1. **Scope**

This plan applies to all information security management system planning in Retirement Capital and will be conducted in line with [MSS DOC 4.1](../Section%204%20-%20context%20of%20organisation/MSS_DOC_4.1.docx).

1. **Responsibilities**
   1. The Information Security Manager is responsible for identifying information security management system risks, and for the development, testing and maintenance of plans to manage those risks.
   2. The Operations Director is responsible for managing business continuity on a day-to-day basis and is also responsible for carrying out the risk assessments on which information security management system planning depends.
   3. The Information Security Manager is responsible for ensuring that all information security issues have been included and appropriately treated in these information security management system plans.
   4. The Department Manager is responsible for key processes are also responsible for identifying and implementing the steps necessary for their continuity.
   5. The Managing Director is responsible for insurance, financial, accounting and legal aspects of the information security management system plans.
   6. The Chief Information Security Officer is responsible for including information security management system responsibilities (where appropriate) in job descriptions.
2. **Information security management system plan**
   1. Identify business interfaces:  
      Each of the critical outward and inward facing business activity or services within the scope of the information security management system is identified and listed, in order of criticality.
   2. Identify key processes:  
      The key processes (including supplier services) in each activity, together with the key resources required for normal operations, as well as the Manager of the process, are identified next and the data is added to record.
   3. Identify assets:   
      The critical assets that are involved in each process are identified and cross-referenced to the asset register.
   4. Identify objectives:  
      Retirement Capital identifies objectives for the information security management system that will be used to determine the efficacy of the implementation during the management reviews ([MSS DOC 9.3](../Section%209%20-%20performance%20evaluation/MSS_DOC_9.3.docx)).
   5. Define and apply risk assessment process  
      Board of Directors approve a methodology for risk assessment which defines Retirement Capital’s approach to identifying risk, the scales to be used for calculating and analysing risks, and the levels of risk that are acceptable within this analysis [RM-ISMS DOC 6.1.2](RM-ISMS_DOC_6.1.2.docx). This will be performed internally through a meeting of all departmental managers.
   6. Create risk treatment plan  
      On the basis of the risk assessment process outcomes, and the determined acceptance levels, create a risk treatment plan.
   7. Implement risk treatment   
      Board of Directors to provide resources and allocate responsibilities for implementing actions to treat risks, including incorporating activities into business processes.
   8. Monitor effectiveness of risk treatment  
      Board of Directors to identify objectives against which the effectiveness of risk treatment will be measured.
   9. Manage incidents  
      The Director (CISO) works with the process owners to devise incident management and information security management system plans (using the standard templates) that follow the information security management system strategy to ensure that any disruptions are mitigated in a way that ensures recovery of the service, process or control within an acceptable timeframe.
   10. Audit  
       Lead Auditor implements and audit programme to monitor compliance with the requirements of the information security management system.
   11. Continuous improvement  
       Non-conformities, incidents and performance analysis will form the basis of improvements to the information security management system, on the basis of individual items and through the management review.

**Document Owner and Approval**

The Director (CISO) is the of this owner document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

The current version of this document is available to all members of staff on the corporate intranet.

This document is approved by the Board of Directors on the issue date shown and is issued on a version-controlled basis under his/her signature.

Signature: Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |