



# Information Security Policy

Panoramic Data policy document

Attribute	Value
Title	Information Security Policy
Document Reference	PDL-POL-004
Author(s)	David Bond; Tim Sansom
Pages	8
Revision	1.26
Status	Released

# 1 Document Control

## 1.1 Revision History

Version	Date	Author(s)	Details
1.1	2018-09-07	David Bond	Released
1.2	2018-10-04	David Bond	Added provisions for: JIRA SEC project; SSL Labs; ZAP Pentesting
1.3	2018-10-18	David Bond	Added provisions for: Patch/vulnerability management; Change management
1.4	2020-11-25	Tim Sansom	Updated and reviewed
1.5	2022-01-10	David Bond	Corrected typo
1.6	2022-05-11	Elizabeth Whyman	Reviewed
1.7	2022-06-12	David Bond	Released
1.8	2022-06-29	David Bond	Release following Operations review
1.9	2023-02-03	David Bond	Updated patching policy
1.10	2023-07-05	David Bond	Reviewed and re-issued
1.11	2023-09-07	David Bond	Updated VPN policy Updated access review policy
1.12	2023-10-12	David Bond	Updates in preparation for ISO-27001 audit
1.13	2023-10-12	David Bond	Further updates in preparation for ISO-27001 audit
1.14	2023-11-01	David Bond	Split out Information Security Manual upon advice from BSI
1.15	2024-01-10	Elizabeth Whyman	Grammatical edits
1.16	2024-01-18	Elizabeth Whyman	Updates following ISO meeting
1.17	2024-02-05	David Bond	Consolidated Information security objectives
1.18	2024-02-06	Tim Sansom	Reviewed business continuity objectives
1.19	2024-02-13	Elizabeth Whyman	OPS-39859 actioned
1.20	2024-02-16	David Bond	Minor alterations following Annual Review
1.21	2024-07-22	David Bond	Disposal policy update
1.22	2024-11-27	David Bond	Actioned: OPS-40258, OPS-40297
1.23	2024-11-30	David Bond	Updated following Board Meeting and Internal Auditor review
1.24	2024-12-16	David Bond	Typo correction
1.25	2025-03-17	David Bond	Updated interested parties' requirements
1.26	2025-07-02	David Bond	Reviewed and re-issued

## 1.2 Company Information

Panoramic Data Limited	
Document Role	Provider of Services
Address	46 Heywood Avenue, Maidenhead, Berkshire SL65 3JA, United Kingdom.
Telephone No.	+44 (0)8432 899811
Registered in England & Wales	6982102

## 1.3 Authors & Authorities

Author(s)	Company	Role	E-mail
David Bond	Panoramic Data	Author	david.bond@panoramicdata.com
Elizabeth Whyman	Panoramic Data	Editor/Reviewer	elizabeth.whyman@panoramicdata.com
Tim Sansom	Panoramic Data	Reviewer	tim.sansom@panoramicdata.com

## 1.4 Table of Contents

1	Document Control .....	2
1.1	Revision History.....	2
1.2	Company Information .....	3
1.3	Authors & Authorities .....	3
1.4	Table of Contents.....	3
2	Policy.....	4
2.1	Introduction .....	4
2.2	Scope .....	4
2.3	Purpose .....	5
2.4	Policy aims .....	5
2.5	Information security objectives .....	6
2.6	Roles and Responsibilities .....	7
2.7	Meeting policy objectives .....	7
2.8	Changes to the policy .....	7
2.9	Relevant authorities .....	8
2.10	Special interest groups .....	8

## 2 Policy

### 2.1 Introduction

Panoramic Data Limited (henceforth “PDL”) operates an Information Security Management System (ISMS) in the context of PDL’s business of software development, operation, maintenance and related services. This document provides an overall policy for IT Security, as managed by the ISMS.

This section details the policy's aim, scope and roles.

### 2.2 Scope

The Scope of this Policy is in the:

"Provision of software development, operations and maintenance; and related professional and managed services."

This is in accordance with the Statement of Applicability version 24.1.

#### 2.2.1 Interested parties

Our stakeholders are organizations and individuals that have an interest in our success and vice versa. As part of doing business with us, there will be an exchange of information, of a variety of classifications.

PDL’s specific stakeholder groups have the following needs and expectations (requirements) concerning information security:

Stakeholder Group	Specific requirements
Clients	Ensuring that personal, commercial and operational data confidentiality, integrity and availability is maintained and that contractual obligations are adhered to.
Contractors	Ensuring that personal and commercial data confidentiality, integrity and availability is maintained and that contractual obligations are adhered to.
Employees	Ensuring that personal data confidentiality, integrity and availability is maintained and that contractual obligations are adhered to.
Government	Ensuring that all legal obligations relating to company reporting are accurate and that all company activities are legal.
Owner(s)	Maintaining company value and contractual obligations are adhered to and that contractual obligations are adhered to.
Society	Ensuring that PDL’s systems do not have a detrimental effect on wider society
Suppliers	Ensuring that personal and commercial data confidentiality, integrity and availability is maintained and that contractual obligations are adhered to.

The detailed list of stakeholders of each type can be found on our [Stakeholders Wiki Page](#) and all may be considered to be interested in our ISMS. The Client page contains a list of products and services used by each client, and this is used to scope this policy's applicability to each.

#### 2.2.2 Independent review

This policy is reviewed annually as part of maintaining ISO 27001 certification.

### 2.3 Purpose

This policy's purpose is to:

- Continually improve our ISMS
- Meet our legal and contractual obligations
- Establish ISO 27001:2022 objectives
- Avoid IT security problems that may be expensive and time-consuming to resolve

Prevention is much better than cure. Effective security is a team effort requiring the participation and support of each member of staff (including temporary, agency, interim, contractor or consultant staff).

It is the responsibility of all staff to know and follow all guidelines in this document, in support of this purpose.

### 2.4 Policy aims

This policy's aims are to:

- Ensure the confidentiality, integrity, and availability of data relevant to the success of the business
- Minimise the deliberate or accidental disclosure, corruption, or destruction of information ('data loss') that has the potential to harm our business
- Minimise the impact to the services that we provide ('service impact') that has the potential to harm our business
- Protect stakeholder data
- Reduce the risk of IT problems
- Permit continued operation if something does go wrong
- Keep secure valuable company information, such as source code, plans and designs
- Meet our professional obligations towards our stakeholders

## 2.5 Information security objectives

This section details the Information Security objectives which meet this policy's aims.

Objective	Control	Measurement / Data Location	Cadence
To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations	Management review of policy and ISMS manual	<ul style="list-style-type: none"> <li>Recording of meeting</li> <li>Updated policy</li> <li>Tickets of corrective actions</li> <li>Communication of updated policies within one month of update to all staff, and in the case of this document, update of the company website</li> </ul>	Annually
To manage risk relating to Information Security at a strategic level	Risk register review	<ul style="list-style-type: none"> <li>Risk register is up to date</li> <li>RTPs are up to date</li> <li>Associated tickets are created and assigned</li> </ul>	Monthly
To manage individual security incidents and tasks	Incident handling controls	<ul style="list-style-type: none"> <li>ISMS related tickets are updated/closed by their due date, as automatically monitored</li> </ul>	Weekly
To ensure that the policies and ISMS manual are adhered to	Internal audit External audit	<ul style="list-style-type: none"> <li>Internal audit results folder in the Operations SharePoint</li> <li>External audit results and certification</li> </ul>	Annually
To ensure all software developed meets design objectives and data confidentiality, integrity and availability objectives	Software development controls	<ul style="list-style-type: none"> <li>Security Designs</li> </ul>	<ul style="list-style-type: none"> <li>Upon design</li> </ul>
		<ul style="list-style-type: none"> <li>Quality Assurance Testing</li> </ul>	<ul style="list-style-type: none"> <li>Per minor release</li> </ul>
		<ul style="list-style-type: none"> <li>Automated security vulnerability scanning</li> </ul>	<ul style="list-style-type: none"> <li>Monthly</li> </ul>
To ensure the continued operation of critical business functions during and after unexpected disruptions or disasters	Business continuity controls	<ul style="list-style-type: none"> <li>The existence of an identified replacement for all suppliers to minimize supply chain disruptions</li> <li>The existence of an identified deputy for IS personnel</li> <li>Evidence of communication in one or more channels (Microsoft Teams, email, website and phone) to keep everyone informed during a critical incident</li> <li>There is documented testing of backup and restore procedures as per the "regular backup tests" JIRA ticket</li> </ul>	ASAP when needed
To ensure that all staff are aware of the latest policies and procedures relating to Information Security	Awareness controls	<ul style="list-style-type: none"> <li>Written confirmation from staff to line managers that they have read the latest updates</li> </ul>	Upon change

## 2.6 Roles and Responsibilities

Roles and responsibilities regarding this policy are as follows:

- The Managing Director has overall responsibility for:
  - IT security strategy
  - The ISMS
- The Head of Operations in their role as Data Protection Officer (DPO), is the designated security authority with responsibility for:
  - Maintaining and implementing this policy
  - Ensuring adherence to the Information Security Manual (PDL-POL-012)
  - Identification and management of Information Security vulnerabilities
- The Head of R&D is responsible for:
  - Software security design and implementation
  - Maintaining and implementing the Software Development Lifecycle Policy (PDL-POL-008)
- The Internal Auditor is responsible for:
  - Performing Internal Audit tasks relating to ISO27001 certification
- All members of the Senior Management Team (“Heads of”) are responsible for ensuring that the policy:
  - Is in line with the organisation’s objectives
  - Implementation is sufficiently well resourced
  - It is sufficiently well communicated amongst stakeholders
  - Considers stakeholder consultation as part of continual improvements
  - Achieves its intended outcomes (see above)
  - Is compatible with ISO 27001’s requirements
- All staff have a responsibility to:
  - Comply with this policy

The staff identified above will have sufficient competency to perform their assigned responsibilities as set out in the Information Security Manual Section 4.1.2 “Information Security in Staff Selection”.

## 2.7 Meeting policy objectives

Behaviours that ensure the objectives of this policy are achieved are covered in the Information Security Manual (PDL-POL-012).

## 2.8 Changes to the policy

This policy is reviewed annually, or when events mandate an update. In the meantime, management should be contacted with any questions, suggestions, or feedback.

## 2.9 Relevant authorities

Panoramic Data Limited maintains registration with the Information Commissioner's Office. The Head of Operations is nominated as the Data Protection Officer.

## 2.10 Special interest groups

Panoramic Data Limited maintains registration with the National Cyber Security Centre <https://my.ncsc.gov.uk/>. The relationship is managed by Head of Operations.

Panoramic Data Limited monitors the Dotnet Announcements Team for security bulletins at <https://github.com/dotnet/announcements>. The relationship is managed by the Head of R&D.

Signed for and on behalf of Panoramic Data Limited	
Signature	
Name	David Bond
Title	Director
Date	