Information Security at Mastek

Mastek is a global digital engineering and cloud transformation partner, delivering cutting-edge services in Digital Engineering & Experience, Data Automation & AI, Oracle Cloud, Salesforce, and Managed Cloud Services. Mastek empower organizations across diverse industries—including Healthcare & Life Sciences, Retail, Manufacturing & Technology, Financial Services, Government & Public Sector, Higher Education, Construction, Hospitality, Transportation, and Media—to accelerate innovation and achieve impactful business outcomes.

Mastek's CISO office plays a critical role in protecting the company's digital assets and brand integrity. By championing a proactive security-first approach and fostering a culture of shared responsibility, Mastek reinforces its unwavering commitment to safeguarding sensitive data and earning the continued trust of customers and partners worldwide.

Strengthening Trust through ISO/IEC 27001:2022 & ISO/IEC 27701:2019 - Certified Information Security and Privacy Management:

At Mastek, we champion a proactive approach to both information security and privacy with robust, globally recognized frameworks: ISO 27001 for Information Security Management and ISO 27701 for Privacy Information Management. Together, these certifications demonstrate our unwavering commitment to protecting critical data, ensuring privacy, and maintaining trust. Mastek is proudly certified with both Cyber Essentials and Cyber Essentials Plus, demonstrating our dedication to maintaining robust cybersecurity standards. In addition, an independent auditing agency performs annual audits and issues SOC 1 Type II and SOC 2 Type II attestation reports, ensuring our processes and controls meet rigorous industry requirements.

Our integrated management system centers on the **Confidentiality, Integrity, Availability** and **Privacy** delivering:

- **Confidentiality** – Sensitive data is secured and accessible only to authorized users, minimizing risks of breaches or accidental exposure.
- **Integrity** – Data accuracy and consistency are rigorously maintained, preventing unauthorized modifications.
- **Availability** – Authorized users enjoy reliable access to essential systems and information, supported by strong business continuity plans.
- **Privacy** – Enhanced controls and processes safeguard personal data, ensuring compliance with global privacy regulations and respecting individual rights.

Through these rigorous standards, Mastek assures customers, partners, and stakeholders of our dedication to safeguarding digital assets, respecting privacy, and upholding their confidence.

Certified and Globally Trusted

At Mastek, we power our security and privacy commitments with a world-class Information Security Management System (ISMS) and Privacy Information Management System, proudly certified to ISO/IEC

27001: 2022 and ISO/IEC 27701:2019 standards. Mastek is proudly certified with both Cyber Essentials and Cyber Essentials Plus, demonstrating our dedication to maintaining robust cybersecurity standards. In addition, an independent auditing agency performs annual audits and issues SOC 1 Type II and SOC 2 Type II attestation reports, ensuring our processes and controls meet rigorous industry requirements. These globally recognized certifications reflect our unwavering dedication to safeguarding data, protecting privacy, and delivering trusted, secure solutions across every facet of our business.

Information Security Governance

At Mastek, our Information Security and Privacy Management System (ISMS) and Privacy Information Management System (PIMS) emphasizes strong governance to ensure a unified and structured approach to protecting information assets across the organization. Led by the Chief Information Security Officer (CISO), the ISMS team comprises experts in Risk & Governance, Audit & Compliance, and Security Operations, all working collaboratively to support the CISO in managing and overseeing information security.

The CISO holds direct accountability for cybersecurity and IT security, while the Chief Information Officer (CIO) acts as the overall steward of information security, ensuring that security initiatives align seamlessly with Mastek's strategic objectives. Together, they establish and maintain robust governance frameworks to effectively mitigate risks and safeguard the company's critical information.

Priority for the Committee

At Mastek, our Cyber Security, Privacy & AI Governance Committee is deeply committed to upholding the highest standards of information security and data privacy—core pillars that protect our company and empower our clients. Through quarterly risk reviews driven by our Risk Management Committee, we maintain a proactive and transparent approach. The committee stays informed with real-time insights from the CISO Office on security posture, updates on operational IT risks from our Global IT team.

Information Security Strategy Highlights

At the core of our security strategy is a commitment to safeguarding data, ensuring business continuity, and staying ahead of emerging threats. Key features of our program include:

- **Leadership-Driven Security**
  Our Chief Information Security Officer (CISO) provides strategic oversight and expert guidance to drive a robust and resilient security framework.
- **Proactive Risk Management**
  We actively identify and mitigate technical and operational risks to protect our most critical information assets.
- **Next-Generation Cybersecurity Technologies**
  Leveraging advanced tools and technologies, we stay ahead of the curve to defend against an ever-evolving threat landscape.
- **Secure Software Development**
  Security is built into every step of our software development lifecycle, from initial design to final deployment and testing.

- **Controlled and Secure Change Management**
  Our streamlined change management processes ensure that system updates are securely implemented with minimal disruption.
- **Resiliency and Continuity Planning**
  We prioritize business continuity through comprehensive disaster recovery plans and rigorous testing to ensure operational resilience.
- **Independent and In-Depth Assessments**
  Regular internal audits and third-party assessments help validate and strengthen our security posture.
- **Continuous Security Posture Monitoring**
  We conduct ongoing assessments to ensure our defenses remain strong, adaptive, and responsive.
- **24/7 Threat Detection and Response**
  Our cybersecurity operations are monitored around the clock to detect, respond to, and neutralize threats in real time.
- **Zero Trust Access Controls**
  With Zero Trust architecture and role-based access management, we ensure only the right people have the right access at the right time.

Information Security Policy

At Mastek, directives from our Cybersecurity, Privacy, and AI Governance Committees are seamlessly translated into actionable Information Security Policies under the leadership of our Chief Information Security Officer (CISO), ensuring strategic alignment and operational excellence across the organization.

At Mastek, our Global Information Security Policy provides clear, comprehensive guidance on the acceptable and responsible use of technology across the organization.
Built on globally recognized standards such as ISO and the National Institute of Standards and Technology (NIST), our robust framework of IT Risk and Information Security policies, standards, and procedures reflects our unwavering commitment to data protection and operational integrity.

The policy outlines key protocols covering password protection, acceptable usage, email practices, and individual security responsibilities—ensuring every employee, entity, and affiliated partner upholds the highest standards of information security.

To remain adaptive and resilient, our Information Security Policy is reviewed annually—or updated as needed in response to shifts in the cybersecurity landscape. All updates are made easily accessible to Mastek employees through our internal intranet portal.

Mastek's Cyber Resilience Powered by Incident Management Excellence

At Mastek, our Chief Information Security Officer (CISO) leads a dedicated focus on standardization and systematic risk reduction. Mastek deploy robust technology and security controls that safeguard our facilities and critical information assets from unauthorized access, ensuring uncompromised confidentiality, integrity, and availability.

Our cyber resilience strategy embraces a dual approach: leveraging state-of-the-art cybersecurity solutions to prevent threats, alongside a proven recovery framework to swiftly manage and recover from any incidents. Aligned with the NIST framework, Mastek implements best-in-class security practices and maintains comprehensive, well-documented procedures—enabling us to confidently navigate today's dynamic threat landscape.

Mastek's dedicated Security Operations Center (SOC) is the backbone of our proactive cyber defense strategy, delivering around-the-clock monitoring, advanced threat detection, incident response, and deep-web threat intelligence.

Our SOC team remains constantly vigilant—identifying, analyzing, and mitigating emerging risks before they can impact our operations. We lead comprehensive initiatives to address modern cybersecurity challenges, including credential leak detection, privileged access management, cloud security, and phishing prevention.

In the event of a security incident, our specialized Security Incident Response Team (SIRT) is activated immediately to contain and resolve threats. Incidents can be swiftly reported through secure channels, including email and a dedicated intranet portal, ensuring quick escalation and expert response.

To further strengthen organizational resilience, Mastek prioritizes robust business continuity and disaster recovery (BC/DR) planning. Regular simulations and recovery drills validate the effectiveness of our strategies, ensuring alignment with ISO 22301 standards and uninterrupted availability of critical systems and services.

At Mastek, cybersecurity is more than protection—it's about building trust, enabling continuity, and staying resilient in a rapidly evolving digital world.

Human-Centric Security: Awareness, Education, and Vigilance

At Mastek, we recognize that **cybersecurity starts with people**. We deliver continuous awareness training to employees and contractors alike—empowering them to play an active role in defending our digital ecosystem.

This initiative is built on the pillars of awareness, education, and vigilance, aiming to reduce human-related risks in cybersecurity incidents and instill a shared sense of responsibility for protecting Mastek's information assets.

Our ongoing training and engagement programs equip individuals with the knowledge and skills to detect and respond to evolving threats. Regular sessions cover critical topics including phishing prevention, password hygiene, social engineering awareness, and data protection best practices—creating a well-informed, cyber-conscious workforce.

To embed security into our culture, we have implemented several key policies and practices across the organization:

- Internal access to up-to-date information security and cybersecurity policies
- Mandatory awareness training for all personnel, supported by compliance tracking and evidence

- A clearly defined escalation process for reporting suspicious activity
- Integration of security performance into employee evaluations and disciplinary frameworks

To reinforce these efforts, we use a multi-channel communication strategy—combining newsletters, posters, e-learning modules, and gamified content—to keep cybersecurity top of mind.

Additionally, we leverage proactive technologies such as phishing simulations, Zero Trust architecture and role-based access controls to reduce risk from the human attack surface—while also minimizing user fatigue.

Regular risk assessments across stakeholder groups help us track awareness levels, identify gaps, and continuously enhance our programs—ensuring that security is not just a process, but a mindset shared across the entire organization.

Comprehensive Cybersecurity Audits, Compliance & Vulnerability Management

At Mastek, our **Information Security Management System (ISMS)** and PIMS is built on a foundation of rigorous verification, continuous oversight, and proactive control mechanisms—ensuring our security posture remains strong, compliant, and resilient.

To elevate assurance levels and maintain trust, we implement a comprehensive suite of monitoring and validation practices, including:

- **Real-Time Security and Network Monitoring**
  Continuous surveillance of our networks and information systems ensures ongoing compliance with global security standards and regulations.
- **Zero Trust Architecture with Continuous Validation**
  Mastek enforce Zero Trust principles—verifying every user, device, and system before granting access to Mastek's information assets, helping ensure secure and compliant interactions across our digital environment.
- **Proactive Vulnerability Assessments & Penetration Testing**
  Regular audits of platforms and applications identify potential vulnerabilities, while external penetration testing and simulated attacks by reputable third-party experts provide independent assurance of our robust defenses.
- **Annual SOC 1 Type II & SOC 2 Type II Certification**
  Mastek systems are independently assessed each year against the Trust Service Criteria for Security, Confidentiality, and Availability, ensuring industry-aligned controls and practices.
- **Ongoing Internal Audits for Customer Projects**
  Mastek conducts continuous, risk-based internal audits tailored to specific client requirements—evaluating alignment with our information security policies and ensuring consistent compliance across every engagement.

Through these initiatives, we don't just maintain compliance—we deliver continuous confidence to our stakeholders by proactively managing risk, validating controls, and reinforcing trust in everything we do.