Information Security Policy

Document Classification:	public
Version:	1.3
Date:	16.01.2024
Author:	Clemens Lasslesberger

History

Author	Change	Version	Date
Clemens Lasslesberger, Daniel Sieder, Christian Rathgeber	Initial Creation	1.0	28.09.2023
Clemens Lasslesberger	Addenda to Human resource security	1.1	04.12.2023
Matthias Hausegger Clemens Lasslesberger	Addenda and review	1.2	15.01.2024
Matthias Hausegger Clemens Lasslesberger	Completion of Document	1.3	16.01.2024

Contents

1 Introduction

ONTEC AG, is a privately held stock corporation based in Austria, which offers Information Technology Services in three different lines of business.

Managed IT Services supports companies of all sizes in managing their IT tasks, providing support through service level agreements and hosting of customer environments.

Development of individual software solutions for business-critical processes and infrastructure. For more than 20 years, leading companies with complex tasks and high-quality standards have placed their trust in our broad national and international industry and technical know-how.

Artificial intelligence offers great potential for many companies and enables completely new business models. We have made it our mission to uncover this potential among our customers and to implement corresponding AI solutions. For our in-house further development, we carry out research projects in collaboration with renowned universities and non-university institutes in Austria.

ONTEC uses a Management System called Holacracy to organize itself. It provides flat hierarchy which allows ONTEC to be an agile and flexible company.

More information about holacracy and about the holacracy constitution can be found here:
https://en.wikipedia.org/wiki/Holacracy
https://www.holacracy.org/constitution/4-1/

2 Information security policies and organization of information security

Information Security, for ONTEC AG means, to protect confidentiality, integrity and availability and is a global objective for ONTEC AG. Therefore, it operates an Information Security Management System (ISMS). The execution and operational management of the ISMS objectives are achieved by Chief Information Security Officer (CISO) and all persons who fulfil a security relevant role. The information security steering group provides objectives and controls to improve organisation wide security.

Information security policies define objectives, procedures, periodic reoccurring tasks and processes to ensure and improve information security. All relevant documents subject to periodic reviews and updates to match the continuous changing environment, but all documents are reviewed at least once every three years. If needed documents can be updated on demand. All Policies define accountability and responsibility for implementing and maintaining security and privacy measures. To establish and communicate policies the predefined governance process as defined in the holacracy constitution is used. This ensures that all members of the organisation know which policies apply for them and how to comply with these policies.

Part of the ISMS is also to identify interested Parties and their needs and requirements towards ONTEC. Identified parties are customers, partner companies, owners, employees, executives, the public, competitors, contractors, distributors, and vendors. Another important interested party is the legislator. The ISMS ensures that legal requirements and compliance is respected throughout the company.

ONTEC keeps risks as low as possible, the organization avoids risk where possible and invests resources in mitigating risk through treatment. Risks are identified and reviewed periodically and countermeasures to risks are tracked through a treatment plan. Applied treatment also gets reviewed and it will be the decision of the Security Steering group to either accept the residual risk or apply another treatment if possible. To conquer risks effectively each risk has a risk owner responsible to provide the resources needed for mitigation. If chances can be directly linked to a risk the decision if the risk can be taken is part of quarterly held risk management meetings.

The criteria for assessing risk in the context of the organization's risk taking are defined in a dedicated ISMS document Risk Assessment and Treatment Process.

2.1 Mobile Devices and teleworking

ONTEC AG offers its employees different work options that include onsite and remote presence. For this reason, remote work is treated in a same way as onsite. Strict technical and security controls are implemented regardless of the location of the device. All ONTEC devices are fully encrypted and have a centrally managed endpoint security solution. Files are stored centrally on company hosted shares and a company hosted private cloud solution.

To ensure the security of teleworking, remote access security controls include a secure VPN connection. For Critical systems a second factor is necessary to connect. Mobile devices are managed through a Mobile device Management Solution. Employees are allowed to use a personal mobile device which needs to comply with the compliance policies configured in the MDM solution. Furthermore, all apps and access to company resources is only possible through a separated, locked workspace on the mobile device.

3 Human resources security

To ensure that ONTEC AG protects itself from any malicious intend through new hires, several Interviews are conducted before hiring. All candidates must provide proof of their education and/or certification. They also need to provide a clean criminal record. If any doubt persists former employers are contacted to get a better picture of the candidate. Besides security relevant matters, the personal and technical skillset and if they are a match for the existing team is also part of the decision.

After successful recruitment, new employees must sign the ONTEC AG terms of use. A non-disclosure agreement and a secrecy agreement are part of the contract of employment which needs to be signed as well. All these documents ensure that confidentiality, throughout and after the employment, is provided. To continuously improve security awareness regular events are held at ONTEC.

If Customer Projects require another level of secrecy, additional NDA Contracts are signed. ONTEC operates on a need-to-know base to keep distributed information as low as possible.

4 Asset management

All assets of ONTEC AG are listed in an inventory. Each asset has an owner who takes responsibility for the asset. All assets are classified into different types (i.e., physical, logical, or information assets) and into different roles (i.e., Client Hardware, Server Hardware, Appliance) For Client Hardware of any type, the user is the owner of the asset and therefore responsible. A terms of use policy ensures that User-Owned-assets are treated correctly. All other Assets are owned by a corresponding role (TAC) – the Technical Account Manager. This ensures that assets and their configuration are supported from the vendor and regularly updated.

A lifecycle is in place to ensure hardware support for all ONTEC AG devices. If the end of the lifecycle is reached devices are wiped and are available for sale to employees. Storage of any kind will be disposed through a professional service and the destruction is documented.

5 Access control

ONTEC follows the principles of need to know and least privilege in all layers of access control.

5.1 Physical access control

To prevent unwanted access to any resource onsite, the office location is broken down into different zones. The zones divide the space into a public area where the front desk is located as well as an office space and a restricted zone, all zones are physical separated from each other. External persons who wish to visit ONTEC must register when entering the premises and are obliged to wear a visible badge, and require a personal escort in special areas, while in the office.

5.2 Logical Access Control

To ensure that users only have access to what they need, formal processes for creation, registration, deregistration, and assignment of new rights are in place. All changes to existing rights are tracked and documented through tickets. All given rights are reviewed periodically, and findings are documented as well. If a user account is no longer used due to termination of business relationships, all access is revoked.

Users are responsible and are held accountable for safeguarding their authentication information. Secure logon procedures are implemented where required by the access control policy. Password systems require interactive logins for users. Procedures and technical controls are in place to ensure adequate quality passwords, following the leading best practise.

6 Cryptography

A key component in the set of defenses available to organizations to protect their classified information is the use of cryptographic techniques. ONTEC uses cryptography to protect:

- Confidentiality – ensuring that information cannot be read by a unauthorized person
- Integrity – proving that data has not been altered in transit or whilst stored.
- Authentication – proving the identity of an entity requesting access to resources.

- Non- repudiation – proving that an event did or did not occur or that a message was sent by an individual

These safeguards apply to all systems, people and processes that constitute the organization’s information systems who have access to ONTEC systems. The primary objective of cryptographic measures is protecting our data and services.

It is vital that cryptographic keys are protected from modification, loss, destruction, and unauthorized disclosure. There is a process over the entire life cycle that ensures that all phases are carried out properly.

Cryptographic methods and algorithms are chosen through the current best practice and are documented in detail in the cryptographic policy.

7 Operations security

To ensure correct and secure processing of information, operational tasks and procedures and responsibilities are implemented. Information security related risks are managed accordingly.

To provide structure, a change policy is in place. All changes are designed as the ITIL framework suggests and are documented in through the ONTEC ticketing system. Capacity Management guarantees that all members of ONTEC have enough resources. All resources are continuously monitored and adapted to meet both existing and future requirements.

All networks of ONTEC are segregated in different testing and production networks. The segregation controls work on different levels e.g., physical, virtual, and based on the user’s permissions assigned through our rights management. ONTEC Systems are hardened through best practises to achieve operation system level security.

To properly manage all entities of ONTEC a central time service is established, and all clocks are synchronized.

7.1 Anti-Malware

To provide protection against malware a central managed endpoint security solution is used at ONTEC. If a device is compromised or at risk a security incident will be logged, and it will be dealt with it according to the Information Security Incident policy. Security Awareness is spread in the organization through informational events, this further decreases the attack surface of ONTEC.

7.2 Backup and Recovery

Backup copies of information, software, and system images are taken and tested regularly in accordance with backup strategy and related policies. The objective is to ensure protection against the loss of data. Backup policies define the frequency of creating backups, appropriate security controls, and retention periods, taking into consideration the criticality and value of information and recovery point objectives. After the expiry of the backup retention period, information is securely deleted or disposed of.

7.3 Logging and Monitoring

All non-Client Infrastructure Components which grant access to any resource of ONTEC AG log these attempts no matter if these are successful or not. All produced logs are forwarded to a central Logging Cluster.

The collected Logs can provide insights for security and operative incidents. The Centralized Logging can also actively raise an incident. In Case of a security incident the logs can be compared with the original source to verify that they have not been tampered with.

All raised security incidents follow the information security incident process.

Any System where ONTEC AG is contractually bound with a Service Level Agreement needs to be actively monitored. This happens through a redundant Monitoring instance. All new machines get added to the monitoring through an automated creation mechanism.

Security Event Logs are collected on our centralized Log Management. High Log on Counts, suspicious changes to rights, creation of users or additions to privileged groups all get logged and alerted upon.

7.4 Vulnerability Management

Information about technical vulnerabilities regarding ONTEC systems is continuously monitored and processed. If ONTEC systems are exposed to a vulnerability the ranks severe or critical the information security incident policy and process are used as guideline to act upon the vulnerability.

Vulnerability identification methods include vulnerability scanners, penetration testing, abonnements of relevant security bulletins and alerts from CERT’s. All vulnerabilities are rated through the common vulnerability scoring system (CVSS) and are treated. Depending on impact and exposure, remediation is achieved as vulnerabilities are treated through a normal or an emergency change.

8 Network security

Networks are logically separated as often as possible in the ONTEC infrastructure, depending on their intended use. This means that we take care to separate clients from servers, guests from internal systems and development, production and customer systems from each other. All network communication is controlled fine granular by firewalls on all ONTEC sites.

If the creation of a network is required or changes to existing ones are needed, it needs to be documented. Therefore, all changes are done through the implemented Change Process. Risks regarding new networks are evaluated through a member of the information security team. Any Access to a network is part of the rights management process and follows a need-to-know practise.

9 System acquisition, development, and maintenance

Security requirements of information systems ensure that security and privacy are an integral part of information systems during their entire lifecycle.

The requirements for information security controls are included in the business and technical requirements for new information systems or development of existing information systems, taking into consideration all relevant criteria, risk, and sensitivity of a system, with detailed analysis of all publicly exposed systems.

Information publicly available via public-facing services are protected from fraudulent activity, modification of information involved incomplete transmission, routing errors, unauthorized message duplication, or message replays.

10 Information security incident management

To ensure a quick, effective, and orderly response to information security incidents, an information security policy is in place. This policy provides a guideline which assists in the response to an information security incident.

The objectives the policy provides are:

- concise overview of how ONTEC AG will respond to an incident affecting its information security.
- responsibilities who will respond to an incident and their roles and responsibilities.
- describe the facilities that are in place to help with the management of the incident.
- definitions of how decisions are made in relation to our response to an incident.
- explain how communication within the organization and with external parties will be handled.
- provide contact details for key people and external agencies.
- define what will happen once the incident is resolved.

11 Business continuity management

Information security continuity is always embedded within business continuity management (BCM) to ensure the protection of information and systems and to anticipate and prepare for harmful events.

Plans are developed to ensure management in unfavourable situations (e.g., in the event of a crisis or disaster); all plans developed include an information security perspective. Processes, procedures, and controls are developed and implemented that guarantee the required level of continuity for information security during an adverse situation. Verification, review, and testing of continuity plans are conducted periodically or in the event of changes in the environment, to ensure that the plans are valid and effective during adverse situations.

12 Compliance

Management of information security and the implementation of related processes, policies, and procedures are independently reviewed at predefined intervals or when significant changes relevant to security and privacy domains occur.

Reviews also include an inspection on a technical level assessing the effectiveness and efficiency of technical measures. To ensure compliance with legislative, regulatory, and contractual requirements, processes for identification and monitoring of applicable legislation and contractual requirements are implemented.

Legal and contractual compliance includes the management of the intellectual property. Legal documentation and related records are protected from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with applicable regulatory and business requirements.