Operations Security Policy

Policy Owner: Pedro Piñera Buendía

Effective Date: Oct 16, 2024

Purpose

To ensure the correct and secure operation of information processing systems and facilities.

Scope

All Tuist GmbH information systems that are business critical and/or process, store, or transmit company data. This Policy applies to all employees of Tuist GmbH and other third-party entities with access to Tuist GmbH networks and system resources.

Documented operating procedures

Both technical and administrative operating procedures shall be documented as needed and made available to all users who need them.

Change management

Changes to the organization, business processes, information processing facilities, production software and infrastructure, and systems that affect information security in the production environment and financial systems shall be tested, reviewed, and approved prior to production deployment. All significant changes to in-scope systems and networks must be documented.

1. Change Documentation and Review:
    - All significant changes to systems, networks, and processing facilities must be documented.
    - The documentation must encompass the change's purpose, specification, potential impact considering dependencies, and deployment plan.
    - Changes should be tested and reviewed in environments segregated from both production and development (e.g., staging environments).
2. Approval and Authorization:
    - Changes with substantial impact on information security and operational functionalities, must obtain formal authorization before deployment.
    - Emergency changes may be expedited but must undergo a retrospective review and authorization.
3. Change Management Procedures:
    - Planning and Impact Assessment: Evaluate potential impacts of the changes considering system dependencies.
    - Authorization: Secure necessary approvals before initiating changes
    - Communication: Inform relevant internal and external stakeholders about the planned changes, schedules, and expected impact in advance.
    - Testing and Quality Control: Ensure changes are tested thoroughly (refer to section 8.29 for testing and acceptance specifics) and meet quality standards before implementation.
    - Implementation and Deployment: Execute changes in alignment with the planned deployment schedule
    - Emergency Management: Remediation: If changes fail or present unexpected issues, they shall be reverted
    - Documentation Maintenance: Ensure that the ticketing systems or the code repository platform keeps record of changes, commits and deployments.
4. Continuity and Consistency:
    - Ensure that the ICT continuity plans, response, and recovery procedures are updated to remain appropriate and consistent with the changes made.
    - Ensure operating documentation and user procedures are modified and remain suitable.
5. Security and Integrity:
    - Ensure that changes preserve and do not compromise the confidentiality, integrity, and availability of information in processing facilities and systems.

Capacity management

The use of processing resources and system storage shall be monitored and adjusted to ensure that system availability and performance meets Tuist GmbH requirements.

Human resource skills, availability, and capacity shall be reviewed and considered as a component of capacity planning and as part of the annual risk assessment process.

Scaling resources for additional processing or storage capacity, without changes to the system, can be done outside of the standard change management and code deployment process.

Data leakage prevention

In adherence to this Data Leakage Prevention Policy, and in order to minimize the risk of leakage of sensitive information, the organization shall:

- Identify and classify information in accordance with the *Data Management Policy*
- Provide awareness training to users including the appropriate use and handling of sensitive information

Consider the use of technical monitoring and Data Loss Prevention (DLP) tools in accordance with the risks to the organization and data subjects.

Web filtering

The organization shall ensure safe, secure, and appropriate internet use by the organization's personnel.

Website Access and Blocking:

- Implement mechanisms, such as secure DNS and IP address or domain blocking, to restrict access to websites that pose a substantial risk due to their content or known distribution of malware, viruses, or phishing materials.
- Employ browsers and anti-malware technologies capable of automatic website blocking or configuration for the same.
- Unless justified by legitimate business reasons, consider blocking access to websites with:
    1. Information upload capabilities.
    2. Known or suspected malicious content.
    3. Act as command and control servers.
    4. Identified as malicious through threat intelligence.
    5. Sharing of illegal content.

Usage Rules and Guidelines:

- User shall conform to all company rules in accordance with the Code of Conduct and the Acceptable Use Policy found in the *Information Security Policy.*

Separation of development, staging and production environments

Development and staging environments shall be strictly segregated from production SaaS environments to reduce the risks of unauthorized access or changes to the operational environment. Confidential production customer data must not be used in development or test environments.

Refer to the *Data Management Policy* for a description of Confidential data. If production customer data is approved for use in the course of development or testing, it shall be scrubbed of any such sensitive information whenever feasible.

Systems and network configuration, hardening, and review

Systems and networks shall be provisioned and maintained in accordance with the configuration and hardening standards described in Appendix A to this policy.

Firewalls and/or appropriate network access controls and configurations shall be used to control network traffic to and from the production environment in accordance with this policy.

Production network access configuration rules shall be reviewed at least annually. Tickets shall be created to obtain approvals for any needed changes.

Protection from malware

In order to protect the company's infrastructure against the introduction of malicious software, detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Anti-malware protections shall be utilized on all company-issued endpoints except for those running operating systems not normally prone to malicious software. Additionally, threat detection and response software shall be utilized for company email. The anti-malware protections utilized shall be capable of detecting common forms of malicious threats and performing the appropriate mitigation activity (such as removing, blocking or quarantining).

Tuist GmbH should scan all files upon their introduction to systems, and continually scan files upon access, modification, or download. Anti-malware definition and engine updates should be configured to be downloaded and installed automatically whenever new updates are available. Known or suspected malware incidents must be reported as a security incident.

It is a violation of company policy to disable or alter the configuration of anti-malware protections without authorization.

Information backup

The need for backups of systems, databases, information and data shall be considered and appropriate backup processes shall be designed, planned and implemented. Backup procedures must include procedures for maintaining and recovering customer data in accordance with documented SLAs. Security measures to protect backups shall be designed and applied in accordance with the confidentiality or sensitivity of the data. Backup copies of information, software and system images shall be taken regularly to protect against loss of data. Backups and restore capabilities shall be periodically tested, not less than annually.

Backups must be stored separately (using a logical database backup) from the production data location.

Tuist GmbH does not regularly backup user devices like laptops. Users are expected to store critical files and information in company-sanctioned file storage repositories.

Backups are configured to run daily on in-scope systems. The backup schedules are maintained within the backup application software.

A backup restore test should be performed at least annually to validate the backup data and backup process.

Logging & monitoring

Production infrastructure shall be configured to produce detailed logs appropriate to the function served by the system or device. Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and reviewed through manual or automated processes as needed. Appropriate alerts shall be configured for events that represent a significant threat to the confidentiality, availability or integrity of production systems or Confidential data.

Logging should meet the following criteria for production applications and supporting infrastructure:

- Log user log-in and log-out
- Log CRUD (create, read, update, delete) operations on application and system users and objects
- Log security settings changes (including disabling or modifying of logging)
- Log application owner or administrator access to customer data (i.e. Access Transparency)
- Logs must include user ID, IP address, valid timestamp, type of action performed, and object of this action.
- Logs must be stored for at least 30 days, and should not contain sensitive data or payloads

Protection of log information

Logging facilities and log information shall be protected against tampering and unauthorized access.

Administrator & operator logs

System administrator and system operator activities shall be logged and reviewed and/or alerted in accordance with the system classification and criticality.

Data restore logs

In the event the company needs to restore production data containing PII from backups, either for the purposes of providing services or for testing purposes, shall be logged or tracked in auditable tickets.

Clock synchronization

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to network time servers using reputable time sources.

File integrity monitoring and intrusion detection

Tuist GmbH production systems shall be configured to monitor, log, and self-repair and/or alert on suspicious changes to critical system files where feasible.

Alerts shall be configured for suspicious conditions and engineers shall review logs on a regular basis.

Unauthorized intrusions and access attempts or changes to Tuist GmbH systems shall be investigated and remediated in accordance with the *Incident Response Plan*.

Control of operational software

The installation of software on production systems shall follow the change management requirements defined in this policy.

Threat intelligence

Information relating to information security threats should be collected and analyzed to produce threat intelligence.

Collection: Draw from diverse sources, such as blogs, news articles, vendor updates, public databases, and industry communities.

Analysis: Examine the data to derive actionable insights and enable proactive response initiatives. Report any actionable insights or specific threats to the Security Team.

Dissemination: Ensure effective communication of threat intelligence to pertinent teams for effective action. The Security Team shall disseminate actionable information via communication channels, such as slack, email and emergency alerts.

Feedback: Cultivate continuous improvement by leveraging feedback for policy enhancements. Integrate feedback into policy amendments and conduct regular policy reviews.

Technical vulnerability management

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities shall be evaluated, and appropriate measures taken to address the associated risk. A variety of methods shall be used to obtain information about technical vulnerabilities, including scanning and vendor alerts.

Vulnerability scans shall be performed on public-facing systems in the production environment at least quarterly.

The IT and Engineering departments shall evaluate the severity of vulnerabilities identified from any source, and if it is determined to be a risk-relevant critical or high-risk vulnerability, a service ticket will be created. The Tuist GmbH assessed severity level may differ from the level automatically generated by scanning software or determined by external researchers based on Tuist GmbH's internal knowledge and understanding of technical architecture and real-world impact/exploitability. Tickets are assigned to the system, application, or platform owners for further investigation and/or remediation.

Vulnerabilities assessed by Tuist GmbH shall be patched or remediated in the following timeframes:

Determined Severity	Remediation Time
Critical	30 Days
High	30 Days
Medium	60 Day
Low	90 Days
Informational	As needed

Service tickets for any vulnerability which cannot be remediated within the standard timeline must show a risk treatment plan and planned remediation timeline.

Restrictions on software installation

Rules governing the installation of software by users shall be established and implemented in accordance with the Tuist GmbH *Information Security Policy.*

Information systems audit considerations

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

Systems security assessment & requirements

Risks shall be considered prior to the acquisition of, or significant changes to, systems, technologies, or facilities. Where requirements are formally identified, any relevant security requirements shall be included. The acquisition of new suppliers and services shall be made in accordance with the *Third-Party Management Policy*.

The company shall perform an annual network security assessment that includes a review of major changes to the environment such as new system components and network topology.

Data masking

Tuist GmbH will implement data masking based on risk or a specific requirement to do so.

Techniques Guidance:

- Adopt appropriate techniques such as data masking, pseudonymization, or anonymization to protect PII and other sensitive data effectively.
- Guarantee that pseudonymization and anonymization methods effectively break the link between PII and individuals or sensitive data elements.
- Confirm all elements of the information are considered for adequate data anonymization.
- Employ additional data masking methods, such as encryption, character nulling/deleting, varying numbers and dates, substitution, and replacing values with their hashes.

Data Masking Considerations:

- Design data queries and masks to disclose only the minimally required data to users, safeguarding privacy and security.
- Develop mechanisms for data obfuscation, considering specific circumstances under which certain data should be concealed from users.
- Provide options for PII principals to control the visibility of their obfuscated data and adhere to any applicable legal or regulatory requirements related to data masking.

Using Data Masking, Pseudonymization, or Anonymization:

- Determine the suitable strength level, access controls, user agreements, and usage restrictions for processed data.
- Prevent the combination of processed data with other information to identify PII principals and ensure traceability of provided and received processed data.

Exceptions

Requests for an exception to this policy must be submitted to the IT Manager for approval.

Violations & enforcement

Any known violations of this policy should be reported to the IT Manager. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version history

Version	Date	Description	Author	Approver
1.0	Oct 16, 2024	Version 1.0	Pedro Piñera Buendía	Pedro Piñera Buendía

APPENDIX A - Configuration and hardening standards

Servers and Virtual Machines

This is the standard for system-level server and virtual server (VM) configuration hardening. Some customization to these settings may be required to configure the system for its specific target environment, such as setting the proper names, groups, authentication settings, and other personalization options.
In addition all physical and virtual systems must adhere to the following technical requirements:

- All vendor default passwords (including default passwords on operating systems, software providing security services, application and system accounts, Simple Network Management Protocol (SNMP) community strings, etc.) must be changed before a system is installed on the network.
- Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, SNMP, etc.) must be removed or disabled before a system is installed on the network.
- Only one primary function may be implemented per server or virtual machine to prevent functions that require different security levels from coexisting on the same system.
- Only necessary services, protocols, daemons, etc., may be enabled, and only as required for the function of the system. All unnecessary functionality (such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers) must be disabled.
- All security patches identified as critical, high, or medium must be applied to systems within SLAs established in this policy.
- Ensure systems are aligned with industry-standard baselines (CIS Benchmarks, NIST Guidelines).

Technical Adherence

- Vendor Defaults: All default configurations, especially passwords, must be altered prior to network integration.
- Role Specialization: Maintain a singular primary function per VM to uphold segregation of duties and reduce lateral movement opportunities.
- Patch Management: Establish a patch management strategy to meet defined SLAs.

Network Standards

- Management of network rules and settings may only be performed by authorized members of the Engineering team and all changes must comply with change Management procedures defined in the Operations Security Policy.
- Supported network controls for production networks are firewalls and network access control lists (NACLs). Management of production network systems is accomplished through the use of a centralized configuration management system and secure access protocols.
- In the production environment, defined rules and configurations must be enforced to control traffic from untrusted networks (e.g. publicly available services) to internal production networks.
- Network control systems must be configured to use default Network Address Translation to prevent the disclosure of internal IP addresses to the Internet.
- Mobile devices connecting to production networks must meet the requirements of the Mobile Device Policy found in the Information Security Policy.
- All network control systems must be configured with default antispoofing rules to block or deny inbound internal addresses originating from the Internet.
- External configurations must limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
- Use of insecure services and protocols without justification and documentation of additional security features implemented to mitigate risk is prohibited.
- Remote access sessions must be configured to enforce timeout after a specified period of 2 hours.
- Remote-access technologies for vendors and business partners used to access production systems must be enabled only when needed for business purposes and immediately deactivated after use.
- Any hybrid networks with both cloud and on-premise access shall be scanned and tested at least annually to ensure that security requirements are maintained.
- Change Management: Any alterations to network settings must adhere to the change management processes.

Traffic Management in Production Environments

- Rule Enforcement: Strictly enforce predefined rules, which should be revisited and validated at least annually.
- Remote Access Control: Ensure strict control and auditing of remote access, restricting and logging all connections.

NACLs and Traffic Control

- Establish stringent rules governing traffic in accordance with a define business justification

Cloud Hardening

Identity and Access Management (IAM)

- Least Privilege Principle: Ensure each entity (user, service, system) possesses minimal necessary access.
- Enforce Multi-Factor Authentication (MFA) for production access

Data Storage and Management

- Data Encryption: Ensure encryption for data at rest and in transit in accordance with the Cryptography Policy
- Private Endpoints: Enable private endpoints and VPNs to safeguard against data interception.
- Data Lifecycle Management: Configure backups for customer data repositories.

Network Security

- Isolation: Utilize VPC and subnets to isolate environments and segment networks.
- Firewalls: Implement cloud-native or third-party firewall solutions and DDoS protection services.

Monitoring and Logging

- Logging: Configure logging focusing on write-once-read-many storage to prevent tampering.
- Alerting: Implement cloud-based alerting (Amazon CloudWatch, Azure Alerts) for real-time incident response.

Container Hardening

Image Security

- Secure Source Image: Create images only from Tuist GmbH-authorized base images or repositories
- Minimalist Design: Adopt minimal base images to reduce attack vectors.

Runtime Security

- Runtime Analysis: Implement runtime security tools for live vulnerability and threat detection.

Network Security

- Policy-Based Controls: Implement network policies using third party or cloud native tools.

Orchestration Security

- API Server: Shield the API server with appropriate firewalls, IAM controls, and secure communication channels.
- RBAC: Establish and periodically review orchestration access privileges, ensuring conformance to the least privilege principle.

CI/CD Security

- Dependency Scanning: Scan for vulnerable dependencies during build processes