

Redefining IT Support

Information Security Policy



Classification: **Public**

This document is intended for public distribution and may be freely shared. All rights reserved.

Document Control

Document Owner	Glyn Cheesman – Head of Security (GRC)
Classification	Public
Approver	Simon Bond – Managing Director
Last Review Date	29/09/2026
Review Frequency	Annual
Next Review Date	29/09/2027
Version	10.0

Note: the current version of this policy is always available at trust.cyansolutions.co.uk.

Table of Contents

1 Introduction 3

2 ISO/IEC 27001..... 3

3 Security Framework 3

4 Leadership and Commitment Policy 4

5 Security Goals and Strategy 4

6 Goals 5

7 Continual Improvement Policy 6

8 Information Classification..... 7

9 Policy Approval, Communication and Review..... 7

10 Additional Information 7

Document Control

This document is considered uncontrolled if it is printed or downloaded from CYAN’s DMS.

1 Introduction

This Information Security Policy defines how information security is set up, managed, measured, reported on and developed within Cyan Solutions Ltd ("CYAN"), in order to protect the confidentiality, integrity and availability of the information we hold and process, both our own and that of our customers.

2 ISO/IEC 27001

CYAN has held ISO/IEC 27001 certification since June 2017, when an independent, UKAS-accredited certification body confirmed that our information security management system (ISMS) met the requirements of the standard. In 2025 we transitioned the ISMS to ISO/IEC 27001:2022.

We maintain this certification through annual external surveillance audits and a full recertification audit every three years, supported by our own programme of internal audits.

The scope of our certification is:

"Provision of fully managed IT support services, including cyber security, cloud solutions, business continuity, VoIP and communications, network management, and IT professional services to SMEs and Non-profit organisations across the UK."

Because of the part our services play in our customers' day-to-day operations, privacy and continuity, the ISMS covers all information systems, people, locations and business processes involved in delivering and supporting those services. That includes cloud-hosted environments, remote and mobile working, and relevant outsourced functions and suppliers.

3 Security Framework

Aligning our information security with ISO/IEC 27001 gives CYAN an internationally recognised framework for building and running our information security and privacy programme. Our controls are selected from the organisational, people, physical and technological controls in Annex A of ISO/IEC 27001:2022, and recorded in our Statement of Applicability. Customers and prospects can then evaluate our security programme against a well-known standard, as well as against their own specific needs.

ISO/IEC 27001 is also the baseline against which we map our legal, regulatory and contractual requirements. The ISMS forms part of our wider Business Management

Document Control

This document is considered uncontrolled if it is printed or downloaded from CYAN's DMS.

System, alongside our ISO/IEC 20000-1 certified service management system and our Cyber Essentials Plus certification.

Protecting our customers' information and our own is achieved through:

- education and awareness for our staff
- security and data protection requirements for our suppliers
- risk assessment, testing and review
- internal audit
- our information classification and handling policies

4 Leadership and Commitment Policy

CYAN's Board is committed to information security and privacy, and to the continual improvement of the ISMS. Information security is represented at Board level, and the Head of Security (GRC) is accountable for the performance of the ISMS and reports on it to the Board. The ISO Committee supports the Board in overseeing the ISMS and making sure it remains understood and effective at every level of the organisation.

This commitment is demonstrated by:

- supporting the operation of the ISMS and our ISO/IEC 27001 certification
- encouraging a culture of security awareness and vigilance
- providing the resources needed to establish, maintain and improve the ISMS
- making sure legal, regulatory and contractual requirements, and the needs of our customers, are met
- overseeing information security at quarterly Board meetings, including risk, legal and regulatory requirements, security controls and certification

The Board and ISO Committee recognise that, as a managed service provider, CYAN must secure the technologies, systems and facilities we use to deliver our services, so that our customers, partners and staff receive a safe and reliable service, with information security risk kept within acceptable levels.

5 Security Goals and Strategy

CYAN is committed to safeguarding the confidentiality, integrity and availability of all physical and electronic information assets, both our customers' and our own. Our information security goals are delivered through the policies and controls within the ISMS, and are aligned with our business goals and Business Growth Plan, our customers' requirements, our legal and contractual obligations, and the requirements of our ISO/IEC certifications.

Document Control

This document is considered uncontrolled if it is printed or downloaded from CYAN's DMS.

Our goals are supported by information security objectives that are specific, measurable, achievable, relevant and, where applicable, time-bound. Each objective has an owner and a way of measuring progress. The objectives are set out in the ISMS and are measured, and reviewed to make sure they remain relevant, at the annual management review.

6 Goals

Information security and data privacy are central to how CYAN operates. Our goals are to:

- meet the security and privacy needs of our customers and partners
- maintain our ISO/IEC 27001 and Cyber Essentials Plus certifications, aiming for no nonconformities at audit
- fulfil our legal, regulatory and contractual obligations
- keep information confidential, in line with our classification and handling policies (confidentiality)
- maintain the accuracy and completeness of customer information (integrity)
- give customers access to their information when they need it, including during and after a major security incident (availability)
- identify risks continually and keep them within our agreed risk appetite
- be prepared to respond to and recover from security incidents, through a tested incident response plan
- protect the wellbeing and safety of our staff
- educate and motivate our staff so that they consider security in everything they do, reducing the risk of a security incident
- make sure our staff can access and support systems where and when they are needed, while keeping risk at an acceptable level

Our information security objectives are measured, and reviewed to make sure they remain relevant, at the annual management review. The Board oversees information security at a higher level every quarter, including risk, legal and regulatory requirements, security controls and certification.

7 Continual Improvement Policy

Continual improvement is a key part of our information security programme. CYAN aims to keep improving how effectively we reduce risk and meet our information security and privacy objectives. We do this by:

- identifying best practice relevant to our services and the market we operate in
- taking a proactive approach to information security, rather than waiting for issues to arise
- making our information security activities measurable
- reviewing and acting on metrics and on the results of audits, risk assessments, vulnerability scanning and security testing
- recording nonconformities and corrective actions, finding their root causes and checking that the actions taken are effective
- learning from security incidents and from exercises such as tabletop tests
- holding a formal management review at least once a year, covering security objectives, audit results, corrective actions, the risk register and priority security projects
- maintaining a security awareness programme that educates staff on our security policies and checks their understanding

Ideas for improvement can come from many sources, including customers, partners, staff, suppliers, audits, risk assessments, incidents and security testing. When evaluating improvement proposals, we consider:

- the benefit to the business and its stakeholders
- the level of risk in not implementing the proposal
- the time needed to implement it
- the resources required
- the cost and value for money

8 Information Classification

CYAN classifies all information within the scope of the ISMS according to its sensitivity. This lets us apply the right level of protection to each type of information and asset, whatever form it takes, through our controls, policies, procedures, training, and the design of our systems and networks.

How information is classified, labelled and handled is set out in our Information Classification Policy, which applies to our own information and to customer information we hold or process.

9 Policy Approval, Communication and Review

This policy is approved by the Managing Director on behalf of the Board. It is reviewed at least annually by the Head of Security (GRC), with any proposed changes considered by the ISO Committee, and sooner if there is a significant change to CYAN's business practices, infrastructure or ISMS scope.

The policy is communicated to all staff and is available to them through our document management system. This policy, and our Information Security Policy statement summarising it, are published on the CYAN Trust Centre.

10 Additional Information

For further information about our ISMS or our ISO/IEC 27001 certification, contact our security team at infosec@cyansolutions.co.uk or visit the CYAN Trust Centre at trust.cyansolutions.co.uk.

Glyn Cheesman, Head of Security (GRC)

End of Document