INFORMATION SECURITY POLICY FOR SUPPLIERS

IMEC VZW

Table of contents

Definitions

Imec Information (also referred to simply as "Information"): encompasses all information, regardless of its form or medium, created, generated, collected, stored, processed, received, used, or transmitted by imec. Imec Information can be in electronic or non-electronic form and includes but is not limited to documents, images, videos, audio files, databases, emails, and any other form of knowledge. Imec Information may be public, restricted, confidential, or strictly confidential, it may be structured or unstructured and can originate from internal or external sources such as Suppliers, partners, customers, or other external parties. It covers both tangible and intangible information, including intellectual property, proprietary business insights, trade secrets, financial records, personal data of employees and customers, and any other material that is pertinent to imec's operations, legal obligations, and strategic objectives.

Supplier: within the scope of this policy, "Supplier" refers to any entity, organization, or individual that is not part of imec, that may come into contact with or have access to imec Information, regardless of the nature or duration of their engagement with imec. This includes but is not limited to vendors, contractors, subcontractors, consultants, service providers, business partners, or agents of another party that has a business relationship with imec, whether through contractual agreements, partnerships, or other formal arrangements.

Abbreviations

- IDS: Intrusion Detection System - is an automated system that detects/monitors a network or systems for malicious activity or policy violations and alerts an administrator or security information & event management system.
- IPS: Intrusion Prevention Solution – is a security device that can monitor network and/or system activities for undesirable behavior. An IPS can react autonomously in real time to security events by blocking or preventing such activities.
- MFA: Multi-Factor Authentication - is a security enhancement that allows you to present an additional authentication factor when logging in to an account to confirm and verify your identity.
- NDA: Non-Disclosure Agreement – also known as e.g. a confidentiality agreement, is (part of) a legal contract between (at least) two parties that outlines confidential material/knowledge/information that both parties wish to share with one another for certain purposes, but for which they desire to restrict access to.
- RACI - Responsible, Accountable, Consulted, Informed, a manner to assign responsibilities for activities. More details are listed in section 3.5.
- RTO – Recovery Time Objective – is the maximum acceptable amount of time for restoring a network or application and regaining access to data after an unplanned disruption.
- SLA - Service-Level Agreement - is an agreement between 2 parties, i.e. a service provider and a customer. Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user.

1 Purpose

Suppliers may have access to Imec Information during their business engagements with imec. The purpose of this information security policy (hereinafter the "Policy") is to outline the different technical & organizational measures that Suppliers must implement to maintain the confidentiality, integrity, and availability of imec's assets and to safeguard them against unauthorized access, disclosure, alteration, or destruction.

It is the responsibility of the Supplier to ensure that relevant employees have read and understood the requirements of the Policy.

2 Scope

This Policy applies to all Suppliers that are engaged through contractual agreements with imec, covering every service outlined in such contracts. This document complements, without superseding, other Supplier obligations that may arise, e.g., from contracts or other agreements with imec, laws & regulations that apply to Supplier or imec, imec's information, etc.

If this Policy would conflict with any contractual agreement between imec and the Supplier, the contractual agreement shall prevail.

The Supplier will not subcontract or delegate any of its obligations listed in this Policy to any subcontractor or delegate without imec's prior written consent. The Supplier remains solely responsible for fulfilling and ensuring that any employees, subcontractors, or delegates adhere to the security requirements stipulated in this Policy.

Regarding subcontractors, the Supplier must:

- subject its subcontractors with access to Imec Information to a risk assessment with regards to information security and take risk remediating measures where required to ensure the subcontractors are compliant with this Policy.
- ensure that contractual agreements with its subcontractors and cooperation partners maintain an appropriate level of information security, consistent with the standards outlined in this Policy.

3 Policy

3.1 Principles

3.1.1 Roles & Responsibilities

The Supplier must:

- implement and uphold all security requirements listed in this Policy. Suppliers with an established information security management system (ISMS) compliant with leading industry practices which imec recognizes (i.e. ISO/IEC 270001), with a scope that covers the subject of the contractual agreement, shall provide their certification, with scope statement and shall communicate to imec when the ISMS doesn't comply to the standard anymore.
- implement, maintain, and monitor all controls highlighted in this Policy and report periodically upon their effectiveness within their organization.
- assign roles and responsibilities concerning information security to individuals within their organization - starting with (at least) a responsible for information security.
- ensuring "segregation of duties" to avoid conflicts of interest.
- establish ownership and individual accountability for information and systems and their corresponding security controls, in a RACI matrix.

- agree with imec on the geographical locations and countries where Imec Information can be stored and processed.
- take the necessary measures to safeguard Imec Information and ensure that all applicable regulations and legislations are adhered to.

Imec and Supplier shall have periodical meetings to discuss both the service performance (service level agreements), relevant security topics and risks. The meeting and meeting outcome will be documented and sent to the security representative of both imec and Supplier.

3.1.2 Human Resource Security

The Supplier must:

- submit employees with access to Imec Information to a background screening in line with applicable laws and legislation.
- ensure that employees are aware of and comply with their labor agreement and the information security requirements of this Policy when handling Imec information.
- enforce this Policy and any applicable non-disclosure agreement (NDA) between Supplier and imec with employees and subcontractors who have access to Imec Information.
- provide a comprehensive security awareness training program and regular updates (e.g., on new risks, procedures, and policies) to all employees, contractors, and third-party users with access to Imec Information to make sure they are aware of and comply with the expected security behavior of this Policy. The training shall be tailored to everyone's role, starting from their first day.
- ensure that the responsible staff is adequately trained on information security.
- Implement and enforce a clear desk and screen policy and communicate and enforce this policy upon all employees, subcontractors, or delegates.

3.2 Secure Setup

3.2.1 Provisioning of Resources & Asset Management

The Supplier must:

- only process and handle Imec Information using software from reputable, secure, and trusted sources.
- keep applications or operating systems supported and up to date.
- prohibit and prevent the use of unauthorized assets for the transmission, accessing, storing, or processing of Imec Information.
- protect Imec Information, which is stored in physical form, implementing, and using security controls such as a clean desk and screen policy, secure printing, locked storage space, watermarking, etc.
- ensure that Imec Information is assigned information classification labels which reflect the imec classification levels and is handled and protected in accordance with their information classification label.
- assess the Imec information classification levels and ensure that employees are aware of the differences between the classification levels of imec and the Supplier (if present) and ensure the information is managed in line with imec requirements.
- manage, maintain and safeguard Imec Information as indicated in the Supplier policy.
- destroy or return (Imec Information upon contract termination, in line with exit agreements made with imec.
- confirm the deletion of all Imec Information in writing by e-mailing ciso@imec.be after its destruction. Imec will retain this confirmation in its systems for audit purposes.

3.2.2 Network Security

The Supplier must:

- protect Imec Information and systems by restricting unauthorized network access, especially from the external Internet.
- implement defense-in-depth principles such as e.g. network segregation and physical access controls to network equipment using effective network security solutions, such as a firewall, intrusion prevention solution (IPS) or intrusion detection system (IDS) and monitoring solutions, and maintain these solutions, to protect Imec Information at all times.
- implement technologies preventing the intrusion of the network and detect & prevent malicious or unauthorized traffic from entering the network.
- implement security controls to protect transferred information from interception, copying, modification, misrouting, and destruction.
- limit logical access to and between networks as indicated in the section "Identity and Access Management".
- enforce multi-factor authentication (MFA) on remote connection to Imec Information

The Supplier should:

- ensure that all ICT systems that contain Imec Information and are operated by the Supplier (or its sub-contractor) have security measures in place to prevent lateral movement of threats within the network of the Supplier.
- execute regular maintenance activities on network equipment (e.g. health checks, hardening, patching, Vulnerability scanning and change management).
- establish a secure configuration baseline to allow traffic to flow through network devices and disable unnecessary or unused services and ports on network devices and enforce it. The Supplier validates periodically if the device is still compliant with the security baseline and acts accordingly.
- ensure that any servers used to provide the service to imec are only deployed on trusted networks with appropriate security controls.
- perform regular out of band network scans to detect any (possible) unauthorized connections. Communications between devices and management stations/consoles must be secured as well.
- annually review both internal and external firewall rules and ensure that access to the internal network is monitored. Only authorized devices must be allowed through appropriate network access controls.

3.2.3 Identity & Access Management

The Supplier must:

- assign each user a unique user ID, which can be traced back to one unique individual. The usage of shared user accounts to access Imec Information is prohibited, unless explicitly approved by imec.
- restrict access to Imec Information in line with the following principles: need-to-know, need-to-have, least privilege and while considering segregation of duties.
- implement, maintain, and enforce strong access controls to secure information assets, based on best practices.
- ensure that users use a strong and complex password, in line with imec's password requirements and multi-factor authentication for at least remote connections. Passwords must never be communicated in clear text nor together with the account credentials.

- change default passwords or vendor provided password in operating systems during the system/product installation & initial configuration.
- block and investigate multiple failed authentication attempts – When this occurs, the account must be blocked and only be reinstated after verification.
- implement and use a process to reset passwords in a secure way. The process includes provisions for positive identification of the requester.
- appoint an information asset owner who is accountable for granting and maintaining access to employees (Joiner/Mover/Leaver).
- must review access rights to imec information periodically.
- revoke remote and/or physical access rights to imec information when the user has no valid business reason anymore to access Imec Information. This should take place within 24 hrs. of the announcement of the notice period.
- review all privileged access permission at least annually. The frequency of this review should consider the sensitivity and risks related to the privileged account (e.g. source code).
- restrict access to administrator interfaces to only privileged users. Access is based on individual user authentication, with business motivation. No general user should have access to these privileged interfaces.

3.3 Protect

3.3.1 Physical Security

The Supplier must:

- ensure the implementation and management of the physical security controls at their facilities, information processing locations and datacenters where Imec Information or assets are processed or stored.
- implement physical entry controls that allow only authorized personnel to enter restricted or non-public zones where imec's restricted of (strictly) confidential information is present. An owner must be appointed to manage the list of authorized personnel to these zones.
- grant access through access control systems that have no known vulnerabilities. If there are risks or vulnerabilities known, the Supplier must take risk remediating measures.
- take adequate measures at its (office) locations to prevent threats to the physical integrity or availability of infrastructure, such as back-up power sources, protection of cabling, smoke, heat, and humidity sensors. (Note: this is a non-exhaustive list).
- ensure that information & assets cannot be removed from their security zone, unless authorized and with the necessary adequate protection measures, which depend on the information classification level.

For information processing facilities and datacenters, the Supplier takes the following measures:

- access to these zones must be limited as much as possible and be requested in advance, with a clear motivation/business reason and be approved by the individual responsible for the restricted zone.
- The selected datacenter must be tier 3 or higher, depending on the availability requirements stipulated in the contractual agreement.
- host Imec Information only in datacenters which have a valid ISO 27001 certification and SOC 2 certification for security management (or similar certifications that demonstrate a resilient security organization audited by an independent auditor).
- the datacenter of information processing facilities should be resilient to withstand physical threats such as fire, flooding, power disruptions, etc. using fire/smoke alarms & extinguishers, humidity sensors and elevated floors, uninterruptable power

supply, etc.

3.3.2 Application, Infrastructure & Network Monitoring

The Supplier must:

- ensure resource capacity for systems and network devices so they can accommodate current and future business requirements.
- ensure that systems (incl. applications), servers, security devices and network equipment log (key) events (e.g. events with an impact on confidentiality, integrity, or availability of services)
- regularly review access logs for signs of malicious behavior or unauthorized access.
- regularly review system and network logs for anomalies or malicious behavior.
- provide (when requested by imec) logs about the use of accounts used to access imec information, and logs about the impersonation of, or attempt to impersonate, individuals with access to imec information.
- retain imec information or log information only for the purpose of its intended & permitted purpose. The retention period for logs is 180 days, but exceptions are possible, considering the intended and permitted purpose.

The Supplier should:

- analyze logs (centrally) and appropriately secure them. These logs should be used as well by the Supplier's incident response capability for identifying or investigating incidents or breaches related to Imec Information.
- store the logs in an appropriate and secure manner, with (amongst other) controls to prevent the alteration or deletion of log files and access restrictions for administrators of the system the logs are from.
- have automated controls deployed which primary purpose is to identify and block suspicious emails to prevent malware infections and respond appropriately.

3.3.3 Operational Security

The Supplier must:

- apply changes to production systems in a controlled manner. Software should be installed on operational systems following a change management process.
- maintain separate environments for production and non-production systems to avoid unauthorized access or changes to the environment.
- implement anti-malware software or an equivalent security control to mitigate the risk of malware compromise and spread. If used, the Supplier will keep the anti-malware software up to date.
- ensure that anti-virus software is installed on user endpoints, network ingress and egress locations, and servers. The anti-virus software must be updated frequently and receive daily virus signature updates from a trusted & reputable source.
- maintain the systems that contain Imec Information and ensure they are up to date with the latest upgrades, updates, bug fixes, and new versions and with any other modifications necessary to ensure security of imec information.
- test its security systems regularly to validate whether they meet the requirements of this policy or of the contractual agreement.

The Supplier should:

- respond to cyber-attacks (such as malware and/or viruses) and initiate corrective and mitigating actions to reduce impact and recover from the threat.
- periodically subject the applications, systems, and networks where imec information resides to a vulnerability scan. Detected vulnerabilities must be remediated without

undue delay.

- test all patches first in an environment of which the configuration mirrors the target environment (production) to ensure that successfully tested changes are introduced into the production environment.
- perform post-implementation testing to ensure the successful implementation of patches and the operation of the system/software/application.
- deploy appropriate countermeasures if a system cannot be patched. The Supplier will inform imec in writing of the risk and remediating measures.

3.3.4 Secure development & maintenance

The following section is only applicable for Suppliers which perform development activities on behalf of imec, within an imec ICT environment.

The Supplier must:

- develop and implement code in a secure environment using imec coding standards or standards which are based on industry standards and best practices (e.g. OWASP).
- store created code in a secure repository where it is protected from being modified or altered without authorization.
- prohibit storing production data or restricted or (strictly) confidential Imec Information in non-production environments.
- test code for security flaws prior to promoting it to production.
- ensure that all development activities occur in an environment separate from the production environment.

The Supplier should:

- not grant developers unmonitored access to production environments.
- implement segregation of duties for production and non-production environments.
- apply static and dynamic analysis tools to verify that secure coding practices are being adhered to.

3.3.5 Encrypt

The Supplier must:

- ensure proper and effective implementation and use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
- encrypt Imec Information both at rest and in transit using modern encryption techniques and in accordance with industry best practices.
- not use encryption protocols that have publicly known vulnerabilities which could be exploited.
- use cryptographic controls in agreement with existing legal, regulatory, and contractual requirements.

The Supplier should:

- evaluate the encryption method periodically for its adequacy and opt for strong encryption techniques. Operational and performance impact should be considered as well.
- procure certificates from reputable, approved, and vetted Certificate Authorities (CA).
- manage cryptographic keys using a key management system, governing generation, issuance, distribution, storage, changing, revocation, recovery, backup, destruction, logging, authorized use, authorized access, and auditing.

3.3.6 Incident Response

Imec will provide a contact for incident response activities and is responsible for making decisions on actions to resolve incidents concerning imec network, systems, or data, including forensic activities such as gathering of evidence (if needed).

The Supplier must:

- provide contact details for its security operation center or point of contact for reporting security incidents (both during and outside of business hours).
- Periodically perform (preferably with an independent qualified security provider) an IT security assessment / threat simulation covering IT infrastructure including disaster recovery site and all applications/systems which store or process imec information.
- inform imec without delay of (suspected) security incidents concerning: imec data, systems used to provide services to imec, or system/application managed by imec. The Supplier will support imec throughout the evaluation process for incidents, such as providing logs or additional information to determine the root cause of an incident.
- communicate relevant identified risks to imec and address them in an effective manner, in agreement with imec. If a risk related to the subject of the contract cannot be remediated or sufficiently reduced by the Supplier, the Supplier notifies imec within a reasonable timeframe, as agreed upon in the service level agreement.

3.4 Audit & Compliance

- In case the Supplier cannot comply with one or more security requirements listed in this Policy, the Supplier must communicate this, as well as the risk(s) and/or security issue(s) which could have an impact on imec's information and/or ICT environment,
- infrastructure or data, to imec's information security team in writing via ciso@imec.be .
- The Supplier must provide imec with proof that it attains an adequate information security level, in line with the protection needs of Imec Information. This can be done by communicating results of certification audits or attestations.
- Supplier shall provide Imec, external auditors with a legitimate interest or competent regulatory authorities access to any relevant information to perform a security audit of any site, system, software, or other product used by the Supplier or its subcontractors in the performance of the services and to review Supplier's compliance with its obligations under its assignment.
- Imec will announce this audit, via written notice, minimum 10 business days ahead (or less if requested by competent regulatory authorities).
- Imec will be allowed to perform such an audit once a year (unless the request is initiated by an external auditor or competent regulatory authority), or after each occurrence of an information security incident. The Supplier shall fully co-operate with the audit and provide all assistance and accesses reasonably requested by imec in relation to any such audit.
- If failed controls are identified during an audit, imec will perform a risk assessment and will specify the timeframe within which the risk should be remediated. The Supplier must complete the remediation actions within the predetermined timeframe.
- If significant findings of non-compliance are identified, imec reserves the right to perform a follow-up audit to confirm the remediation of the findings.
- The Supplier will implement information security requirements, in relation to all relevant legislative, statutory, regulatory, and contractual requirements. Next to that,

the Supplier performs periodical security reviews of systems to validate compliance with the security requirements listed in this document. When control fails, the Supplier informs imec and proposes a remediation plan.

- If services are subcontracted by Supplier, Supplier shall impose the compliance and audit requirements listed in this security policy on its subcontractors.

3.5 Roles & Responsibilities

Roles and responsibilities between the Supplier and imec must be clearly allocated. Shared responsibilities must be avoided unless no other option is viable and must be documented.

The following table defines RACI concept and provides an example in the table below.

Description		
R	Responsible	People or stakeholders who do the work.
A	Accountable	Stakeholder who is the "owner" of the work and delegates work to the "responsible". This individual must sign off or approve when the task, objective or decision is complete.
C	Consulted	People or stakeholders whose input is requested before the work can be done (typically subject matter experts). These people are "in the loop" and active participants.
I	Informed	People who are kept up to date on progress or decisions.

Task / Activity	Imec	(C)ISO/PM*	External Provider	…
Report on performance of the delivered service, reference to SLA/RTO	C	A	R	
Report on security events/incidents that could affect directly or indirectly the service delivery	C	A	R	
Report on changes that could affect the service delivery or the security/protection of the processed data	C	R	A	
Report on access management of accesses to client work environment (physical and digital)	C	A	R	
Commit to respond and fulfil third-party risk assessments/audits		R	A	
Commit to mitigate or justify identified risks from assessments/audits and provide update on status	C	R	A	

*Note: the (C)ISO role is the information security responsibility assigned at Supplier side.

Classification	Description	Example	Consequences of loss	Sharing Restrictions	Protective measures
Public information	Information intended and designed to share with the public has no negative impact when disclosed.	Marketing materials, approved media releases, presentations given at public conventions, etc.	No negative consequences on imec's turnover or revenue, its intellectual property, its reputation, or level of trust from its partners.	None	None
Restricted information	Information that has no or only minor negative impact if inappropriately or unintentionally disclosed	imec internal communications	A breach does not result in financial damage, loos, or trust from partners, nor reputational damage. Unauthorized disclosure of this information would be inappropriate or inconvenient to imec or its partners.	Must only be shared on need-to-know basis	Additional requirements: visibly assigned label, storage location must have access controls, access to be reviewed every 2 years, disposal of information based on contractual agreements
Confidential information	Information which has significant negative impact if inappropriately or unintentionally disclosed	Contracts, project information, financial reporting, information covered under an NDA, trade secrets, HR information, sales conference presentations, BSC, KPI's, etc.	The information is sensitive for imec and/or its partners. A breach results in significant financial damage to €10 M euro, loss of trust from partners, lawsuits/penalties, loss of intellectual property and/or reputation.	Must be covered by an NDA prior to sharing with third parties.	Additional requirements: Physical copies to be shredded or disposed via confidentiality container, access review to be performed yearly
Strictly confidential information	Information which leads to a critical negative impact if inappropriately or unintentionally disclosed	Information contractually limited to named individuals, critically sensitive personal data such as health-related information	A breach results in significant financial damage over € 10 M euro, loss of contracts, irreparable loss of trust from partners, lawsuits, penalties, loss of research revenue, and/or irreversible reputational damage	No additional restrictions are imposed.	Additional requirements: the application of encryption on data at rest, in transit and in use, sharing of information on name basis, watermarking of electronic and/or physical copies, bi-annual access reviews