yoummday

Security Whitepaper

Overview of all IT Security Controls

Yoummday GmbH
Infanteriestr. 11a
80797 München

Author: Yoummday CISO
Contact: security@yoummday.com
Version: (17.07.2026)

Table of contents

Intro

This whitepaper summarizes the IT security controls Yoummday has implemented to protect its information assets, operations, and customer data. It is intended for security and procurement teams conducting vendor due diligence, and for customers seeking assurance over Yoummday's security posture.

Yoummday operates an Information Security Management System (ISMS) aligned with ISO/IEC 27001, covering governance, technical controls, incident response, and third-party risk management. These controls are reviewed on a defined audit and maintenance cadence, and updated as our threat landscape and infrastructure evolve.

This document provides a summary overview rather than exhaustive technical detail. Supporting evidence — including audit reports, penetration test summaries, and policy documentation — is available on request under NDA.

Security Controls

The following IT Security Controls are implemented at Yoummday.

Endpoint Encryption

Endpoint encryption for hard disks is a security measure that protects data by converting it into unreadable code, accessible only with the correct decryption key. This ensures that even if our hard disks are lost or stolen, the data remains secure and inaccessible to unauthorized users.

Microsoft BitLocker provides full disk encryption, securing data on Windows devices by encrypting the entire drive. Our BitLocker uses Trusted Platform Module (TPM) to enhance security by ensuring that the encryption keys are stored safely and are inaccessible without proper authorization.

Documented ISMS Security Policies

According to our ISO27001 ISMS documentation management, a structured approach is defined and implemented for publishing IT Security Policies and Guidelines. Those support the secure operation of Yoummday's business. Process name: P-38 Approval of QMS and ISMS documents

Roles and Responsibilities

A clear description of Roles and Responsibilities is defined in both: a RACI matrix in ISMS and within the operating teams. It defines roles like CISO, Head of IT and Process Managers as well as the assignment of tasks to these roles.

Technical Guidelines and Concepts

For the secure technical operation of the Yoummday infrastructure, IT has defined structured and documented guidelines and technical concepts. Those give staff detailed instructions about secure configuration and hardening and are applied to relevant systems.

Examples are: cryptography concept.

SIEM Analysis

Security Information and Event Management (SIEM) is implemented to manage and analyze security data, enabling the detection and response to potential threats in real-time for Yoummday server systems. Yoummday is leveraging Elastic Security, built on the Elastic Stack which enhances SIEM capabilities by ingesting, normalizing, and analyzing security data through powerful search and visualization features.

Vulnerability Management

Vulnerability scanning and management is a critical security control within our IT Security Strategy. This automated process scans networks, applications, and devices to detect potential vulnerabilities that could be exploited. Tenable Vulnerability Management is used for this control by enabling comprehensive scanning across the IT infrastructure environment and web applications.

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) is a security solution designed to monitor, detect, and respond to threats on endpoints such as computers and mobile devices. EDR tools continuously collect and analyze data from endpoints to identify suspicious activities and potential breaches.

Yoummday uses Microsoft Defender's capabilities to provide comprehensive protection by detecting and investigating advanced threats across our organization’s network. Incoming alerts are monitored and investigated accordingly.

Security Incident Response

Our Incident response involves a structured approach to addressing and managing security incidents. When a potential security incident is detected, the process begins with immediate identification and classification to assess its severity and potential impact. Next, containment measures are implemented to prevent the incident from causing further damage. The affected systems are then analyzed to determine the root cause, and steps are taken to eradicate the threat and remediate any vulnerabilities. After the threat is neutralized, the systems are restored to normal operation, and thorough documentation is completed. Finally, a post-incident review is conducted to learn from the event and improve future response strategies, ensuring continuous enhancement of the organization's security posture.

For well-known security incident types pre-defined runbooks are documented. An emergency coordinator takes care of managing the security incident over its life cycle. The coordinator is also responsible to establish an emergency team, if needed, and for proper communication to involved stakeholders.

IT Security Advisory

The internal IT security advisory service, provided by the CISO team, assists other departments in evaluating and enhancing the security of their projects. This service involves a thorough review of project plans and implementations to identify potential IT security risks. The CISO team offers expert guidance on best practices, security requirements, risk mitigation strategies and threat modeling depending on the demand. They collaborate closely with project teams to ensure that security measures are integrated effectively throughout the project lifecycle. This proactive approach helps departments safeguard sensitive data and maintain the organization's overall security posture.

Penetration Testing

The penetration test program service, provided by the CISO team, is designed to detect vulnerabilities in an organization's infrastructure and web applications. This service involves simulating cyber-attacks to identify and exploit security weaknesses before malicious actors can. For this external suppliers are hired who conduct thorough assessments, including network, system, and application tests, to uncover potential vulnerabilities. They provide executive and detailed reports with findings and recommendations for remediation. By proactively identifying and addressing security gaps, the penetration test program enhances overall cybersecurity resilience. A tailored penetration test is executed at least once a year.

Threat Intelligence

The internal threat intelligence service, provided by the CISO team, monitors relevant vendors and markets for security threats that could impact the organization's systems. This service involves continuously gathering and analyzing threat data from various sources to identify potential risks and emerging threats (OpenCVE, bugalert and more). The CISO team evaluates the applicability of these vulnerabilities to the organization's environment and provides timely alerts and recommendations for mitigating actions. By staying informed about the latest security threats, this service helps ensure Yoummday's systems remain protected against potential exploits.

Awareness Training

Our security awareness training program is designed to empower employees with the knowledge and skills needed to protect company assets from cyber threats. The training covers a wide range of topics, including phishing, password security, and safe browsing practices, ensuring that employees are well-prepared to identify and respond to potential risks. Real-world scenarios and interactive modules are used to enhance engagement and retention. To ensure effectiveness, the training is regularly updated to reflect the latest threat landscape and incorporates assessments to measure understanding. Additionally, participation is tracked and reported, with follow-up training provided as needed to address any gaps. We are leveraging an online platform for both our internal employees and our talents.

Data Protection and Privacy

To comply with GDPR and local regulations, Yoummday has a dedicated data protection team. The data protection team is led by our VP Legal & GC and Legal Privacy Counsel who also act as data privacy coordinators throughout the company. The team is extended by our external dedicated data protection officer (DPO) and oversees all data protection and data privacy concerns. The data protection team is consulted in all major projects to ensure data protection from the outset, in line with our privacy-by-design principle.

Credential Leakage Monitoring

At Yoummday, we are committed to safeguarding the security of our users and customers by partnering with an external service for credential leakage monitoring. This service continuously scans a wide range of online sources for any signs of compromised credentials, allowing us to quickly identify potential threats. If a credential leak is detected, the CISO Team promptly alerts affected users and takes necessary actions, such as requiring password changes or additional verification.

Secure Supplier Access Gateway / Privileged Remote Access (PRA)

Our secure supplier access solution based on BeyondTrust provides vendors with controlled, least-privilege access to Yoummday's systems without exposing internal networks or credentials. It enforces multi-factor authentication (MFA), session monitoring, and just-in-time access to minimize security risks associated with third-party access. The solution ensures that all supplier interactions are logged and audited.

Account Reviews / Recertifications

Account reviews, also known as recertifications, are conducted regularly to ensure that all user access rights remain appropriate and aligned with the principle of least privilege. As part of our security governance, all standard user accounts undergo a comprehensive review at least once per year. Privileged accounts, due to their elevated access and higher risk potential, are reviewed more frequently. These privileged account recertifications are performed quarterly to ensure strict oversight and timely adjustment of access rights. This structured review process supports compliance, strengthens access control, and reduces the risk of unauthorized or excessive permissions.

Elevated control for Admins using Privileged Identity Management (PIM)

Microsoft Privileged Identity Management (PIM) secures administrative access by replacing standing privileged roles with just-in-time elevation, reducing the attack window for compromised accounts. It enforces approval workflows, MFA, and time-bound activation with full auditability, so high-risk admin actions are tightly controlled and traceable. This strengthens least-privilege governance, limits lateral movement opportunities, and improves detection and response for identity-based attacks.

AI assisted penetration tests

Regular penetration testing applied using AI-assisted tooling (e.g. Strix, HexStrike AI). Executed on demand to identify, prioritize and validate security weaknesses across systems. Maintained by the CISO Team.

Dev credential scanning

Prevents credentials and secrets from being committed to source code. GitLab Secret Detection runs as a mandatory job in the CI/CD pipeline's Security Scanning stage on every Merge Request targeting protected branches; a failing pipeline blocks the merge until resolved. GitLab Push Rules (server-side pre-receive hooks) additionally reject direct pushes of secrets to repositories. Secrets are kept out of code by storing them in protected CI/CD variables or in Passbolt rather than being committed. Mandatory code review of every Merge Request explicitly covers secure handling of secrets and credentials, and direct commits to protected branches are prohibited (merge-only workflow requiring approvals and a passing pipeline).