Miracle42

Organizational and Technical Measures

March 23

Part of itm8®

Content

Introduction

Miracle 42 is dedicated to ensuring the protection of personal data in accordance with the EU General Data Protection Regulation (GDPR). To fulfill this obligation, Miracle 42 implements the ISO/IEC 27001:2022 standard for information security management, which defines the framework for establishing, implementing, maintaining, and continuously improving information security.

Organizational and Technical Measures

Governance

To ensure the implementation, improvement, anchoring, and management of information security and data protection, Miracle 42 has created a Governance model that includes:

- Implemented a set of information security policies.
- Defined roles and responsibilities for information security.
- Implemented an appropriate level of functional separation.
- Ensured that information security is anchored in management.
- Ensured necessary contact points with authorities and interest groups.
- Ensured that information security is part of our project management model.

Asset Management

Miracle 42 controls information assets to ensure protection and proper registration and use. This includes implementing the following measures:

- Information assets are registered.
- Employees are instructed in the acceptable use of assets, including special security requirements for assets outside the company's locations.
- Ensure that assets are returned after use.
- Procedures for secure disposal and reuse of equipment, including data deletion.

Information Protection

Miracle 42 has implemented a range of measures that form the basis for good protection of information, including:

- Data is classified and labeled according to sensitivity and confidentiality.
- Rules for transferring information within the organization and between other stakeholders are established.
- Rules for protecting personally identifiable information are established.
- Ensuring that data is deleted when the organization no longer has a basis for storing it.
- When transferring personal data to test and development systems, either pseudonymization or anonymization of personal data is carried out.

Employee Security

Employees are an important part of maintaining and improving information security. Therefore, several measures have been established to ensure that Miracle 42's employees contribute to maintaining and improving information security in the organization, including:

- All employees must be able to present a clean criminal record.
- Confidentiality and non-disclosure agreements are entered into with all employees.
- All employees are trained and tested in information security and GDPR upon hiring, and then continuously during their employment.
- Rules and controls for secure remote work are established.
- Disciplinary consequences for violations of the organization's security rules are communicated.

Physical Security

Adequate measures for physical security have been implemented to prevent physical access or damage to information assets. This includes:

- Access control and monitoring of access to office locations and data centers.
- Use of ID and access cards for employees, and guest cards for guests to ensure clear identification.
- Measures for burglary protection, and alarms for burglaries
- Minimization of access to data centers
- Video surveillance of entrances
- Guidelines for working in secure areas are implemented.
- Rules for clean desk and locking the screen when leaving the workplace.
- Rules for placement of equipment so that critical equipment is only placed under lock and key.
- Cables and other equipment are secured against sabotage.
- Equipment is maintained in accordance with the supplier's instructions and recommendations.

System and Network Security

Systems and networks are secured by applying secure standards for installation and configuration of new assets. Once systems are established, they are maintained and monitored through the following measures.

- Documented operating procedures are implemented for backup, patch management, and capacity management, among other things
- Systems for malware protection are implemented.
- Networks are secured and segmented to limit access to the necessary.
- Change management is used to minimize errors resulting from changes and installations.
- Configurations are controlled and monitored to ensure that required security settings are adhered to.
- Procedures are implemented to ensure that test and development systems are protected in the same way as production systems or otherwise do not pose an increased risk.
- Cryptography is used in communication over open networks or as agreed upon with Miracle 42's customers.
-

Application Security

When performing development tasks for internal systems or for customers, Miracle 42 has implemented several measures that minimize the risk of breaches of confidentiality, integrity, or availability.

- Access to source code is limited to include only necessary developers.
- Procedures have been established for secure development throughout the system life cycle.
- Application security requirements have been defined that are tailored to the criticality of each system.
- Code review is used prior to code approval.
- Procedures are used to ensure functional and security testing after releases.
- Contracts and controls are in place in cases where development is outsourced, ensuring the same security and code testing.
- Separate development, test, and production environments are used where possible.

Identity and Access Management

Miracle 42 has implemented measures to ensure control over users, their access rights to systems, data, and customer systems. This includes:

- Controls for physical and logical access
- Ensuring identities are unique in accessing assets, infrastructure, and systems.
- Employees are trained in protecting authentication information.
- Systems are in place to ensure the use of strong passwords and prevent multiple users from using the same password.
- Access is managed primarily through roles, ensuring that unnecessary access is removed during internal rotations.
- Procedures are in place to ensure that the assignment of rights must be approved before they are established.
- Privileged access is only assigned to a user separate from the employee's daily user account.
- Periodic checks are in place for standard and privileged users.
- Secure authentication (MFA) is used to access critical applications and customer systems.

Threat and Vulnerability Management

Miracle 42 follows the threat landscape to adapt security controls and handle vulnerabilities.

- Miracle 42 continuously monitors and evaluates vendor vulnerabilities.
- Critical vulnerabilities are handled on Miracle 42's systems, and customers are informed of recommended actions.
- Miracle 42 follows the threat landscape from society through announcements from authorities or news in the press or other media.
- Security incidents are analyzed for potentially new threats.
- Vulnerability scans are performed for internal systems, servers, and applications, and for customer systems that purchase this service.
- Vulnerabilities are handled based on a risk assessment and mitigated as much as possible.

Continuity

A number of measures have been established to ensure continuity of data and systems in the event of critical incidents.

- Infrastructure, systems, and applications are configured with the level of redundancy agreed upon with the customer.
- Emergency plans have been established for handling extraordinary critical incidents.
- Emergency plans have been established for Miracle 42's critical systems and services.
- Capacity in infrastructure and storage is monitored and continuously expanded to avoid downtime.
- Backups are made of systems and data, and backup data is protected against compromise.
- Procedures for restoring systems, data, and applications have been established.
- Restore tests are carried out to test employees, procedures, and backup systems.

Vendor Security

Vendors and sub-processors are used to provide services to customers. Miracle 42 requires vendors and sub-processors to minimize the risk of security incidents through vendors.

- Vendors are required to comply with Miracle 42's security guidelines as part of the contract agreement.
- Miracle 42 uses vendors and sub-processors who have adequate security measures in their products or deliveries.
- Miracle 42 supervises vendors and follows up on incidents with vendors.
- Miracle 42 ensures that cloud vendors commit to deleting data after the end of the customer relationship.

Compliance

Miracle 42's Legal and Compliance function ensures compliance with legal and contractual requirements, including the group's compliance with policies and principles and rules. This includes, among other things,

- Planning and conducting internal audits.
- Ensuring that external independent audits are carried out.
- Planning and managing audits from customers.

Information Security Incident Management

Measures have been taken to manage security incidents to minimize the consequences of the incident. Procedures have been implemented for managing information security incidents, including:

- Monitoring and logging to identify security incidents.
- Assessment and analysis of the incident.
- Reaction to the incident based on likely scenarios.
- Learning from security incidents for improvements.
- Collecting evidence in the event of an incident.
- Reporting to the customer and/or authorities.