Olyteck Cyber
Cybersecurity for Microsoft 365

INFORMATION SECURITY · PUBLIC SUMMARY

Information Security Policy

Executive summary of how Olyteck protects the confidentiality, integrity, and availability of information assets handled in the course of providing Olyteck Cyber to its customers.

Document	Information Security Policy - executive summary
Version	1.0 - 29 May 2026
Owner	Olyteck CTO
Review cadence	At least annually
Classification	Public
Full document	Available under non-disclosure agreement on request

Commitment

Olyteck operates Olyteck Cyber, a Microsoft 365 security-posture scanner hosted in the European Union. We are committed to protecting customer data through a layered set of administrative, technical, and physical controls aligned with ISO/IEC 27001, SOC 2 Trust Services Criteria, the OWASP Application Security Verification Standard, the CIS Critical Security Controls, and the EU General Data Protection Regulation.

This policy is reviewed at least annually by the policy owner and approved by Olyteck leadership. All Olyteck personnel and contractors with access to the platform are required to read it on hire and on every material update.

Guiding principles

- Least privilege. Access to systems and data is granted on the smallest scope that allows the job to be done.
- Defence in depth. We assume any single control may fail; controls are layered so that failure of one does not compromise security.
- Privacy by design. Customer data is minimised at collection, kept in the European Union, and not shared with parties outside the documented sub-processor list.
- Transparent assurance. We publish our security posture, sub-processor list, incident-handling commitments, and downloadable documentation in a public Trust Center.
- Continuous improvement. Findings from internal reviews, external audits, and incidents drive specific corrective actions tracked to closure.

Control areas

Area	Summary
Access control	Named accounts. MFA on every system that supports it. Least privilege; quarterly access review; joiner-mover-leaver process.
Cryptography	TLS 1.2 or 1.3 in transit. AES-256 at rest. Secrets stored outside the document root; rotated on a documented cadence.
Secure development	Private repository with branch protection. Peer code review on every change. Automated static analysis and dependency-vulnerability scanning. Staged deployments with rollback.
Vulnerability management	Continuous internal scanning. OWASP ZAP DAST against staging. External penetration testing periodically and prior to major releases.
Logging and monitoring	Append-only security event log retained at least 12 months. Per-tenant audit log of administrative actions. On-call coverage for production-affecting events.
Incident response	Documented process covering detection, containment, eradication, recovery, customer notification (within 72 hours for personal-data incidents), and post-incident review.
Business continuity	Daily encrypted backups in a separate EU region. Recovery exercises performed at least annually. RTO and RPO agreed contractually where required.
Supplier management	Sub-processors bound by written DPA. List published at cyber.olyteck.com/trust. 30-day notice of material changes.
Personnel	Confidentiality and acceptable-use commitments signed on hire. Security awareness training. Encrypted, MFA-protected workstations.
Risk management	Risks identified, assessed, treated, and tracked to closure in the Olyteck risk register, reviewed at least quarterly.

Where to learn more

- Full Security and Architecture Documentation: cyber.olyteck.com/trust
- Sub-processor list, Data Processing Agreement, GDPR one-pager: cyber.olyteck.com/trust

- Detailed Information Security Policy, S-SDLC, pentest summary, BCP exercise report: support@olyteck.com under non-disclosure agreement

Issued as-is

This executive summary is issued by Olyteck and may be relied upon as-is during prospect evaluation and procurement. A counter-signed copy is provided on customer request as part of the contracting paperwork.