Security at Skynamo

We take security seriously here at Skynamo, and we are proud to lead our industry when it comes to protecting your organisation's information.

Compliance certifications and regulations

ISO 27001

We are certified to be compliant with the benchmark information security standard – the ISO 27001:2022 standard for information security management systems.

We received our certification in June 2019.
Our certification was renewed in 2022.
Our certification was renewed in 2025 against the updated ISO 27001:2022 standard.
Certificate to be renewed in 2028.

You can view our certificate here.

Cyber Essentials

Skynamo is Cyber Essentials Certified.

Cyber Essentials is a scheme that addresses the most common Internet-based threats to cyber security, particularly attacks that use widely available tools and demand little skill.

The scheme considers these threats to be:

- hacking — exploiting known vulnerabilities in Internet-connected devices, using widely available tools and techniques
- phishing — and other ways of tricking users into installing or executing a malicious application
- password guessing — manual or automated attempts to log on from the Internet, by guessing passwords

Our certification can be verified here.

Skynamo and the EU General Data Protection Regulation (GDPR)

Skynamo has developed tools and processes to ensure our compliance with requirements imposed by the GDPR and to help our customers comply, too.

To learn more about our GDPR compliance, please read our GDPR discussion document.

Security Practices

Taking security seriously at Skynamo means putting in place appropriate security controls to protect your data and that of your staff and customers that you entrust to us.

Here are some of the key security practices that we have in place to give you this peace of mind.

Organisational Security

Our security efforts are championed by our CEO and managed by our information security committee, a team of senior staff drawn from various areas of the business that drives security actions and ensures continuous vigilance and improvement.

Protecting customer data

Our main security objective is to prevent unauthorised access to customer information. To this end, we take exhaustive steps to identify and mitigate risks, implement best practices, and constantly develop ways to improve.

Securing the Skynamo Apps

A key part of protecting customer data is ensuring that the Skynamo apps that our customers rely on are secure and cannot be abused to gain unauthorised access to that data. Our development team has adopted a "secure by design" approach to our software development efforts and work from a comprehensive list of secure engineering principles when making changes or improvements to our apps. The development methodology ensures that security is addressed at each stage of the development process.

Access control

Skynamo adheres to the principles of least privilege and role-based permissions when provisioning access. Staff are only authorised to access data that they reasonably must handle in order to perform their job. All access is reviewed at least quarterly. Multi-factor authentication is used for all access to systems with sensitive data, including our production environment which houses our customer data.

Where possible and appropriate, Skynamo uses private keys for authentication.

Skynamo requires all staff to use an approved password manager to generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks.

Encryption:

We rely on encryption using the latest recommended secure cipher suites to encrypt all data in transit. Data at rest is encrypted where appropriate, specifically in areas where our risk assessments have indicated that other controls do not adequately protect data without encryption.

Disaster Recovery and Business Continuity Plan:

Skynamo uses services deployed by its hosting provider to distribute production operations across multiple separate physical locations. Backup copies of production data are separately maintained, and recovery of the backups is tested regularly.

Responding to security incidents

Skynamo has established procedures to respond to potential security incidents. All incidents are centrally reported and managed by the security staff. The security committee reviews incidents to detect trends and implement measures to reduce repeated incidents.

External Validation

Our information security management system is internally and externally audited once a year. In addition, we perform application security audits and penetration tests as required, usually after the development of a major new feature or component, but at least annually.

We really do care

Everyone at Skynamo understands the importance of security. We see it as a fundamental non-negotiable property of the service that we provide and know that our customers rely on us to do this.