical to RBLI, and the number of people with access to it should be limited on a "need to know" basis. Data integrity is vital and very strict rules should be applied and adhered to in the usage of this data.
  ***Examples*** *are secret contracts, information relating to dealings with government agencies or the armed services.*

**5. Marking of data classifications**

- Once the data or information owner has set the classification level, this should be clearly marked in the top-right header of printed documents.
- For electronic data or information stored in electronic format, the access rights for users must be established through the use of groups. This procedure will be maintained and managed by a designated person acting on behalf of the data or information owner and it will be this person's responsibility to ensure that users are allocated to a particular user group that does not allow access to information classified higher than the user is permitted to view.
- Data or information owners shall be responsible for carrying out periodic checks to ensure that the correct classifications have been applied, and that access to folders, files, documents etc. is in accordance with the privileges assigned to individual users.

## General responsibilities

- The above guidelines are applicable and relevant to ALL authorised users of RBLI's information systems.
- Only authorised staff may set up new directories, access rights, folders and file naming conventions. These are to be strictly adhered to by all users.
- All users will be responsible for the proper handling of data and information according to the classification levels assigned in terms of this Policy.

## Monitoring and compliance

- Regular spot checks are to be carried out by local management to ensure that these guidelines are adhered to. Breaches or suspected breaches must be recorded and reported in accordance with RBLI's Security Incident Reporting procedures.
- Failure to adhere to this Policy will be considered a breach of RBLI's security policies and may be subject to appropriate disciplinary action.

## References and appendices

- None

**Approved By:**

Philip Defraine

**Date:**