



## Panoram Information Security Policy

Through this Security Policy Panoram Digital has defined its commitment to protecting information through the Information Security Management System (ISMS) which ensures confidentiality, integrity, security, and availability of internal, customer and supplier information.

The ISMS effectiveness is achieved through understanding the risks and opportunities that may impact information within the business and by using a number of controls, including policies, processes, procedures, software, and hardware functions to manage these issues in ways that are beneficial to the business.

These controls are continually monitored, reviewed, and improved to ensure that specific security and business objectives are met. This is operated in conjunction with other business management processes and incorporates the applicable statutory and contractual requirements.

Objectives have been defined primarily through the SWOT and PESTLEE, although some may come from the information security risk assessment and the Management Review. They are designed to drive the management system forward and bring about continual improvement. Objectives will be focused on improving confidentiality, integrity, and availability.

The Information Security Management system has been designed to address legislation as listed in the legal register. Information Security is controlled through the preservation of:

- **Confidentiality:** ensuring that information is accessible only to those authorised to have access;
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods;
- **Availability:** ensuring that authorised users have access to information and associated assets.

The company operates a programme of information security awareness and compliance through company inductions, training, management reviews and internal audits. All employees are empowered to identify any potential security weaknesses and/or events which could be Information Security Incidents and report through the appropriate management channels.


A robust system is in place to continually improve the security controls by:

- Taking account of changes to business requirements and priorities
- Considering new threat and vulnerabilities which may impact the business
- Reviewing the effectiveness of the Management System through Internal Audits and the Management Review process.

Recognising the significant impact of climate change on our operations, we commit to assessing and mitigating climate-related risks to our information assets, promoting energy-efficient practices, and fostering a culture of sustainability via our ISO14001 certification. By integrating these efforts, we safeguard our data and contribute to global climate action for a sustainable future.

The overall intent of this management system is to give customers and other interested parties, confidence in Panoram’s ability to protect all information held or processed by the business.

Greg Wildisen  
Chairman

DocuSigned by:  
  
08C2C0EA09D44C2...

**Disclaimer:** While Panoram aims to ensure the information contained in this document is as complete and accurate as possible, Panoram makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the contents of this document, and expressly disclaims liability for errors and omissions in the contents of this document.

© Panoram Digital Limited 2024

| Document Control |                                     |
|------------------|-------------------------------------|
| Document ID      | Panoram Information Security Policy |
| Version          | 1.5                                 |
| Classification   | Public                              |
| Document Status  | Published                           |
| Modified by      | Greg Wildisen                       |
| Document Date    | 04/11/2024                          |
| Owner            | Greg Wildisen                       |