INFORMATION SECURITY POLICY

The Board and senior management of ProCo, which operates in the areas of Printing and Direct Mail Services, supported by online Web-to-Print & Campaign Management applications and Storage and Distribution facilities, are committed to preserving the Confidentiality, Integrity and Availability of all the physical and electronic information assets throughout the organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information security requirements shall continue to be aligned with Organisational goals and the ISMS is intended to be an enabling mechanism for information sharing, electronic operations, e-commerce and reducing information-related risks to acceptable levels.

The Organisation's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of the ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. The Information Security Manager is responsible for the management and maintenance of the Risk Treatment Plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data back-up procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Manual and are supported by specific, documented policies and procedures.

All employees of the Organisation and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy. All staff, and certain external parties, will receive appropriate training.

The organisation has set Information Security Objectives which have been made as a result of business requirements, customer requirements and as a result of the risk assessment.

The ISMS is subject to continuous, systematic review and improvement.

The Organisation has established an Information Security Management System Team chaired by the Information Security Manager which includes other key staff to support the ISMS framework and to periodically review the security policy.

The Organisation's information Security Policy is reviewed at planned intervals, or when and if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness.

In this policy, "information security" is defined as:

Preserving
This means that management, all full time or part time staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in the Organisation's disciplinary policy. All staff shall receive information security awareness training and more specialised staff shall receive appropriately specialised information security training.

the availability,
This means that information and associated assets shall be accessible to authorised users when required and shall therefore be physically secure. The computer network shall be resilient and the Organisation be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There are appropriate business continuity plans.

confidentiality
This involves ensuring that information is only accessible to those authorised to access it, thereby preventing both deliberate and accidental unauthorised access to the Organisation's information and proprietary knowledge and its systems, including its network(s), website(s), extranet(s), and e-commerce systems.

There are four levels of classification to facilitate this:

- **Private** (includes): Board members, Senior management team, finance team, etc
- **Restricted** (includes): "need to know" information, Job Store, customer data, etc
- **Confidential** (includes): all information assets, such as Proco policies & procedures, etc
- **Public** (includes): information security policy, Proco website, Proco social media sites, etc

and **integrity**
This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorised modification, of either physical assets or electronic data. There shall be appropriate contingency including for network(s), e-commerce system(s), web site(s), extranet(s) and data back-up plans, and security incident reporting. The Organisation shall comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the **physical (assets)**
The physical assets of the Organisation, including but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

and **information assets**
The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, web site(s), extranet(s), intranet(s), PCs, laptops, mobile phones and tablet devices as well as on CD / DVD, USB sticks and any other digital or magnetic media, and information transmitted electronically by any means. In this context "data" also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

of the **Organisation**
the Organisation and such partners that are part of our integrated network and have signed up to our security policy and have accepted our ISMS.

The **ISMS** is the Information Security Management System, of which this policy, the Information Security Manual ("the Manual") and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO27001:2013.

A **SECURITY BREACH** is any incident or activity that causes or may cause a break down in the confidentiality, integrity or availability of the physical or electronic information assets of the Organisation.