SYNERGY SKY

Written Information Security Program

How we protect information, aligned to ISO/IEC 27001:2022



Introduction

Synergy Sky AS ("Synergy Sky," "we," "our") designs, develops, and operates video interoperability and unified communications software and services. This Written Information Security Program (WISP) explains, at a level suitable for customers, partners, prospective clients, and other interested parties, how we protect the confidentiality, integrity, and availability of the information entrusted to us.

This document is deliberately written for a public audience. It summarizes the substance of Synergy Sky's internal Information Security Management System (ISMS) — the full set of policies, procedures, risk assessments, and records that govern day-to-day security practice — without disclosing internal implementation details, vendor-specific configurations, or other information that would itself create security risk if published.

Synergy Sky's ISMS is built around ISO/IEC 27001:2022, the leading international standard for information security management, and is prepared for external certification audit against that standard. Where relevant, each section below references the corresponding ISO/IEC 27001:2022 Annex A control area so that customers and auditors can map our practices directly to the standard.

> *A note on scope and currency: this is a summary document. It is reviewed and updated at least annually, and following any material change to our security program. It does not replace, and is not a substitute for, the specific contractual, security, or data processing terms agreed with individual customers, which take precedence in the event of any inconsistency.*

Why we publish this document

Security is not something we consider optional or something we treat as purely a technology problem — it is a company-wide discipline that touches our people, our processes, our physical facilities, and our technology. We publish this WISP because:

- Customers and prospective customers increasingly need to understand our security posture as part of their own vendor risk management and due diligence.
- Transparency about how we manage information security builds trust and supports the informed decisions of our interested parties.
- It reflects our own internal accountability — writing our practices down publicly is itself a discipline that reinforces consistent execution.

About ISO/IEC 27001:2022

ISO/IEC 27001:2022 is an internationally recognized standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system. It requires organizations to identify information security risks systematically, select and implement appropriate controls to treat those risks, and to subject the whole system to ongoing measurement, internal audit, and management review. The standard's Annex A sets out 93 reference

controls organized into four themes: organizational, people, physical, and technological. This document follows that structure.

About Synergy Sky and the Scope of Our Security Program

Synergy Sky AS is headquartered in Oslo, Norway, with operations also based in New York, and delivers its products and services through Synergy Sky AS and its wholly owned subsidiaries, Synergy Sky Inc. and Synergy Sky Ltd.

The scope of our ISMS covers the people, processes, and technologies responsible for the management, development, support, marketing, and sale of Synergy Sky's software and services. This includes our corporate offices, our product development and operations environments, the third-party data centers and cloud platforms that host our production services, and the workforce — employees, contractors, and consultants — who work within that environment.

Synergy Sky maintains a register of critical suppliers and service providers that store or process Synergy Sky or customer information, and applies supplier management controls (described in Section 13) to those relationships as part of the ISMS boundary.

Governance

Accountability for information security sits with Synergy Sky's leadership team, who set the strategic direction for the ISMS, approve information security objectives, and receive regular reporting on risk, incidents, and audit results through scheduled management review meetings. Day-to-day coordination of the program is carried out by our Information Security Coordinators, who are responsible for implementation, training, monitoring, and continual improvement of the ISMS across the business.

Our Guiding Principles

Our approach to information security is built on a small number of consistent principles that apply across every policy and control described in this document:

- We protect the confidentiality, integrity, and availability of our own information and the information entrusted to us by our customers and partners.
- We comply with applicable information security, privacy, and data protection laws in the jurisdictions in which we operate.
- We grant access to sensitive information only to those who need it, and only at the minimum level of privilege required to do their job — the principle of least privilege.
- We invest in our people, because an informed and vigilant workforce is our most effective security control.
- We communicate our security expectations clearly, and make our policies available to our workforce and, as appropriate, to interested parties.
- We set measurable information security objectives and hold ourselves accountable to them.

- We treat information security as a continually improving program, not a fixed state.

How We Organize Information Security (ISO/IEC 27001:2022 Annex A.5, Clause 5)

Synergy Sky has established a formal organizational structure to initiate, coordinate, and maintain information security, consistent with ISO/IEC 27001:2022 Clause 5.3 (organizational roles, responsibilities and authorities) and the related Annex A organizational controls.

Roles and responsibilities

- Executive Leadership Team; sets strategic direction, approves policy and risk acceptance criteria, and reviews ISMS performance at planned management review meetings.
- Information Security Coordinators; plan, implement, and monitor the ISMS day to day; maintain policy documentation; coordinate training and awareness; and support risk assessment and incident response.
- Managers; lead by example, ensure their teams are trained and aware of their security responsibilities, and ensure compliance with policy within their departments.
- All personnel; are responsible for following Synergy Sky's security policies, reporting suspected security events promptly, and completing required training.
- Legal Counsel; supports the assessment of legal, regulatory, and contractual security and privacy obligations, and is engaged on exceptions, incidents, and regulatory notifications.

Segregation of duties and independence

Where practical, Synergy Sky separates conflicting duties and areas of responsibility to reduce the risk of unauthorized or unintentional modification or misuse of information and systems — for example, separating software development activity from production operations, and separating risk ownership from the function that facilitates risk assessment.

Contact with authorities and special interest groups

Synergy Sky maintains defined channels for contacting relevant regulatory authorities and law enforcement where required (for example, in connection with a personal data breach), and maintains awareness of developments in the information security field through relevant special interest groups, industry advisories, and vendor and vulnerability notification services.

People: Human Resource Security (ISO/IEC 27001:2022 Annex A.6)

People are both our strongest defense and, if unprepared, our greatest area of risk. Synergy Sky applies security requirements at every stage of the employment lifecycle.

Before employment

- Candidates undergo background verification proportionate to the role, classification of information to be accessed, and applicable legal requirements — including identity and right-to-work verification, reference checks, and confirmation of education and professional qualifications, with more detailed vetting (such as criminal or financial checks) applied only where warranted by role and permitted by law.
- Employment and engagement terms include confidentiality obligations and require agreement to our Information Security Policy and Employee Handbook before access is granted.

During employment

- All employees and relevant contractors receive information security and data privacy training at onboarding and on a recurring basis, covering topics such as the CIA triad (confidentiality, integrity, availability), information classification and handling, incident recognition and reporting, and applicable privacy regulations including GDPR.
- Awareness activities include periodic phishing simulations and other exercises designed to test and reinforce vigilance.
- A formal, graduated disciplinary process applies to confirmed violations of information security or privacy requirements.

Termination or change of role

- Access rights are removed promptly upon termination, and adjusted immediately upon a change of role, in line with the new duties assigned.
- Departing personnel are reminded of ongoing confidentiality obligations that survive the end of their engagement.
- Company assets — hardware, software, and data — must be returned upon termination or change of engagement, with secure erasure applied where personal devices were used for company business.

Asset Management and Information Classification (ISO/IEC 27001:2022 Annex A.5.9–A.5.14, A.7.10, A.8.9–A.8.10)

Synergy Sky maintains an inventory of information assets, including hardware, software, and the systems that process them, with a designated owner accountable for each. A separate, more detailed inventory of IT assets supports vulnerability identification and patching.

Our three-tier classification scheme
All information at Synergy Sky is classified into one of three tiers, from least to most sensitive, which determines the handling and protective controls that apply:

- Public Information — information Synergy Sky has deliberately made available to the general public, such as press releases and published marketing materials.
- Confidential Information — information that could cause harm to Synergy Sky, our customers, or our people if disclosed improperly, including financial data, contracts, source code, and internal policies.
- Highly Confidential Information — a subset of Confidential Information carrying the risk of serious or irreparable harm if disclosed, such as personal data, security audit and penetration test findings, risk assessments, and strategic or financial plans.

Unless clearly marked or evidently intended as public, all Synergy Sky and customer information is treated as at least Confidential by default.

Handling, storage, and disposal

- Highly Confidential Information sent by electronic media must be encrypted and, where applicable, password protected, and shared only on a strict need-to-know basis.
- Systems or physical records containing Highly Confidential Information are kept in physically secured locations, accessible only to those with a defined business need.
- When equipment or media reaches end of life, Synergy Sky ensures data is securely destroyed or the media is rendered unreadable using accepted data destruction standards (consistent with NIST SP 800-88 guidance) — simply deleting files or reformatting is never considered sufficient.

Access Control and Identity Management (ISO/IEC 27001:2022 Annex A.5.15–A.5.18, A.8.2–A.8.5)

Access to Synergy Sky's systems and information is granted on the basis of business role and the principle of least privilege — individuals receive only the access required to perform their job, and no more.

Core requirements

- Access is granted, modified, and revoked through documented, auditable procedures, tied to changes in role, responsibility, or employment status.
- Role-based access control is used wherever practical, standardizing access by business function rather than granting bespoke access to each individual, which also simplifies periodic access reviews.
- Administrative or privileged access is granted only where there is a clear business need, is limited to the extent feasible, and requires demonstrated competency to use the relevant system safely.

- Standard access rights are reviewed at least annually; privileged access rights are reviewed at least twice a year.

Authentication

- Passwords must meet defined strength requirements and must never be reused across Synergy Sky and non-Synergy Sky accounts.
- Two-factor (multi-factor) authentication is required wherever it is available, and is mandated for secure remote access.
- Remote connections to development and production networks are protected via encrypted VPN connections.
- Secret authentication information (passwords, cryptographic keys, tokens) is treated as Highly Confidential and must never be shared, written down insecurely, or hinted at.

Identity lifecycle

Synergy Sky manages the full lifecycle of identities with access to information assets — covering communication platforms, cloud services, productivity tools, and network services — through defined workflows for account registration, provisioning, periodic review, and revocation.

Cryptography (ISO/IEC 27001:2022 Annex A.8.24)

Synergy Sky uses encryption to protect Confidential and Highly Confidential Information, both at rest and in transit, using only generally accepted, industry-standard algorithms and protocols.

- Data transfers involving Highly Confidential Information must be encrypted, and Confidential Information is encrypted wherever feasible.
- Approved algorithms include AES for symmetric encryption (minimum 128-bit, with 256-bit preferred) and current TLS versions for data in transit, consistent with recognized industry guidance such as the OWASP Cryptographic Storage Cheat Sheet.
- Cryptographic keys are treated as Highly Confidential Information, generated using industry-standard random number generation, tracked, rotated periodically according to risk, and never known to only a single individual (other than where a key relates solely to an individual's own access credentials).
- Any use of cryptography must be approved by the appropriate technical authority; ad hoc or unapproved cryptographic implementations are not permitted.

Limited, documented exceptions exist for legacy interoperability with certain third-party endpoint hardware that does not support current protocol versions; these exceptions are risk-assessed, time-bound, and reviewed periodically.

Physical and Environmental Security (ISO/IEC 27001:2022 Annex A.7)

Synergy Sky protects the physical locations and equipment that support its information systems, whether in its own offices or in third-party hosting facilities.

Layered access zones

- Zone 1 — general building access, controlled by building management.
- Zone 2 — Synergy Sky office areas, access controlled by Synergy Sky and limited to approved personnel and escorted visitors.
- Zone 3 — secure areas such as data closets and server rooms, restricted to personnel with a defined, role-based need.
- Zone 4 — third-party hosting locations; our hosting providers are required to maintain 24/7 physical monitoring of their facilities, including video surveillance, access logging, and intrusion detection.

Day-to-day physical practices

- A clear desk and clear screen approach: workstations are locked when unattended, and Confidential or Highly Confidential material in physical form is stored in locked drawers or offices when not in use.
- Computer screens are positioned so that sensitive information cannot be viewed by unauthorized individuals.
- Production systems are hosted in facilities that provide environmental monitoring (temperature, humidity, fire detection), protected power supplies, and segregated power and communications cabling.
- Equipment taken off-premises (including for home or remote working) is subject to controls determined by risk assessment; equipment reaching end of life is securely disposed of or reused according to its information classification.

Operations Security (ISO/IEC 27001:2022 Annex A.8.6–A.8.17)

Change and configuration management

Changes to production systems follow a formal, documented change management process, and baseline ('known good') configurations are maintained for production environments using automation to ensure consistency and reduce the risk of human error.

Capacity and availability management

Capacity requirements are monitored and projected based on business criticality, current trends, and anticipated growth, with system tuning applied to maintain availability and performance.

Separation of environments

Development, testing, and production environments are logically separated to prevent unintended impact on live services and to reduce the risk of unauthorized

access to production data. Developers are granted access to production only in limited, specific circumstances such as troubleshooting.

Malware protection
Endpoint protection appropriate to each operating system is deployed across corporate and production computing environments, combined with user awareness training, with documented and risk-assessed exceptions for a small number of environments where such software could itself affect service availability.

Backup
Business continuity and disaster recovery arrangements include documented backup and recovery procedures for the data and software needed to restore Synergy Sky's environments following an incident.

Logging and monitoring
Access to information systems is logged and monitored in accordance with documented procedures to support detection of unauthorized activity and to provide an audit trail for investigations.

Technical vulnerability management
Synergy Sky operates a structured vulnerability management process. Vulnerabilities are identified through multiple channels — including vendor and CVE notifications, malware identification, and regular vulnerability scanning — and are assessed to determine whether affected assets fall within scope, prioritized by severity and business impact, and tracked through to remediation. This process is currently being updated to align fully with ISO/IEC 27002:2022 guidance and current industry severity scoring (CVSS v3.x), as part of our active pre-certification improvement program.

Data leakage prevention
Controls are applied to systems, networks, and devices that process, store, or transmit sensitive information to reduce the risk of unauthorized data exfiltration.

Network and Communications Security (ISO/IEC 27001:2022 Annex A.8.20–A.8.23)

- Firewalls and other perimeter controls separate Synergy Sky's trusted network from the internet, configured according to current technical standards; unauthorized internet connections outside these controls are not permitted.
- Networks are segregated according to information classification and access control requirements, with Highly Confidential Information segmented from the wider network to the extent technically feasible.
- Formal standards and procedures govern the secure transfer of information over any communication channel, taking into account information sensitivity, applicable regulation, and contractual obligations.
- Confidentiality or non-disclosure agreements are used to protect information shared with external parties, and are reviewed regularly.

Secure Development (ISO/IEC 27001:2022 Annex A.8.25–A.8.34)

Security is built into Synergy Sky's software development lifecycle from the outset, following a "security by design" approach.

- Source code is stored in a secure, access-controlled repository providing version control, a complete history of changes, and non-repudiation.
- Coding standards address consistency, modularity, and clear documentation, and prohibit practices such as hardcoded credentials or storing and transmitting passwords in clear text.
- Automated static and dynamic code analysis runs as part of the continuous integration pipeline, with critical findings resolved within the same development cycle and high findings resolved in the next.
- All code changes undergo peer review, with a documented, test-first approach to unit and security testing before code is merged.
- Software passes through structured testing phases — component and functional testing, performance and end-to-end testing, user acceptance testing, and pre-release exploratory testing — before release.
- Development, staging, and production environments are kept logically separate, and the same development policy and vulnerability management practices apply to work carried out by outsourced or third-party developers.
- Regular independent security testing, including penetration testing, is scheduled to validate the effectiveness of these controls.

Supplier and Third-Party Relationships (ISO/IEC 27001:2022 Annex A.5.19–A.5.23)

Synergy Sky relies on a limited number of critical suppliers, including cloud hosting and infrastructure providers, and manages the information security risk of these relationships throughout the supplier lifecycle.

- Suppliers with access to Synergy Sky or customer information are evaluated for their ability to maintain appropriate security safeguards before engagement.
- Security and data protection requirements are incorporated into supplier contracts, including — where personal data is processed — a Data Processing Addendum consistent with GDPR and other applicable data protection laws, covering matters such as confidentiality, sub-processing, security incident notification, and international data transfer safeguards (including Standard Contractual Clauses where relevant).
- High-risk suppliers are subject to ongoing monitoring and periodic review against agreed service levels and security requirements.
- Changes to a supplier's service delivery or contractual arrangements are managed through Synergy Sky's formal change management process.

Information Security Incident Management (ISO/IEC 27001:2022 Annex A.5.24–A.5.28, A.6.8)

Synergy Sky maintains a documented Incident Response Plan describing how we detect, assess, contain, remediate, and recover from information security incidents, and how we communicate about them.

Reporting

All personnel are required to report any suspected or actual information security incident immediately to security@synergysky.com, rather than investigating independently. External parties who become aware of a potential issue affecting Synergy Sky are directed to the same address. Reported security events are formally acknowledged within four hours of being raised.

Assessment and response

Each reported event is assessed for its impact on confidentiality, integrity, and availability, classified by severity, and — where personal data may be affected — is escalated for privacy impact analysis to determine whether a regulatory breach notification is required. A dedicated incident response team investigates, contains, remediates, and documents each confirmed incident, engaging legal counsel and, where appropriate, law enforcement, our insurers, and affected customers.

Learning from incidents

Every incident is subject to post-incident review to identify root cause, evaluate the effectiveness of our detection and response, and drive corrective action to reduce the likelihood of recurrence. The Incident Response Plan itself is tested periodically and reviewed at least annually.

Business Continuity and Resilience (ISO/IEC 27001:2022 Annex A.5.29–A.5.30, A.8.14)

Synergy Sky maintains a Business Continuity Plan to ensure that critical business operations, and the confidentiality, integrity, and availability of information, can be sustained under adverse conditions.

- Synergy Sky has identified its core business functions and the critical resources and communication systems that support them, and prioritizes recovery based on defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- The plan assigns clear responsibilities for recovering critical systems and coordinating with external vendors and hosting providers during a disruption.
- Business continuity arrangements are tested and reviewed at least annually, and updated to reflect changes in the business or its critical systems.

As part of our current pre-certification improvement program, Synergy Sky is extending its documented contingency planning to cover each of its critical systems individually, building on the existing company-wide Business Continuity Plan.

Legal, Regulatory, and Contractual Compliance (ISO/IEC 27001:2022 Annex A.5.31–A.5.36)

Synergy Sky operates across multiple jurisdictions and maintains awareness of, and compliance with, the laws and regulations applicable to its business, including information security, data protection, and anti-corruption requirements.

Data protection and privacy

As a company headquartered in Norway operating within the European Economic Area, Synergy Sky's data protection practices are led by the EU General Data Protection Regulation (GDPR) and Norwegian implementing law, with additional requirements layered in for other jurisdictions in which we or our customers operate, including the UK GDPR and Data Protection Act 2018, and applicable US state privacy laws.

- Personal data is processed only for defined, documented purposes, in accordance with data processing agreements executed with our customers.
- International transfers of personal data are protected using recognized legal transfer mechanisms, including EU and UK Standard Contractual Clauses, as applicable.
- Synergy Sky supports customers' exercise of data subject rights and cooperates with data protection impact assessments and regulatory inquiries as required under our contractual and legal obligations.

Anti-corruption and business ethics

Synergy Sky maintains an Anti-Corruption Policy, led by the requirements of Norwegian law (including the Norwegian Penal Code) and incorporating relevant international frameworks such as the OECD Anti-Bribery Convention, the Council of Europe Criminal Law Convention on Corruption, the EU's anti-money-laundering framework, and the UK Bribery Act, given Synergy Sky's international customer base and operations. The policy sets out a clear, company-wide prohibition on facilitating payments and describes reporting channels for suspected violations.

Records and documentation

Synergy Sky's information security policies and procedures are formally reviewed, approved, version-controlled, and made available to relevant audiences according to their classification, consistent with our documented Control of ISMS Documents and Records procedure.

Risk Management (ISO/IEC 27001:2022 Clause 6, Clause 8)

Risk management is the foundation of Synergy Sky's ISMS. We maintain a systematic, repeatable process for identifying, analyzing, evaluating, and treating information security risks.

- Risks are identified across all information assets within ISMS scope, with a named risk owner assigned accountability for each.
- Risk is analyzed by combining likelihood and consequence (impact) against a documented risk matrix, producing a risk level used to prioritize treatment.

- Risk treatment options include avoiding, mitigating, transferring/sharing, or formally accepting a risk; treatment decisions and residual risk acceptance are recorded in a risk register.
- Controls selected to treat risk are compared against the reference controls in ISO/IEC 27001:2022 Annex A and recorded, together with their implementation status and justification, in Synergy Sky's Statement of Applicability.
- Risks rated High require review and cannot be accepted solely by the risk owner — they are escalated to top management.
- A full risk assessment is performed at least annually and whenever significant changes occur, with results and treatment status reported to management review.

Synergy Sky is currently refreshing its enterprise-wide risk register and treatment plan as a priority action ahead of external certification, to ensure the register fully reflects the current risk landscape and treatment status for all in-scope information assets.

Measuring Performance and Continual Improvement (ISO/IEC 27001:2022 Clause 9, Clause 10)

Internal audit

Synergy Sky conducts internal audits of its ISMS processes and controls, with a baseline of comprehensive annual coverage, increasing in frequency for higher-risk areas or those with previous findings. Audit results are reported to management and tracked to resolution.

Management review

Leadership formally reviews the ISMS at planned intervals, considering audit results, risk assessment outcomes, incident trends, interested party feedback, and progress against information security objectives, and directs any resulting changes to policy, resourcing, or the risk treatment plan.

Corrective action and nonconformities

Where a nonconformity is identified — whether through audit, incident review, or day-to-day monitoring — Synergy Sky investigates the root cause and implements corrective action to prevent recurrence, documenting the outcome as part of the ISMS records.

Information security objectives

Measurable information security objectives are proposed by the Information Security Coordinators and approved by leadership, taking into account risk assessment results and applicable requirements. Progress against these objectives is reviewed at each management review meeting.

Document Review

This document will be reviewed annually and updated to reflect the findings of the review. It will also be reviewed following a major incident which requires a review of the Policy and supporting guidance, or a major change which impacts the Policy.

Document History

Version	Details	Revised by	Date of Issue
0.1	Initial draft of new WISP prepared and issued for stakeholder review.	Gareth Mann-Tighe	
1.0	Reviewed and published	Mark Dumas	Aug 10, 2026