# Information Security Requirements for Suppliers

January 2026

**Objective**

Define all the Security Guidelines that must be complied with to protect the Information disclosed by Nemak.

These Security Guidelines form an integral part of any agreement entered into between Nemak and Supplier, and Supplier shall comply with these to protect the confidentiality and integrity of the Information. These requirements may be supplemented by means of other security requirements, any service level agreement or any other document agreed between Nemak and Supplier.

**Scope**

This document applies to all Suppliers that have or may have access to any type of information owned and/or disclosed by Nemak.

**Exceptions**

In case that it is not possible to comply with a security requirement, it should be notified to Nemak at the following email for its corresponding evaluation: isec.suppliers@nemak.com

**Definitions**

***Nemak***
Nemak, S.A.B. de C.V. and its subsidiaries.

***Agreement***
Any agreement, purchase order, nomination letter or other document setting forth the terms and conditions under which the products and/or services are to be supplied and/or rendered to Nemak.

***CSIRT** (Cyber Security Incident Response Team)*
Nemak's Cyber Security Incident Response Team.

***Information***
All confidential and proprietary information held by, and relating in any manner to, Nemak or its businesses, clients, suppliers, or any third party.

***Audit***
Periodic review of Supplier's performance and compliance with any Agreement.

***Supplier***
Any natural person or legal entity that provides products and/or services to Nemak.

***Infrastructure Platforms and Services***
Nemak's systems, applications, and/or network elements and databases.

***Physical Resources***
Hardware or physical equipment used solely for purposes of the provision of the services or supply of the products (e.g. computers, printers, servers, monitors, mobile devices, removable storage media, etc.).

***Logical Resources***
Software, systems, or applications to which access is granted solely for purposes of the provision of the services or supply of the products.

***SLA***
Service Level Agreement

| | |
|---|---|
| **Roles and Responsibilities** | ***Nemak:***<br>Communicates the appropriate regulations and measures of Nemak to third parties<br>***Supplier:***<br>Ensures the compliance of the information security requirements |
| **General Requirements** | • Supplier shall take all necessary measures to protect any Information to which it has access to, including the Platforms and Services of the Nemak Infrastructure, whether derived from the provision of services or the supply of products or for any other reason that Supplier requires access to the Information, Platform and/or Infrastructure Services of Nemak.<br>• Supplier shall comply, and shall cause any subcontractors to comply with, the Security Guidelines set forth herein, and shall maintain evidence that demonstrates such compliance.<br>• Always comply with these Security Guidelines, even if the scope of the services has been modified by Nemak and Supplier.<br>• Sign Nemak's Global Business Code for Suppliers, it being understood that only those Security Guidelines that relate to the services that are to be rendered will be applicable to Supplier. |
| **Confidentiality** | • Supplier acknowledges that the Information disclosed by Nemak to which Supplier, its employees or subcontracted personnel have and/or will have access, is the property of Nemak, its clients, suppliers and/or third parties, and is protected by confidentiality undertakings.<br>• Supplier shall establish policies, procedures, and controls to prevent any unauthorized disclosure of the Information by employees or subcontracted personnel who have access to the Information.<br>• Access to Information and to the Infrastructure Platform and Services shall be granted only to those employees and/or personnel subcontracted by Supplier on a need-to-know basis and solely with respect to the provision of the services or supply of products.<br>• Supplier represents and warrants that personal data or confidential information may only be used for business purposes and in strict alignment with any Agreements between the parties, as well as with any Nemak policies and the applicable law.<br>• Supplier shall ensure the confidentiality of the Information to which it has access to by executing one or several non-disclosure agreements.<br>• Supplier shall take proactive measures to correctly safeguard personal data or confidential information that is disclosed to it for the purpose of the supply of products and/or services. |
| **Physical Security** | • Supplier shall ensure that personal data and confidential information is only accessed by authorized personnel under the need-to-know basis.<br>• Supplier shall take the necessary measures to protect its own facilities and IT equipment and infrastructure.<br>• Supplier and/or subcontracted personnel shall always comply with Nemak's Physical Security policies and procedures. |
| **Supplier's Personnel** | • Supplier's personnel shall avoid any conflicts of interest as set forth in Nemak's Global Business Code for Suppliers. |

| | |
|---|---|
| | • Supplier will be responsible for the fact that its staff is competent and/or certified for the provision of the services and that it maintains this level during the term of the Agreement. The competence and/or certification of the staff must be able to be demonstrated to the satisfaction of Nemak.<br>• Supplier shall inform its personnel in writing about the content of this document. In case it so requires, Nemak may request Supplier to confirm in writing that it informed its personnel about the content of this document, and Supplier shall ensure the strict adherence and compliance with it by its personnel or any subcontracted personnel. |
| **IT Infrastructure Acceptable Use Policy** | • Supplier shall always make good use of the Physical and Logical Resources provided by Nemak |
| **Logical Access Control** | • Employees and/or personnel subcontracted by Supplier must accept the Information Security requirements. Evidence of the acceptance of such terms and conditions shall be available if required by any audit or for any other purposes.<br>• Supplier agrees to have a policy for passwords in its own infrastructure systems, with the following criteria:<br>  ○ Minimum length of 10 characters, with at least one character from each of the 3-character groups (lowercase, uppercase, numbers).<br>  ○ Systems should be configured to require a password change at least once every 12 months, or immediately should there be the slightest indication that the password has been compromised in any way, or if there is doubt that a third party may know it.<br>• Upon termination of services or contract, Supplier shall disable or eliminate employee or third-party accounts to use Supplier's IT Infrastructure.<br>• If Nemak provides accounts and passwords to connect to Nemak's systems, they shall not be disclosed and/or shared with any third party or staff of Supplier who are not part of the provision of the services or supply of products. For individualized accounts granted by Nemak, they must not be disclosed and/or shared among staff even if they are part of the provision of the services or supply of products.<br>• Supplier shall be responsible for any activity carried out with the accounts and passwords provided by Nemak to Supplier personnel.<br>• Nemak will terminate Supplier's access to the Information when:<br>  ○ The purpose has been fulfilled.<br>  ○ There is a breach by Supplier of these Security Guidelines.<br>  ○ Any suspicious activity is detected.<br>  ○ When Nemak deems it convenient.<br>• In the event that Nemak provides user accounts (e.g., Active Directory accounts, VPN access, Email, etc.) to Supplier or Supplier subcontracted third parties, Supplier must immediately notify to Nemak should any of the following apply:<br>  ○ The employee or subcontracted third party is terminated or is no longer having a contractual relation with the Supplier.<br>  ○ The employee or subcontracted third party is no longer providing services to Nemak.<br>Notifications must be sent to Nemak's Supplier liaison manager and to Nemak's Information Security: isec.suppliers@nemak.com |

**IT Infrastructure Management**

*Network Access*

- Supplier network shall be protected by firewalls and may only be accessed by Supplier's personnel.
- Supplier's personnel shall use an active directory user to connect to the network.

*Secure Erase*

- Upon termination of the business relationship with Nemak or when requested by Nemak, whichever happens first, Supplier shall apply the secure erase of information to ensure the proper deletion (or return, if applicable) of Information.

*Antimalware Protection*

- Supplier will maintain the products and equipment used for the provision of the services or supply of the products with the latest antimalware versions and updates provided by the manufacturer. Firewall in computer equipment must be enabled to block any malware attempt.

*Vulnerability Management*

- Supplier shall scan for vulnerabilities within the IT Infrastructure to detect, notify and remedy the vulnerabilities found in the provision of the services or supply of products, as well as in Supplier's equipment used for the provision of the services or supply of products.
- Supplier shall implement a remediation plan in case of any vulnerabilities.

*Systems Patching*

- Supplier shall ensure that servers, user PCs and mobile devices are patched within maximum 60 days after the patch release.

*Remove VPN Access*

- Supplier agrees to use VPN to connect to its facilities only with Active Directory authentication and no other connection options. If possible, Supplier shall use Multifactor Authentication with VPN.
- VPN access shall not be shared between individuals.

**Use of Cloud Services**

In case of cloud service providers, Supplier agrees to include the following provisions for the protection of Nemak's data and availability of services:

- Provide dedicated support in the event of an information security incident in the cloud service environment.
- Support the organization in gathering digital evidence, taking into consideration laws and regulations for digital evidence across different jurisdictions.
- Provide required backup of data and configuration information and securely managing backups as applicable.
- Provide and return information such as configuration files, source code, logs and data that are owned by the organization, when requested during the service provision or at termination of service.

The cloud service provider always must notify:

| | |
|---|---|
| | • Changes to the technical infrastructure (e.g. relocation, reconfiguration, or changes in hardware or software) that affect or change the cloud service offering.<br>• Processing or storing information in a new geographical or legal jurisdiction.<br>• Use of peer cloud service providers or other sub-contractors (including changing existing or using new parties). |
| **Information Security Awareness** | • Supplier shall implement awareness and learning programs (across their employees) with respect to information security, taking preventive measures, and implementing policies, procedures, and controls on how to classify and manage information.<br>• Supplier must provide its employees with basic security training at least once a year, ensuring they are aware of:<br>○ Phishing risks<br>○ Keeping safe their password<br>○ Use of strong passwords<br>○ Social engineering<br>○ Social media |
| **Cybersecurity Risks and Incident Management** | • Supplier shall identify cybersecurity risks and take appropriate action towards preventing any security incidents.<br>• In case that Supplier is involved in a Security Incident that affects Nemak, then Supplier, in coordination with the CSIRT, shall work together to return to normal operations.<br>• Supplier shall immediately notify Nemak of any actual or potential cyber security incident and data breach. |
| **Business Continuity** | • Supplier shall develop business continuity plans for critical systems. These plans shall include, but not be limited to, disaster recovery procedures that are tested at least once a year. |
| **Audit** | • Nemak shall have the right to:<br>○ Audit Supplier's performance and compliance with these Security Guidelines.<br>○ Request access to reports/certificates of third parties that validate compliance with the controls linked to the provision of the services or supply of products. |
| **Compliance** | • Supplier shall make good use of any Intellectual Property Rights and Copyrights of Nemak and third parties.<br>• Supplier shall be liable to Nemak with respect to any breach of its responsibilities stated in these Security Guidelines.<br>• Failure by Supplier or any of its subcontracted personnel to comply with these Security Guidelines may cause penalties as specified in the Agreement and the applicable laws.<br>• Supplier agrees to indemnify, defend and hold Nemak harmless in the event of any claim arising from any breach of these Security Guidelines.<br>• These Security Guidelines may be updated from time to time. Supplier shall comply with these Security Guidelines for as long as it maintains a business relationship with Nemak. |
| **Contact Information** | If you have questions or comments with respect to this guideline, you may contact Nemak's Information Security with your inquiry at isec.suppliers@nemak.com. |

**Revisions**

| Version | Date | Requestor | Description of Changes |
|---|---|---|---|
| 1.0 | July/2022 | Ricardo Serrano | Creation of guideline |
| 2.0 | August/2022 | Edwin Macias | Document format changed to guideline |
| 3.0 | March/2023 | Edwin Macias | Section *Logical Access Control* changed:<br>The text related to the end of the services of the Supplier or Subcontracted Third Parties was redefined. |
| 4.0 | January/2024 | Omar Duran | *Use of Cloud Services* section added |
| 4.0 | January/2025 | Omar Duran | Review completed. No changes identified. No change in document version<br>The Russian translation removed |
| 5.0 | January/2026 | Gerardo Vasquez | The Introduction and Purpose section was replaced by the Objective section The content of the Objective section has been updated |

This document follows the general document management process described in:

NPO-GBL-SEC-10 Document Management Policy

**Approved by**

| Version | Date | Name of Approver |
|---|---|---|
| 1.0 | July/2022 | Edwin Macias |
| 2.0 | August/2022 | Alejandro Valdes Flores |
| 3.0 | March/2023 | Alejandro Valdes Flores |
| 4.0 | January/2024 | Edwin Macias |
| 4.0 | January/2025 | Edwin Macias |
| 5.0 | January/2026 | Edwin Macias |

**This document has been created using a translator tool**

# Requisitos de seguridad de la información para proveedores

**Enero 2026**

**Objetivo**

Definir todas las directrices de seguridad que deben cumplirse para proteger la información divulgada por Nemak.

Estas directrices de seguridad forman parte integrante de cualquier acuerdo celebrado entre Nemak y el proveedor, y este último deberá cumplirlas para proteger la confidencialidad e integridad de la información. Estos requisitos podrán complementarse con otros requisitos de seguridad, cualquier acuerdo de nivel de servicio o cualquier otro documento acordado entre Nemak y el proveedor.

**Ámbito**

Este documento se aplica a todos los Proveedores que tengan o puedan tener acceso a cualquier tipo de información propiedad de Nemak y/o divulgada por esta.

**Excepciones**

En caso de que no sea posible cumplir con un requisito de seguridad, se deberá notificar a Nemak a la siguiente dirección de correo electrónico para su correspondiente evaluación: isec.suppliers@nemak.com

**Definiciones**

***Nemak***
Nemak, S.A.B. de C.V. y sus subsidiarias.

***Contrato***
Cualquier acuerdo, orden de compra, carta de nominación u otro documento que establezca los términos y condiciones bajo los cuales se suministrarán y/o prestarán los productos y/o servicios a Nemak.

***CSIRT** (Equipo de Respuesta a Incidentes de Ciberseguridad)*
Equipo de respuesta a incidentes de ciberseguridad de Nemak.

***Información***
Toda la información confidencial y privada que posea Nemak o que esté relacionada de alguna manera con Nemak o sus negocios, clientes, proveedores o cualquier tercero.

***Auditoría***
Revisión periódica del desempeño del proveedor y del cumplimiento de cualquier acuerdo.

***Proveedor***
Cualquier persona física o jurídica que proporcione productos y/o servicios a Nemak.

***Plataformas y servicios de infraestructura***
Los sistemas, aplicaciones y/o elementos de red y bases de datos de Nemak.

***Recursos físicos***
Hardware o equipo físico utilizado exclusivamente para la prestación de los servicios o el suministro de los productos (por ejemplo, computadoras, impresoras, servidores, monitores, dispositivos móviles, medios de almacenamiento extraíbles, etc.).

***Recursos lógicos***
Software, sistemas o aplicaciones a los que se concede acceso exclusivamente con el fin de prestar los servicios o suministrar los productos.

***SLA***
Acuerdo de nivel de servicio

| | |
|---|---|
| **Funciones y responsabilidades** | ***Nemak:***<br>Comunica las normas y medidas apropiadas de Nemak a terceros.<br>***Proveedor:***<br>Garantiza el cumplimiento de los requisitos de seguridad de la información. |
| **Requisitos generales** | • El proveedor tomará todas las medidas necesarias para proteger cualquier información a la que tenga acceso, incluidas las plataformas y los servicios de la infraestructura de Nemak, ya sea derivada de la prestación de servicios o del suministro de productos o por cualquier otra razón por la que el proveedor requiera acceso a la información, la plataforma y/o los servicios de infraestructura de Nemak.<br>• El proveedor deberá cumplir, y hará que cualquier subcontratista cumpla, las Directrices de seguridad establecidas en el presente documento, y deberá conservar pruebas que demuestren dicho cumplimiento.<br>• Cumplir siempre con estas Directrices de Seguridad, incluso si el alcance de los servicios ha sido modificado por Nemak y el Proveedor.<br>• Firmar el Código de Negocios Global para Proveedores de Nemak, quedando entendido que solo serán aplicables al Proveedor aquellas Directrices de Seguridad que se relacionen con los servicios que se prestarán. |
| **Confidencialidad** | • El Proveedor reconoce que la Información divulgada por Nemak a la que el Proveedor, sus empleados o personal subcontratado tienen y/o tendrán acceso, es propiedad de Nemak, sus clientes, proveedores y/o terceros, y está protegida por compromisos de confidencialidad.<br>• El Proveedor establecerá políticas, procedimientos y controles para evitar cualquier divulgación no autorizada de la Información por parte de los empleados o personal subcontratado que tenga acceso a la misma.<br>• El acceso a la Información y a la Plataforma y los Servicios de Infraestructura solo se concederá a aquellos empleados y/o personal subcontratado por el Proveedor que lo necesiten y únicamente en relación con la prestación de los servicios o el suministro de productos.<br>• El Proveedor declara y garantiza que los datos personales o la información confidencial solo podrán utilizarse con fines comerciales y en estricta conformidad con los acuerdos entre las partes, así como con las políticas de Nemak y la legislación aplicable.<br>• El Proveedor garantizará la confidencialidad de la Información a la que tenga acceso mediante la firma de uno o varios acuerdos de confidencialidad.<br>• El Proveedor tomará medidas proactivas para proteger correctamente los datos personales o la información confidencial que se le revele con el fin de suministrar productos y/o prestar servicios. |
| **Seguridad física** | • El proveedor garantizará que solo el personal autorizado tenga acceso a los datos personales y la información confidencial, según sea necesario.<br>• El proveedor tomará las medidas necesarias para proteger sus propias instalaciones y equipos e infraestructura informáticos.<br>• El proveedor y/o el personal subcontratado deberán cumplir en todo momento las políticas y procedimientos de seguridad física de Nemak. |
| **Personal del proveedor** | • El personal del proveedor evitará cualquier conflicto de intereses, tal y como se establece en el Código de Negocios Global para Proveedores de Nemak. |

| | |
|---|---|
| | • El proveedor será responsable de que su personal sea competente y/o esté certificado para la prestación de los servicios y de que mantenga este nivel durante la vigencia del contrato. La competencia y/o certificación del personal deberá poder demostrarse a satisfacción de Nemak.<br><br>• El proveedor informará por escrito a su personal sobre el contenido de este documento. En caso de que lo requiera, Nemak podrá solicitar al proveedor que confirme por escrito que ha informado a su personal sobre el contenido de este documento, y el proveedor se asegurará del estricto cumplimiento y acatamiento del mismo por parte de su personal o de cualquier personal subcontratado. |
| **Política de uso aceptable de la infraestructura de TI** | • El Proveedor hará siempre un buen uso de los recursos físicos y lógicos proporcionados por Nemak. |
| **Control de acceso lógico** | • Los empleados y/o el personal subcontratado por el Proveedor deben aceptar los requisitos de seguridad de la información. Se deberá disponer de pruebas de la aceptación de dichos términos y condiciones si así lo requiere cualquier auditoría o para cualquier otro fin.<br><br>• El Proveedor se compromete a disponer de una política de contraseñas en sus propios sistemas de infraestructura, con los siguientes criterios:<br><br>○ Longitud mínima de 10 caracteres, con al menos un carácter de cada uno de los 3 grupos de caracteres (minúsculas, mayúsculas, números).<br><br>○ Los sistemas deben estar configurados para exigir un cambio de contraseña al menos una vez cada 12 meses, o inmediatamente si hay el más mínimo indicio de que la contraseña se ha visto comprometida de alguna manera, o si existe la duda de que un tercero pueda conocerla.<br><br>• Al término de los servicios o del contrato, el Proveedor desactivará o eliminará las cuentas de los empleados o de terceros para utilizar la infraestructura informática del Proveedor.<br><br>• Si Nemak proporciona cuentas y contraseñas para conectarse a los sistemas de Nemak, estas no se revelarán ni se compartirán con terceros o personal del Proveedor que no forme parte de la prestación de los servicios o el suministro de productos. En el caso de las cuentas individualizadas concedidas por Nemak, no se revelarán ni se compartirán entre el personal, incluso si forman parte de la prestación de los servicios o el suministro de productos.<br><br>• El Proveedor será responsable de cualquier actividad realizada con las cuentas y contraseñas proporcionadas por Nemak al personal del Proveedor.<br><br>• Nemak cancelará el acceso del Proveedor a la Información cuando:<br><br>○ Se haya cumplido el propósito.<br><br>○ Se produzca un incumplimiento por parte del Proveedor de estas Directrices de Seguridad.<br><br>○ Se detecte cualquier actividad sospechosa.<br><br>○ Nemak lo considere conveniente.<br><br>• En caso de que Nemak proporcione cuentas de usuario (por ejemplo, cuentas de Active Directory, acceso VPN, correo electrónico, etc.) al Proveedor o a terceros |

subcontratados por el Proveedor, este deberá notificarlo inmediatamente a Nemak si se da alguna de las siguientes circunstancias:

- El empleado o tercero subcontratado ha sido despedido o ya no tiene relación contractual con el Proveedor.
- El empleado o tercero subcontratado ya no presta servicios a Nemak.

Las notificaciones deben enviarse al responsable de relaciones con los proveedores de Nemak y al departamento de seguridad de la información de Nemak: isec.suppliers@nemak.com

**Gestión de la infraestructura de TI**

*Acceso a la red*

- La red del proveedor estará protegida por cortafuegos y solo podrá acceder a ella el personal del proveedor.
- El personal del proveedor deberá utilizar un usuario de Active Directory para conectarse a la red.

*Borrado seguro*

- Al término de la relación comercial con Nemak o cuando así lo solicite Nemak, lo que ocurra primero, el proveedor aplicará el borrado seguro de la información para garantizar la eliminación adecuada (o la devolución, si procede) de la información.

*Protección contra malware*

- El Proveedor mantendrá los productos y equipos utilizados para la prestación de los servicios o el suministro de los productos con las últimas versiones y actualizaciones antimalware proporcionadas por el fabricante. El firewall de los equipos informáticos deberá estar activado para bloquear cualquier intento de malware.

*Gestión de vulnerabilidades*

- El proveedor escaneará las vulnerabilidades dentro de la infraestructura de TI para detectar, notificar y remediar las vulnerabilidades encontradas en la prestación de los servicios o el suministro de productos, así como en los equipos del proveedor utilizados para la prestación de los servicios o el suministro de productos.
- El proveedor implementará un plan de corrección en caso de que se detecte alguna vulnerabilidad.

*Parcheo de sistemas*

- El proveedor se asegurará de que los servidores, las computadoras de los usuarios y los dispositivos móviles se actualicen en un plazo máximo de 60 días tras el lanzamiento del parche.

*Eliminar el acceso VPN*

- El proveedor se compromete a utilizar la VPN para conectarse a sus instalaciones únicamente con autenticación de Active Directory y sin otras opciones de conexión. Si es posible, el proveedor utilizará la autenticación multifactorial con VPN.
- El acceso VPN no se compartirá entre personas.

| | |
|---|---|
| **Uso de servicios en la nube** | En el caso de los proveedores de servicios en la nube, el proveedor se compromete a incluir las siguientes disposiciones para la protección de los datos de Nemak y la disponibilidad de los servicios:<br>• Proporcionar soporte dedicado en caso de un incidente de seguridad de la información en el entorno del servicio en la nube.<br>• Apoyar a la organización en la recopilación de pruebas digitales, teniendo en cuenta las leyes y normativas sobre pruebas digitales en las diferentes jurisdicciones.<br>• Proporcionar las copias de seguridad necesarias de los datos y la información de configuración y gestionar de forma segura las copias de seguridad según corresponda.<br>• Proporcionar y devolver información como archivos de configuración, código fuente, registros y datos que sean propiedad de la organización, cuando se solicite durante la prestación del servicio o al finalizar el mismo.<br>El proveedor de servicios en la nube siempre debe notificar:<br>• Los cambios en la infraestructura técnica (por ejemplo, reubicación, reconfiguración o cambios en el hardware o el software) que afecten o modifiquen la oferta de servicios en la nube.<br>• El procesamiento o almacenamiento de información en una nueva jurisdicción geográfica o legal.<br>• El uso de proveedores de servicios en la nube homólogos u otros subcontratistas (incluido el cambio de los existentes o el uso de nuevos). |
| **Concienciación sobre la seguridad de la información** | • El proveedor implementará programas de concienciación y aprendizaje (para todos sus empleados) con respecto a la seguridad de la información, tomando medidas preventivas e implementando políticas, procedimientos y controles sobre cómo clasificar y gestionar la información.<br>• El proveedor deberá proporcionar a sus empleados formación básica en materia de seguridad al menos una vez al año, asegurándose de que conozcan:<br>○ Los riesgos de phishing<br>○ Cómo mantener segura su contraseña<br>○ El uso de contraseñas seguras<br>○ Ingeniería social<br>○ Redes sociales |
| **Riesgos de ciberseguridad y gestión de incidentes** | • El proveedor identificará los riesgos de ciberseguridad y tomará las medidas adecuadas para prevenir cualquier incidente de seguridad.<br>• En caso de que el proveedor se vea involucrado en un incidente de seguridad que afecte a Nemak, el proveedor, en coordinación con el CSIRT, colaborará para restablecer el funcionamiento normal.<br>• El proveedor notificará inmediatamente a Nemak cualquier incidente de ciberseguridad real o potencial y cualquier violación de datos. |
| **Continuidad del negocio** | • El proveedor deberá desarrollar planes de continuidad del negocio para los sistemas críticos. Estos planes deberán incluir, entre otros, procedimientos de recuperación ante desastres que se prueben al menos una vez al año. |
| **Auditoría** | • Nemak tendrá derecho a:<br>○ Auditar el desempeño del Proveedor y el cumplimiento de estas Directrices de Seguridad. |

- Solicitar el acceso a informes/certificados de terceros que validen el cumplimiento de los controles relacionados con la prestación de los servicios o el suministro de productos.

**Cumplimiento**

- El proveedor hará un buen uso de los derechos de propiedad intelectual y los derechos de autor de Nemak y de terceros.
- El proveedor será responsable ante Nemak por cualquier incumplimiento de sus responsabilidades establecidas en estas Directrices de Seguridad.
- El incumplimiento por parte del proveedor o de cualquiera de sus subcontratistas de estas Directrices de seguridad podrá dar lugar a las sanciones especificadas en el Acuerdo y en la legislación aplicable.
- El proveedor se compromete a indemnizar, defender y eximir de responsabilidad a Nemak en caso de cualquier reclamación que se derive del incumplimiento de estas Directrices de Seguridad.
- Las presentes Directrices de Seguridad podrán actualizarse periódicamente. El Proveedor deberá cumplir con las presentes Directrices de Seguridad mientras mantenga una relación comercial con Nemak.

**Información de contacto**

Si tiene alguna pregunta o comentario con respecto a esta directriz, puede ponerse en contacto con el departamento de Seguridad de la Información de Nemak enisec.suppliers@nemak.com.

**Revisiones**

| Versión | Fecha | Solicitante | Descripción de los cambios |
|---|---|---|---|
| 1.0 | Julio/2022 | Ricardo Serrano | Creación de directrices |
| 2.0 | Agosto/2022 | Edwin Macias | Formato del documento cambiado a directriz |
| 3.0 | Marzo/2023 | Edwin Macias | Sección *Control de acceso lógico* modificada:<br>Se ha redefinido el texto relacionado con la finalización de los servicios del proveedor o de terceros subcontratados. |
| 4.0 | Enero/2024 | Omar Durán | Se ha añadido la sección *Uso de servicios en la nube.* |
| 4.0 | Enero/2025 | Omar Durán | Revisión completada. No se han identificado cambios. No hay cambios en la versión del documento<br>Se ha eliminado la traducción al ruso. |
| 5.0 | Enero/2026 | Gerardo Vásquez | La sección «Introducción y propósito» se ha sustituido por la sección «Objetivo».<br>Se ha actualizado el contenido de la sección «Objetivo». |

Este documento sigue el proceso general de gestión de documentos descrito en:

NPO-GBL-SEC-10 Política de gestión de documentos

**Aprobado por**

| Versión | Fecha | Nombre del aprobador |
|---|---|---|
| 1.0 | Julio/2022 | Edwin Macias |
| 2.0 | Agosto/2022 | Alejandro Valdés Flores |
| 3.0 | Marzo/2023 | Alejandro Valdés Flores |
| 4.0 | Enero/2024 | Edwin Macías |
| 4.0 | Enero/2025 | Edwin Macias |
| 5.0 | Enero/2026 | Edwin Macias |

**Este documento ha sido creado utilizando una herramienta de traducción.**

# Informationssicherheitsanforderungen für Lieferanten

**Januar 2026**

**Ziel**

Festlegung aller Sicherheitsrichtlinien, die zum Schutz der von Nemak offengelegten Informationen einzuhalten sind.

Diese Sicherheitsrichtlinien sind integraler Bestandteil jeder Vereinbarung zwischen Nemak und dem Lieferanten, und der Lieferant muss diese einhalten, um die Vertraulichkeit und Integrität der Informationen zu schützen. Diese Anforderungen können durch andere Sicherheitsanforderungen, Service Level Agreements oder andere zwischen Nemak und dem Lieferanten vereinbarte Dokumente ergänzt werden.

**Geltungsbereich**

Dieses Dokument gilt für alle Lieferanten, die Zugang zu Informationen jeglicher Art haben oder haben könnten, die Eigentum von Nemak sind und/oder von Nemak offengelegt werden.

**Ausnahmen**

Falls es nicht möglich ist, eine Sicherheitsanforderung zu erfüllen, sollte dies Nemak unter der folgenden E-Mail-Adresse zur entsprechenden Bewertung mitgeteilt werden: isec.suppliers@nemak.com

**Definitionen**

***Nemak***
Nemak, S.A.B. de C.V. und seine Tochtergesellschaften.

***Vereinbarung***
Jede Vereinbarung, Bestellung, Nominierungsurkunde oder jedes andere Dokument, in dem die Bedingungen festgelegt sind, unter denen die Produkte und/oder Dienstleistungen an Nemak geliefert und/oder erbracht werden sollen.

***CSIRT** (Cyber Security Incident Response Team)*
Das Cyber Security Incident Response Team von Nemak.

***Informationen***
Alle vertraulichen und geschützten Informationen, die sich im Besitz von Nemak oder seinen Unternehmen, Kunden, Lieferanten oder Dritten befinden oder in irgendeiner Weise mit diesen in Zusammenhang stehen.

***Audit***
Regelmäßige Überprüfung der Leistung des Lieferanten und der Einhaltung aller Vereinbarungen.

***Lieferant***
Jede natürliche oder juristische Person, die Produkte und/oder Dienstleistungen für Nemak bereitstellt.

***Infrastrukturplattformen und -dienste***
Die Systeme, Anwendungen und/oder Netzwerkelemente und Datenbanken von Nemak.

***Physische Ressourcen***
Hardware oder physische Geräte, die ausschließlich für die Bereitstellung der Dienste oder die Lieferung der Produkte verwendet werden (z. B. Computer, Drucker, Server, Monitore, mobile Geräte, Wechseldatenträger usw.).

***Logische Ressourcen***
Software, Systeme oder Anwendungen, auf die ausschließlich zum Zweck der Erbringung der Dienstleistungen oder der Lieferung der Produkte zugegriffen wird.

***SLA***
Service Level Agreement

| | |
|---|---|
| **Rollen und Verantwortlichkeiten** | ***Nemak:***<br>Kommuniziert die entsprechenden Vorschriften und Maßnahmen von Nemak an Dritte<br>***Lieferant:***<br>Stellt die Einhaltung der Anforderungen an die Informationssicherheit sicher |
| **Allgemeine Anforderungen** | • Der Lieferant ergreift alle erforderlichen Maßnahmen zum Schutz aller Informationen, auf die er Zugriff hat, einschließlich der Plattformen und Dienste der Nemak-Infrastruktur, unabhängig davon, ob diese aus der Erbringung von Dienstleistungen oder der Lieferung von Produkten stammen oder aus einem anderen Grund, aus dem der Lieferant Zugriff auf die Informationen, Plattformen und/oder Infrastrukturdienste von Nemak benötigt.<br>• Der Lieferant muss die hierin festgelegten Sicherheitsrichtlinien einhalten und dafür sorgen, dass alle Subunternehmer diese ebenfalls einhalten, und er muss Nachweise über die Einhaltung dieser Richtlinien aufbewahren.<br>• Diese Sicherheitsrichtlinien sind stets einzuhalten, auch wenn der Umfang der Dienstleistungen von Nemak und dem Lieferanten geändert wurde.<br>• Unterzeichnen Sie den Global Business Code for Suppliers von Nemak, wobei zu beachten ist, dass für den Lieferanten nur die Sicherheitsrichtlinien gelten, die sich auf die zu erbringenden Dienstleistungen beziehen. |
| **Vertraulichkeit** | • Der Lieferant erkennt an, dass die von Nemak offengelegten Informationen, zu denen der Lieferant, seine Mitarbeiter oder Subunternehmer Zugang haben und/oder haben werden, Eigentum von Nemak, seinen Kunden, Lieferanten und/oder Dritten sind und durch Vertraulichkeitsverpflichtungen geschützt sind.<br>• Der Lieferant muss Richtlinien, Verfahren und Kontrollen einrichten, um eine unbefugte Offenlegung der Informationen durch Mitarbeiter oder Subunternehmer, die Zugang zu den Informationen haben, zu verhindern.<br>• Der Zugang zu den Informationen und zur Infrastrukturplattform und den Diensten wird nur den Mitarbeitern und/oder Subunternehmern des Lieferanten gewährt, die diese Informationen benötigen, und zwar ausschließlich im Zusammenhang mit der Erbringung der Dienstleistungen oder der Lieferung der Produkte.<br>• Der Lieferant versichert und garantiert, dass personenbezogene Daten oder vertrauliche Informationen nur für geschäftliche Zwecke und in strikter Übereinstimmung mit den Vereinbarungen zwischen den Parteien sowie mit den Richtlinien von Nemak und den geltenden Gesetzen verwendet werden dürfen.<br>• Der Lieferant gewährleistet die Vertraulichkeit der Informationen, zu denen er Zugang hat, durch den Abschluss einer oder mehrerer Geheimhaltungsvereinbarungen.<br>• Der Lieferant ergreift proaktive Maßnahmen, um personenbezogene Daten oder vertrauliche Informationen, die ihm zum Zweck der Lieferung von Produkten und/oder Dienstleistungen offengelegt werden, ordnungsgemäß zu schützen. |
| **Physische Sicherheit** | • Der Lieferant stellt sicher, dass personenbezogene Daten und vertrauliche Informationen nur von autorisiertem Personal auf der Grundlage des Need-to-know-Prinzips eingesehen werden können.<br>• Der Lieferant ergreift die erforderlichen Maßnahmen zum Schutz seiner eigenen Einrichtungen sowie seiner IT-Ausrüstung und -Infrastruktur.<br>• Der Lieferant und/oder das Subunternehmerpersonal müssen stets die Richtlinien und Verfahren von Nemak zur physischen Sicherheit einhalten. |

| | |
|---|---|
| **Personal des Lieferanten** | • Das Personal des Lieferanten hat Interessenkonflikte gemäß dem Global Business Code for Suppliers von Nemak zu vermeiden.<br>• Der Lieferant ist dafür verantwortlich, dass sein Personal für die Erbringung der Dienstleistungen kompetent und/oder zertifiziert ist und dieses Niveau während der Laufzeit der Vereinbarung aufrechterhält. Die Kompetenz und/oder Zertifizierung des Personals muss zur Zufriedenheit von Nemak nachgewiesen werden können.<br>• Der Lieferant muss sein Personal schriftlich über den Inhalt dieses Dokuments informieren. Falls erforderlich, kann Nemak vom Lieferanten eine schriftliche Bestätigung verlangen, dass er sein Personal über den Inhalt dieses Dokuments informiert hat, und der Lieferant muss die strikte Einhaltung und Befolgung durch sein Personal oder etwaiges Subunternehmerpersonal sicherstellen. |
| **Richtlinie zur akzeptablen Nutzung der IT-Infrastruktur** | • Der Lieferant hat die von Nemak bereitgestellten physischen und logischen Ressourcen stets ordnungsgemäß zu nutzen. |
| **Logische Zugriffskontrolle** | • Mitarbeiter und/oder vom Lieferanten beauftragte Subunternehmer müssen die Anforderungen an die Informationssicherheit akzeptieren. Der Nachweis über die Annahme dieser Bedingungen muss bei Bedarf für Audits oder andere Zwecke vorliegen.<br>• Der Lieferant verpflichtet sich, in seinen eigenen Infrastruktursystemen eine Richtlinie für Passwörter mit den folgenden Kriterien zu haben:<br>  ○ Mindestlänge von 10 Zeichen, wobei mindestens ein Zeichen aus jeder der drei Zeichengruppen (Kleinbuchstaben, Großbuchstaben, Zahlen) enthalten sein muss.<br>  ○ Die Systeme sollten so konfiguriert sein, dass mindestens alle 12 Monate eine Passwortänderung erforderlich ist, oder sofort, wenn auch nur der geringste Hinweis darauf vorliegt, dass das Passwort in irgendeiner Weise kompromittiert wurde, oder wenn Zweifel bestehen, dass ein Dritter es kennen könnte.<br>• Bei Beendigung der Dienstleistungen oder des Vertrags muss der Lieferant die Konten von Mitarbeitern oder Dritten für die Nutzung der IT-Infrastruktur des Lieferanten deaktivieren oder löschen.<br>• Wenn Nemak Konten und Passwörter für die Verbindung mit den Systemen von Nemak bereitstellt, dürfen diese nicht an Dritte oder Mitarbeiter des Lieferanten weitergegeben und/oder mit diesen geteilt werden, die nicht an der Erbringung der Dienstleistungen oder der Lieferung der Produkte beteiligt sind. Individuelle Konten, die von Nemak vergeben werden, dürfen nicht an Mitarbeiter weitergegeben und/oder mit diesen geteilt werden, selbst wenn diese an der Erbringung der Dienstleistungen oder der Lieferung der Produkte beteiligt sind.<br>• Der Lieferant ist für alle Aktivitäten verantwortlich, die mit den Konten und Passwörtern durchgeführt werden, die Nemak dem Personal des Lieferanten zur Verfügung gestellt hat.<br>• Nemak wird den Zugang des Lieferanten zu den Informationen beenden, wenn:<br>  ○ der Zweck erfüllt ist<br>  ○ der Lieferant gegen diese Sicherheitsrichtlinien verstößt.<br>  ○ verdächtige Aktivitäten festgestellt werden.<br>  ○ Nemak dies für angebracht hält. |

- Für den Fall, dass Nemak dem Lieferanten oder vom Lieferanten beauftragten Dritten Benutzerkonten (z. B. Active Directory-Konten, VPN-Zugang, E-Mail usw.) zur Verfügung stellt, muss der Lieferant Nemak unverzüglich benachrichtigen, wenn einer der folgenden Fälle eintritt:
  - Der Mitarbeiter oder Subunternehmer wird gekündigt oder steht nicht mehr in einem Vertragsverhältnis mit dem Lieferanten.
  - Der Mitarbeiter oder Subunternehmer erbringt keine Dienstleistungen mehr für Nemak.

  Benachrichtigungen müssen an den Lieferanten-Verantwortlichen von Nemak und an die Abteilung für Informationssicherheit von Nemak gesendet werden: isec.suppliers@nemak.com

**IT-Infrastrukturmanagement**

*Netzwerkzugang*

- Das Netzwerk des Lieferanten muss durch Firewalls geschützt sein und darf nur von Mitarbeitern des Lieferanten genutzt werden.
- Das Personal des Lieferanten muss sich mit einem Active Directory-Benutzerkonto mit dem Netzwerk verbinden.

*Sicheres Löschen*

- Bei Beendigung der Geschäftsbeziehung mit Nemak oder auf Verlangen von Nemak, je nachdem, was zuerst eintritt, muss der Lieferant die sichere Löschung von Informationen durchführen, um die ordnungsgemäße Löschung (oder gegebenenfalls Rückgabe) von Informationen sicherzustellen.

*Malware-Schutz*

- Der Lieferant wird die für die Erbringung der Dienstleistungen oder die Lieferung der Produkte verwendeten Produkte und Geräte mit den neuesten Antimalware-Versionen und Updates des Herstellers ausstatten. Die Firewall in den Computergeräten muss aktiviert sein, um jegliche Malware-Angriffe zu blockieren.

*Verwaltung von Sicherheitslücken*

- Der Lieferant muss die IT-Infrastruktur auf Schwachstellen überprüfen, um Schwachstellen zu erkennen, zu melden und zu beheben, die bei der Erbringung der Dienstleistungen oder der Lieferung der Produkte sowie in den Geräten des Lieferanten, die für die Erbringung der Dienstleistungen oder die Lieferung der Produkte verwendet werden, festgestellt werden.
- Der Lieferant muss im Falle von Schwachstellen einen Plan zur Behebung dieser Schwachstellen umsetzen.

*System-Patching*

- Der Lieferant muss sicherstellen, dass Server, Benutzer-PCs und mobile Geräte innerhalb von maximal 60 Tagen nach Veröffentlichung des Patches gepatcht werden.

*VPN-Zugang entfernen*

- Der Lieferant verpflichtet sich, für die Verbindung zu seinen Einrichtungen ausschließlich VPN mit Active Directory-Authentifizierung und keine anderen

| | |
|---|---|
| | Verbindungsoptionen zu verwenden. Wenn möglich, muss der Lieferant die Multi-Faktor-Authentifizierung mit VPN verwenden.<br>• Der VPN-Zugang darf nicht zwischen Personen geteilt werden. |
| **Nutzung von Cloud-Diensten** | Im Falle von Cloud-Dienstleistern verpflichtet sich der Lieferant, die folgenden Bestimmungen zum Schutz der Daten von Nemak und zur Verfügbarkeit der Dienste aufzunehmen:<br>• Bereitstellung dedizierter Unterstützung im Falle eines Vorfalls im Bereich der Informationssicherheit in der Cloud-Service-Umgebung.<br>• Unterstützung des Unternehmens bei der Sammlung digitaler Beweise unter Berücksichtigung der Gesetze und Vorschriften für digitale Beweise in verschiedenen Rechtsordnungen.<br>• Bereitstellung der erforderlichen Sicherungskopien von Daten und Konfigurationsinformationen und sichere Verwaltung der Sicherungskopien, soweit erforderlich.<br>• Bereitstellung und Rückgabe von Informationen wie Konfigurationsdateien, Quellcode, Protokollen und Daten, die Eigentum der Organisation sind, wenn dies während der Dienstleistungserbringung oder bei Beendigung der Dienstleistung verlangt wird.<br>Der Cloud-Dienstleister muss stets Folgendes mitteilen:<br>• Änderungen an der technischen Infrastruktur (z. B. Umzug, Neukonfiguration oder Änderungen an Hardware oder Software), die sich auf das Cloud-Service-Angebot auswirken oder dieses verändern.<br>• Verarbeitung oder Speicherung von Informationen in einer neuen geografischen oder rechtlichen Gerichtsbarkeit.<br>• Einsatz von Peer-Cloud-Dienstleistern oder anderen Subunternehmern (einschließlich der Änderung bestehender oder der Nutzung neuer Parteien). |
| **Bewusstsein für Informationssicherheit** | • Der Lieferant muss (für alle seine Mitarbeiter) Sensibilisierungs- und Schulungsprogramme zum Thema Informationssicherheit durchführen, vorbeugende Maßnahmen ergreifen und Richtlinien, Verfahren und Kontrollen zur Klassifizierung und Verwaltung von Informationen implementieren.<br>• Der Lieferant muss seinen Mitarbeitern mindestens einmal jährlich eine grundlegende Sicherheitsschulung anbieten, um sicherzustellen, dass sie sich der folgenden Punkte bewusst sind:<br>○ Phishing-Risiken<br>○ Sichere Aufbewahrung ihrer Passwörter<br>○ Verwendung sicherer Passwörter<br>○ Social Engineering<br>○ Soziale Medien |
| **Risiken für die Cybersicherheit und Vorfallmanagement** | • Der Lieferant muss Cybersicherheitsrisiken identifizieren und geeignete Maßnahmen zur Verhinderung von Sicherheitsvorfällen ergreifen.<br>• Falls der Lieferant in einen Sicherheitsvorfall verwickelt ist, der Nemak betrifft, muss der Lieferant in Abstimmung mit dem CSIRT zusammenarbeiten, um den normalen Betrieb wiederherzustellen.<br>• Der Lieferant muss Nemak unverzüglich über alle tatsächlichen oder potenziellen Cybersicherheitsvorfälle und Datenverstöße informieren. |

| | |
|---|---|
| **Geschäftskontinuität** | • Der Lieferant muss Business-Continuity-Pläne für kritische Systeme entwickeln. Diese Pläne müssen unter anderem Disaster-Recovery-Verfahren umfassen, die mindestens einmal jährlich getestet werden. |
| **Audit** | • Nemak hat das Recht<br>○ die Leistung des Lieferanten und die Einhaltung dieser Sicherheitsrichtlinien zu prüfen.<br>○ Zugang zu Berichten/Zertifikaten von Dritten zu verlangen, die die Einhaltung der Kontrollen im Zusammenhang mit der Erbringung der Dienstleistungen oder der Lieferung der Produkte bestätigen. |
| **Einhaltung** | • Der Lieferant hat die geistigen Eigentumsrechte und Urheberrechte von Nemak und Dritten ordnungsgemäß zu nutzen.<br>• Der Lieferant haftet gegenüber Nemak für jede Verletzung seiner in diesen Sicherheitsrichtlinien festgelegten Pflichten.<br>• Die Nichteinhaltung dieser Sicherheitsrichtlinien durch den Lieferanten oder eines seiner Subunternehmer kann zu Strafen gemäß der Vereinbarung und den geltenden Gesetzen führen.<br>• Der Lieferant verpflichtet sich, Nemak im Falle von Ansprüchen, die sich aus einem Verstoß gegen diese Sicherheitsrichtlinien ergeben, zu entschädigen, zu verteidigen und schadlos zu halten.<br>• Diese Sicherheitsrichtlinien können von Zeit zu Zeit aktualisiert werden. Der Lieferant hat diese Sicherheitsrichtlinien so lange einzuhalten, wie er eine Geschäftsbeziehung mit Nemak unterhält. |
| **Kontakt** | Wenn Sie Fragen oder Anmerkungen zu diesen Richtlinien haben, können Sie sich mit Ihrer Anfrage an die Informationssicherheitsabteilung von Nemak unterisec.suppliers@nemak.com wenden. |

**Änderungen**

| Version | Datum | Anfragender | Beschreibung der Änderungen |
|---|---|---|---|
| 1.0 | Juli/2022 | Ricardo Serrano | Erstellung von Leitlinien |
| 2.0 | August/2022 | Edwin Macias | Dokumentformat in Leitfaden geändert |
| 3.0 | März/2023 | Edwin Macias | Abschnitt *„Logische Zugriffskontrolle”* geändert:<br>Der Text zum Ende der Dienstleistungen des Lieferanten oder der unterbeauftragten Dritten wurde neu definiert. |
| 4.0 | Januar/2024 | Omar Duran | Abschnitt *„Nutzung von Cloud-Diensten”* hinzugefügt |
| 4.0 | Januar/2025 | Omar Duran | Überprüfung abgeschlossen. Keine Änderungen festgestellt. Keine Änderung der Dokumentversion<br>Die russische Übersetzung wurde entfernt. |

| | | | |
|---|---|---|---|
| 5.0 | Januar/2026 | Gerardo Vasquez | Der Abschnitt „Einleitung und Zweck“ wurde durch den Abschnitt „Zielsetzung“ ersetzt.<br>Der Inhalt des Abschnitts „Zielsetzung“ wurde aktualisiert |

Dieses Dokument folgt dem allgemeinen Dokumentenmanagementprozess, der in folgendem Dokument beschrieben ist:

NPO-GBL-SEC-10 Richtlinie zur Dokumentenverwaltung

**Genehmigt von**

| Version | Datum | Name des Genehmigers |
|---|---|---|
| 1.0 | Juli/2022 | Edwin Macias |
| 2.0 | August/2022 | Alejandro Valdes Flores |
| 3.0 | März/2023 | Alejandro Valdes Flores |
| 4.0 | Januar/2024 | Edwin Macias |
| 4.0 | Januar/2025 | Edwin Macias |
| 5.0 | Januar/2026 | Edwin Macias |

**Dieses Dokument wurde mit einem Übersetzungstool erstellt.**

# Requisitos de segurança da informação para fornecedores

**Janeiro de 2026**

**Objetivo**

Definir todas as diretrizes de segurança que devem ser cumpridas para proteger as informações divulgadas pela Nemak.

Essas diretrizes de segurança fazem parte integrante de qualquer acordo celebrado entre a Nemak e o fornecedor, e o fornecedor deve cumpri-las para proteger a confidencialidade e a integridade das informações. Esses requisitos podem ser complementados por meio de outros requisitos de segurança, qualquer acordo de nível de serviço ou qualquer outro documento acordado entre a Nemak e o fornecedor.

**Âmbito**

Este documento se aplica a todos os Fornecedores que tenham ou possam ter acesso a qualquer tipo de informação pertencente e/ou divulgada pela Nemak.

**Exceções**

Caso não seja possível cumprir um requisito de segurança, isso deve ser notificado à Nemak no seguinte e-mail para a correspondente avaliação: isec.suppliers@nemak.com

**Definições**

***Nemak***
Nemak, S.A.B. de C.V. e suas subsidiárias.

***Contrato***
Qualquer acordo, ordem de compra, carta de nomeação ou outro documento que estabeleça os termos e condições sob os quais os produtos e/ou serviços devem ser fornecidos e/ou prestados à Nemak.

***CSIRT** (Equipe de Resposta a Incidentes de Segurança Cibernética)*
Equipe de Resposta a Incidentes de Segurança Cibernética da Nemak.

***Informações***
Todas as informações confidenciais e proprietárias mantidas pela Nemak ou relacionadas de qualquer forma à Nemak ou seus negócios, clientes, fornecedores ou terceiros.

***Auditoria***
Revisão periódica do desempenho do fornecedor e da conformidade com qualquer acordo.

***Fornecedor***
Qualquer pessoa física ou jurídica que forneça produtos e/ou serviços à Nemak.

***Plataformas e serviços de infraestrutura***
Sistemas, aplicativos e/ou elementos de rede e bancos de dados da Nemak.

***Recursos físicos***
Hardware ou equipamento físico utilizado exclusivamente para fins de prestação dos serviços ou fornecimento dos produtos (por exemplo, computadores, impressoras, servidores, monitores, dispositivos móveis, suportes de armazenamento removíveis, etc.).

***Recursos lógicos***
Software, sistemas ou aplicativos aos quais o acesso é concedido exclusivamente para fins de prestação dos serviços ou fornecimento dos produtos.

***SLA***
Acordo de Nível de Serviço

| | |
|---|---|
| **Funções e responsabilidades** | ***Nemak:***<br>Comunica os regulamentos e medidas apropriados da Nemak a terceiros<br>***Fornecedor:***<br>Garante a conformidade com os requisitos de segurança da informação |
| **Requisitos gerais** | • O fornecedor deve tomar todas as medidas necessárias para proteger qualquer informação à qual tenha acesso, incluindo as plataformas e serviços da infraestrutura da Nemak, seja derivada da prestação de serviços ou do fornecimento de produtos ou por qualquer outro motivo que o fornecedor precise acessar as informações, plataformas e/ou serviços de infraestrutura da Nemak.<br>• O fornecedor deve cumprir e fazer com que quaisquer subcontratados cumpram as diretrizes de segurança aqui estabelecidas e deve manter evidências que comprovem tal conformidade.<br>• Sempre cumpra estas Diretrizes de Segurança, mesmo que o escopo dos serviços tenha sido modificado pela Nemak e pelo Fornecedor.<br>• Assine o Código de Negócios Global da Nemak para Fornecedores, ficando entendido que apenas as Diretrizes de Segurança relacionadas aos serviços a serem prestados serão aplicáveis ao Fornecedor. |
| **Confidencialidade** | • O Fornecedor reconhece que as Informações divulgadas pela Nemak às quais o Fornecedor, seus funcionários ou pessoal subcontratado têm e/ou terão acesso são propriedade da Nemak, seus clientes, fornecedores e/ou terceiros, e estão protegidas por compromissos de confidencialidade.<br>• O Fornecedor estabelecerá políticas, procedimentos e controles para impedir qualquer divulgação não autorizada das Informações por funcionários ou pessoal subcontratado que tenham acesso às Informações.<br>• O acesso às Informações e à Plataforma de Infraestrutura e Serviços será concedido apenas aos funcionários e/ou pessoal subcontratado pelo Fornecedor, com base na necessidade de conhecimento e exclusivamente no que diz respeito à prestação dos serviços ou fornecimento dos produtos.<br>• O Fornecedor declara e garante que os dados pessoais ou informações confidenciais só podem ser utilizados para fins comerciais e em estrita conformidade com quaisquer acordos entre as partes, bem como com quaisquer políticas da Nemak e a legislação aplicável.<br>• O Fornecedor garantirá a confidencialidade das Informações às quais tem acesso, celebrando um ou vários acordos de confidencialidade.<br>• O Fornecedor tomará medidas proativas para proteger corretamente os dados pessoais ou informações confidenciais que lhe forem divulgados para fins de fornecimento de produtos e/ou serviços. |
| **Segurança física** | • O fornecedor deve garantir que os dados pessoais e as informações confidenciais só sejam acessados por pessoal autorizado, com base na necessidade de conhecimento.<br>• O fornecedor deverá tomar as medidas necessárias para proteger suas próprias instalações e equipamentos e infraestrutura de TI.<br>• O fornecedor e/ou o pessoal subcontratado devem cumprir sempre as políticas e procedimentos de segurança física da Nemak. |
| **Pessoal do fornecedor** | • O pessoal do fornecedor deve evitar quaisquer conflitos de interesses, conforme estabelecido no Código de Negócios Global da Nemak para Fornecedores. |

| | |
|---|---|
| | • O fornecedor será responsável por garantir que seu pessoal seja competente e/ou certificado para a prestação dos serviços e que mantenha esse nível durante a vigência do Contrato. A competência e/ou certificação do pessoal deve poder ser demonstrada de forma satisfatória para a Nemak.<br>• O fornecedor deve informar seu pessoal por escrito sobre o conteúdo deste documento. Caso seja necessário, a Nemak pode solicitar ao fornecedor que confirme por escrito que informou seu pessoal sobre o conteúdo deste documento, e o fornecedor deve garantir o cumprimento e a conformidade estritos com o mesmo por parte de seu pessoal ou de qualquer pessoal subcontratado. |
| **Política de Uso Aceitável da Infraestrutura de TI** | • O Fornecedor deverá sempre fazer bom uso dos Recursos Físicos e Lógicos fornecidos pela Nemak. |
| **Controle de acesso lógico** | • Os funcionários e/ou pessoal subcontratado pelo Fornecedor devem aceitar os requisitos de Segurança da Informação. A prova da aceitação de tais termos e condições deve estar disponível se exigida por qualquer auditoria ou para quaisquer outros fins.<br>• O Fornecedor concorda em ter uma política para senhas em seus próprios sistemas de infraestrutura, com os seguintes critérios:<br>○ Comprimento mínimo de 10 caracteres, com pelo menos um caractere de cada um dos 3 grupos de caracteres (minúsculas, maiúsculas, números).<br>○ Os sistemas devem ser configurados para exigir uma mudança de senha pelo menos uma vez a cada 12 meses, ou imediatamente caso haja o menor indício de que a senha foi comprometida de alguma forma, ou se houver dúvida de que um terceiro possa conhecê-la.<br>• Após o término dos serviços ou do contrato, o Fornecedor deverá desativar ou eliminar as contas de funcionários ou terceiros para usar a Infraestrutura de TI do Fornecedor.<br>• Se a Nemak fornecer contas e senhas para conexão aos sistemas da Nemak, elas não deverão ser divulgadas e/ou compartilhadas com terceiros ou funcionários do Fornecedor que não façam parte da prestação dos serviços ou fornecimento dos produtos. No caso de contas individualizadas concedidas pela Nemak, elas não devem ser divulgadas e/ou compartilhadas entre os funcionários, mesmo que façam parte da prestação dos serviços ou fornecimento dos produtos.<br>• O Fornecedor será responsável por qualquer atividade realizada com as contas e senhas fornecidas pela Nemak ao pessoal do Fornecedor.<br>• A Nemak encerrará o acesso do Fornecedor às Informações quando:<br>○ A finalidade tiver sido cumprida.<br>○ Houver uma violação por parte do Fornecedor destas Diretrizes de Segurança.<br>○ For detectada qualquer atividade suspeita.<br>○ Quando a Nemak considerar conveniente.<br>• No caso de a Nemak fornecer contas de usuário (por exemplo, contas do Active Directory, acesso VPN, e-mail, etc.) ao Fornecedor ou a terceiros subcontratados pelo Fornecedor, o Fornecedor deverá notificar imediatamente a Nemak caso se aplique qualquer uma das seguintes situações: |

- O funcionário ou terceiro subcontratado é demitido ou não tem mais relação contratual com o Fornecedor.
- O funcionário ou terceiro subcontratado não presta mais serviços à Nemak.

As notificações devem ser enviadas ao gerente de relacionamento com fornecedores da Nemak e ao departamento de Segurança da Informação da Nemak: isec.suppliers@nemak.com

**Gerenciamento de infraestrutura de TI**

*Acesso à rede*

- A rede do fornecedor deve ser protegida por firewalls e só pode ser acessada pelo pessoal do fornecedor.
- O pessoal do fornecedor deve usar um usuário do Active Directory para se conectar à rede.

*Apagamento seguro*

- Após o término da relação comercial com a Nemak ou quando solicitado pela Nemak, o que ocorrer primeiro, o fornecedor deverá aplicar a exclusão segura de informações para garantir a exclusão adequada (ou devolução, se aplicável) das informações.

*Proteção antimalware*

- O Fornecedor manterá os produtos e equipamentos utilizados para a prestação dos serviços ou fornecimento dos produtos com as versões e atualizações antimalware mais recentes fornecidas pelo fabricante. O firewall nos equipamentos de informática deve estar ativado para bloquear qualquer tentativa de malware.

*Gerenciamento de vulnerabilidades*

- O fornecedor deverá verificar se há vulnerabilidades na infraestrutura de TI para detectar, notificar e corrigir as vulnerabilidades encontradas na prestação dos serviços ou fornecimento dos produtos, bem como nos equipamentos do fornecedor utilizados para a prestação dos serviços ou fornecimento dos produtos.
- O fornecedor deverá implementar um plano de correção em caso de vulnerabilidades.

*Aplicação de patches nos sistemas*

- O fornecedor deve garantir que os servidores, computadores dos usuários e dispositivos móveis recebam as atualizações no prazo máximo de 60 dias após o lançamento das atualizações.

*Remover acesso VPN*

- O fornecedor concorda em usar VPN para se conectar às suas instalações apenas com autenticação do Active Directory e nenhuma outra opção de conexão. Se possível, o fornecedor deverá usar autenticação multifatorial com VPN.
- O acesso VPN não deve ser compartilhado entre indivíduos.

**Uso de serviços em nuvem**

No caso de provedores de serviços em nuvem, o Fornecedor concorda em incluir as seguintes disposições para a proteção dos dados da Nemak e a disponibilidade dos serviços:

- Fornecer suporte dedicado em caso de incidente de segurança da informação no ambiente de serviços em nuvem.

| | |
|---|---|
| | • Apoiar a organização na coleta de evidências digitais, levando em consideração as leis e regulamentos para evidências digitais em diferentes jurisdições.<br>• Fornecer o backup necessário de dados e informações de configuração e gerenciar os backups com segurança, conforme aplicável.<br>• Fornecer e devolver informações como arquivos de configuração, código-fonte, registros e dados que são de propriedade da organização, quando solicitado durante a prestação do serviço ou no término do serviço.<br>O provedor de serviços em nuvem deve sempre notificar:<br>• Alterações na infraestrutura técnica (por exemplo, realocação, reconfiguração ou alterações no hardware ou software) que afetem ou alterem a oferta de serviços em nuvem.<br>• Processamento ou armazenamento de informações em uma nova jurisdição geográfica ou legal.<br>• O uso de provedores de serviços em nuvem parceiros ou outros subcontratados (incluindo a mudança de parceiros existentes ou o uso de novos). |
| **Conscientização sobre segurança da informação** | • O fornecedor deve implementar programas de conscientização e aprendizagem (para todos os seus funcionários) com relação à segurança da informação, tomando medidas preventivas e implementando políticas, procedimentos e controles sobre como classificar e gerenciar informações.<br>• O fornecedor deve fornecer aos seus funcionários treinamento básico em segurança pelo menos uma vez por ano, garantindo que eles estejam cientes de:<br>○ Riscos de phishing<br>○ Manutenção da segurança de suas senhas<br>○ Uso de senhas fortes<br>○ Engenharia social<br>○ Redes sociais |
| **Riscos de segurança cibernética e gerenciamento de incidentes** | • O fornecedor deve identificar os riscos de segurança cibernética e tomar as medidas adequadas para prevenir quaisquer incidentes de segurança.<br>• Caso o Fornecedor esteja envolvido em um Incidente de Segurança que afete a Nemak, o Fornecedor, em coordenação com o CSIRT, deverá trabalhar em conjunto para retornar às operações normais.<br>• O fornecedor deverá notificar imediatamente a Nemak sobre qualquer incidente de segurança cibernética real ou potencial e violação de dados. |
| **Continuidade dos negócios** | • O fornecedor deverá desenvolver planos de continuidade dos negócios para sistemas críticos. Esses planos deverão incluir, entre outros, procedimentos de recuperação de desastres que sejam testados pelo menos uma vez por ano. |
| **Auditoria** | • A Nemak terá o direito de:<br>○ Auditar o desempenho do Fornecedor e a conformidade com estas Diretrizes de Segurança.<br>○ Solicitar acesso a relatórios/certificados de terceiros que validem a conformidade com os controles relacionados à prestação de serviços ou fornecimento de produtos. |
| **Conformidade** | • O fornecedor deverá fazer bom uso de quaisquer direitos de propriedade intelectual e direitos autorais da Nemak e de terceiros. |

- O fornecedor será responsável perante a Nemak por qualquer violação das suas responsabilidades estabelecidas nestas Diretrizes de Segurança.
- O não cumprimento destas Diretrizes de Segurança pelo fornecedor ou por qualquer membro do seu pessoal subcontratado pode resultar em penalidades, conforme especificado no Contrato e nas leis aplicáveis.
- O fornecedor concorda em indenizar, defender e isentar a Nemak de qualquer responsabilidade no caso de qualquer reclamação decorrente de qualquer violação destas Diretrizes de Segurança.
- Estas Diretrizes de Segurança podem ser atualizadas periodicamente. O fornecedor deverá cumprir estas Diretrizes de Segurança enquanto mantiver uma relação comercial com a Nemak.

**Informações de contato** Se você tiver dúvidas ou comentários sobre esta diretriz, entre em contato com o departamento de Segurança da Informação da Nemak pelo e-mailisec.suppliers@nemak.com .

**Revisões**

| Versão | Data | Solicitante | Descrição das alterações |
|---|---|---|---|
| 1.0 | Julho/2022 | Ricardo Serrano | Criação de diretrizes |
| 2.0 | Agosto/2022 | Edwin Macias | Formato do documento alterado para diretriz |
| 3.0 | Março/2023 | Edwin Macias | Seção *Controle de acesso lógico* alterada:<br>O texto relacionado ao término dos serviços do Fornecedor ou Terceiros Subcontratados foi redefinido. |
| 4.0 | Janeiro/2024 | Omar Duran | Seção *Uso de serviços em nuvem* adicionada |
| 4.0 | Janeiro/2025 | Omar Duran | Revisão concluída. Nenhuma alteração identificada. Nenhuma alteração na versão do documento<br>Tradução para o russo removida |
| 5.0 | Janeiro/2026 | Gerardo Vasquez | A seção Introdução e Objetivo foi substituída pela seção Objetivo<br>O conteúdo da seção Objetivo foi atualizado |

Este documento segue o processo geral de gestão de documentos descrito em:

NPO-GBL-SEC-10 Política de Gerenciamento de Documentos

**Aprovado por**

| Versão | Data | Nome do aprovador |
|---|---|---|
| 1.0 | Julho/2022 | Edwin Macias |
| 2.0 | Agosto/2022 | Alejandro Valdes Flores |
| 3.0 | Março/2023 | Alejandro Valdes Flores |

| | | |
|---|---|---|
| 4.0 | Janeiro/2024 | Edwin Macias |
| 4.0 | Janeiro/2025 | Edwin Macias |
| 5.0 | Janeiro/2026 | Edwin Macias |

**Este documento foi criado usando uma ferramenta de tradução.**

# Požadavky na bezpečnost informací pro dodavatele

**Leden 2026**

**Cíl**

Definovat všechny bezpečnostní pokyny, které je nutné dodržovat za účelem ochrany informací poskytnutých společností Nemak.

Tyto bezpečnostní pokyny tvoří nedílnou součást jakékoli smlouvy uzavřené mezi společností Nemak a dodavatelem a dodavatel je povinen je dodržovat, aby byla zajištěna důvěrnost a integrita informací. Tyto požadavky mohou být doplněny dalšími bezpečnostními požadavky, jakoukoli smlouvou o úrovni služeb nebo jakýmkoli jiným dokumentem dohodnutým mezi společností Nemak a dodavatelem.

**Rozsah**

Tento dokument se vztahuje na všechny dodavatele, kteří mají nebo mohou mít přístup k jakémukoli typu informací vlastněných a/nebo zveřejněných společností Nemak.

**Výjimky**

V případě, že není možné splnit bezpečnostní požadavek, je třeba o tom informovat společnost Nemak na následující e-mailové adrese, aby mohla provést odpovídající hodnocení: isec.suppliers@nemak.com

**Definice**

***Nemak***
Nemak, S.A.B. de C.V. a její dceřiné společnosti.

***Smlouva***
Jakákoli smlouva, objednávka, jmenovací dopis nebo jiný dokument stanovující podmínky, za kterých mají být produkty a/nebo služby dodány a/nebo poskytnuty společnosti Nemak.

***CSIRT** (tým pro reakci na kybernetické bezpečnostní incidenty)*
Tým společnosti Nemak pro reakci na kybernetické bezpečnostní incidenty.

***Informace***
Veškeré důvěrné a proprietární informace, které jsou v držení společnosti Nemak nebo jejích obchodních partnerů, klientů, dodavatelů nebo jakékoli třetí strany, nebo se jakýmkoli způsobem týkají těchto subjektů.

***Audit***
Pravidelné přezkoumávání výkonnosti dodavatele a dodržování jakékoli smlouvy.

***Dodavatel***
Jakákoli fyzická nebo právnická osoba, která poskytuje produkty a/nebo služby společnosti Nemak.

***Infrastrukturní platformy a služby***
Systémy, aplikace a/nebo síťové prvky a databáze společnosti Nemak.

***Fyzické zdroje***
Hardware nebo fyzické zařízení používané výhradně pro účely poskytování služeb nebo dodávek produktů (např. počítače, tiskárny, servery, monitory, mobilní zařízení, vyměnitelné paměťové médium atd.).

***Logické zdroje***
Software, systémy nebo aplikace, k nimž je přístup povolen výhradně za účelem poskytování služeb nebo dodávání produktů.

***SLA***
Smlouva o úrovni služeb

| | |
|---|---|
| **Role a odpovědnosti** | ***Nemak:***<br>Sděluje příslušné předpisy a opatření společnosti Nemak třetím stranám<br>***Dodavatel:***<br>Zajišťuje dodržování požadavků na bezpečnost informací |
| **Obecné požadavky** | • Dodavatel přijme veškerá nezbytná opatření k ochraně veškerých informací, ke kterým má přístup, včetně platforem a služeb infrastruktury společnosti Nemak, ať již pocházejí z poskytování služeb nebo dodávek produktů, nebo z jakéhokoli jiného důvodu, pro který dodavatel vyžaduje přístup k informacím, platformám a/nebo infrastrukturním službám společnosti Nemak.<br>• Dodavatel je povinen dodržovat bezpečnostní pokyny stanovené v tomto dokumentu a zajistit, aby je dodržovali i všichni subdodavatelé, a je povinen uchovávat důkazy prokazující takové dodržování.<br>• Vždy dodržujte tyto bezpečnostní pokyny, i když byl rozsah služeb změněn společností Nemak a dodavatelem.<br>• Podepište Globální obchodní kodex společnosti Nemak pro dodavatele, přičemž se rozumí, že pro dodavatele budou platit pouze ty bezpečnostní pokyny, které se vztahují k poskytovaným službám. |
| **Důvěrnost** | • Dodavatel bere na vědomí, že informace poskytnuté společností Nemak, ke kterým má nebo bude mít přístup dodavatel, jeho zaměstnanci nebo subdodavatelé, jsou majetkem společnosti Nemak, jejích klientů, dodavatelů a/nebo třetích stran a jsou chráněny závazky mlčenlivosti.<br>• Dodavatel zavede zásady, postupy a kontrolní mechanismy, aby zabránil jakémukoli neoprávněnému zveřejnění informací zaměstnanci nebo subdodavatelským pracovníkům, kteří k těmto informacím mají přístup.<br>• Přístup k informacím a k infrastrukturní platformě a službám bude poskytnut pouze těm zaměstnancům a/nebo subdodavatelům dodavatele, kteří tyto informace potřebují znát, a to výhradně v souvislosti s poskytováním služeb nebo dodávkou produktů.<br>• Dodavatel prohlašuje a zaručuje, že osobní údaje nebo důvěrné informace mohou být použity pouze pro obchodní účely a v přísném souladu s jakýmikoli dohodami mezi stranami, jakož i s jakýmikoli zásadami společnosti Nemak a platnými právními předpisy.<br>• Dodavatel zajistí důvěrnost informací, ke kterým má přístup, uzavřením jedné nebo několika dohod o mlčenlivosti.<br>• Dodavatel přijme proaktivní opatření k řádné ochraně osobních údajů nebo důvěrných informací, které mu byly sděleny za účelem dodávky produktů a/nebo služeb. |
| **Fyzická bezpečnost** | • Dodavatel zajistí, aby k osobním údajům a důvěrným informacím měli přístup pouze oprávnění zaměstnanci, kteří je potřebují znát.<br>• Dodavatel přijme nezbytná opatření k ochraně svých vlastních zařízení a IT vybavení a infrastruktury.<br>• Dodavatel a/nebo subdodavatelský personál musí vždy dodržovat zásady a postupy fyzického zabezpečení společnosti Nemak. |
| **Zaměstnanci dodavatele** | • Zaměstnanci dodavatele se vyhýbají jakýmkoli střetům zájmů, jak je stanoveno v Globálním obchodním kodexu pro dodavatele společnosti Nemak. |

| | |
|---|---|
| | • Dodavatel bude odpovědný za to, že jeho zaměstnanci jsou kompetentní a/nebo certifikovaní pro poskytování služeb a že si tuto úroveň udržují po celou dobu trvání smlouvy. Kompetence a/nebo certifikace zaměstnanců musí být prokázána k uspokojení společnosti Nemak.<br>• Dodavatel písemně informuje své zaměstnance o obsahu tohoto dokumentu. V případě potřeby může společnost Nemak požádat dodavatele o písemné potvrzení, že informoval své zaměstnance o obsahu tohoto dokumentu, a dodavatel zajistí, aby jej jeho zaměstnanci nebo subdodavatelé přísně dodržovali a řídili se jím. |
| **Zásady přijatelného používání IT infrastruktury** | • Dodavatel je povinen vždy řádně využívat fyzické a logické zdroje poskytované společností Nemak. |
| **Logická kontrola přístupu** | • Zaměstnanci a/nebo subdodavatelé dodavatele musí přijmout požadavky na bezpečnost informací. Důkaz o přijetí těchto podmínek musí být k dispozici, pokud to vyžaduje audit nebo jiné účely.<br>• Dodavatel souhlasí s tím, že ve svých vlastních infrastrukturních systémech bude mít zásady pro hesla s následujícími kritérii:<br>  ○ Minimální délka 10 znaků, s alespoň jedním znakem z každé ze tří skupin znaků (malá písmena, velká písmena, číslice).<br>  ○ Systémy by měly být nakonfigurovány tak, aby vyžadovaly změnu hesla alespoň jednou za 12 měsíců, nebo okamžitě, pokud existuje sebemenší náznak, že heslo bylo jakýmkoli způsobem kompromitováno, nebo pokud existuje pochybnost, že jej může znát třetí strana.<br>• Po ukončení služeb nebo smlouvy dodavatel deaktivuje nebo odstraní účty zaměstnanců nebo třetích stran pro používání IT infrastruktury dodavatele.<br>• Pokud společnost Nemak poskytne účty a hesla pro připojení k systémům společnosti Nemak, nesmějí být sdělovány a/nebo sdíleny s žádnou třetí stranou nebo zaměstnanci dodavatele, kteří se nepodílejí na poskytování služeb nebo dodávkách produktů. Individuální účty poskytnuté společností Nemak nesmějí být sdělovány a/nebo sdíleny mezi zaměstnanci, i když se podílejí na poskytování služeb nebo dodávkách produktů.<br>• Dodavatel nese odpovědnost za veškeré činnosti prováděné s účty a hesly poskytnutými společností Nemak zaměstnancům dodavatele.<br>• Společnost Nemak ukončí přístup dodavatele k informacím, pokud:<br>  ○ Byl splněn účel.<br>  ○ dojde k porušení těchto bezpečnostních pokynů ze strany dodavatele.<br>  ○ Bude zjištěna jakákoli podezřelá činnost.<br>  ○ když to společnost Nemak považuje za vhodné.<br>• V případě, že společnost Nemak poskytne uživatelské účty (např. účty Active Directory, přístup k VPN, e-mail atd.) dodavateli nebo subdodavatelům dodavatele, musí dodavatel neprodleně informovat společnost Nemak, pokud nastane některá z následujících situací:<br>  ○ Zaměstnanec nebo subdodavatelská třetí strana ukončila pracovní poměr nebo již nemá smluvní vztah s dodavatelem. |

- Zaměstnanec nebo subdodavatelská třetí strana již neposkytuje služby společnosti Nemak.

Oznámení musí být zaslána manažerovi pro styk s dodavateli společnosti Nemak a oddělení informační bezpečnosti společnosti Nemak: isec.suppliers@nemak.com

**Správa IT infrastruktury**

*Přístup k síti*

- Síť dodavatele musí být chráněna firewally a přístup k ní mají pouze zaměstnanci dodavatele.
- Zaměstnanci dodavatele musí pro připojení k síti používat uživatele Active Directory.

*Bezpečné vymazání*

- Po ukončení obchodního vztahu se společností Nemak nebo na žádost společnosti Nemak, podle toho, co nastane dříve, dodavatel provede bezpečné vymazání informací, aby zajistil jejich řádné smazání (nebo vrácení, je-li to možné).

*Ochrana proti malwaru*

- Dodavatel bude udržovat produkty a zařízení používané k poskytování služeb nebo dodávkám produktů s nejnovějšími verzemi antimalwaru a aktualizacemi poskytovanými výrobcem. Firewall v počítačovém vybavení musí být aktivován, aby blokoval jakékoli pokusy o malware.

*Správa zranitelnosti*

- Dodavatel provede skenování zranitelností v rámci IT infrastruktury za účelem detekce, oznámení a nápravy zranitelností zjištěných při poskytování služeb nebo dodávkách produktů, jakož i v zařízeních dodavatele používaných k poskytování služeb nebo dodávkám produktů.
- Dodavatel musí v případě jakýchkoli zranitelností implementovat nápravný plán.

*Opravy systémů*

- Dodavatel zajistí, aby servery, uživatelské počítače a mobilní zařízení byly opraveny do 60 dnů od vydání opravy.

*Odstranění přístupu přes VPN*

- Dodavatel souhlasí s tím, že k připojení ke svým zařízením bude používat VPN pouze s ověřením Active Directory a bez dalších možností připojení. Pokud je to možné, dodavatel bude používat vícefaktorové ověřování s VPN.
- Přístup k VPN nesmí být sdílen mezi jednotlivci.

**Používání cloudových služeb**

V případě poskytovatelů cloudových služeb se dodavatel zavazuje zahrnout následující ustanovení pro ochranu dat společnosti Nemak a dostupnost služeb:

- Poskytovat specializovanou podporu v případě incidentu v oblasti bezpečnosti informací v prostředí cloudových služeb.
- Podporovat organizaci při shromažďování digitálních důkazů s přihlédnutím k zákonům a předpisům týkajícím se digitálních důkazů v různých jurisdikcích.
- Poskytovat požadované zálohování dat a konfiguračních informací a bezpečně spravovat zálohy podle potřeby.

| | |
|---|---|
| | • Poskytovat a vracet informace, jako jsou konfigurační soubory, zdrojový kód, protokoly a data, která jsou vlastnictvím organizace, pokud o to bude požádáno během poskytování služby nebo při ukončení služby.<br><br>Poskytovatel cloudových služeb musí vždy oznámit:<br><br>• Změny technické infrastruktury (např. přemístění, rekonfigurace nebo změny hardwaru nebo softwaru), které ovlivňují nebo mění nabídku cloudových služeb.<br><br>• Zpracování nebo ukládání informací v nové geografické nebo právní jurisdikci.<br><br>• Využití služeb jiných poskytovatelů cloudových služeb nebo jiných subdodavatelů (včetně změny stávajících nebo využití nových stran). |
| **Povědomí o bezpečnosti informací** | • Dodavatel zavede programy zvyšování povědomí a vzdělávání (pro všechny své zaměstnance) v oblasti bezpečnosti informací, přijme preventivní opatření a zavede zásady, postupy a kontroly týkající se klasifikace a správy informací.<br><br>• Dodavatel musí svým zaměstnancům poskytovat základní školení v oblasti bezpečnosti alespoň jednou ročně, aby si byli vědomi:<br><br>○ Rizik phishingu<br>○ Bezpečnosti svých hesel<br>○ Používání silných hesel<br>○ Sociálním inženýrstvím<br>○ Sociální média |
| **Rizika kybernetické bezpečnosti a řízení incidentů** | • Dodavatel je povinen identifikovat kybernetická bezpečnostní rizika a přijmout vhodná opatření k prevenci bezpečnostních incidentů.<br><br>• V případě, že se dodavatel stane účastníkem bezpečnostního incidentu, který má dopad na společnost Nemak, bude dodavatel v koordinaci s CSIRT spolupracovat na obnovení normálního provozu.<br><br>• Dodavatel je povinen neprodleně informovat společnost Nemak o jakémkoli skutečném nebo potenciálním incidentu kybernetické bezpečnosti a porušení ochrany osobních údajů. |
| **Kontinuita podnikání** | • Dodavatel vypracuje plány kontinuity podnikání pro kritické systémy. Tyto plány musí zahrnovat mimo jiné postupy pro obnovu po havárii, které jsou testovány alespoň jednou ročně. |
| **Audit** | • Společnost Nemak má právo:<br>○ Auditovat výkon dodavatele a dodržování těchto bezpečnostních pokynů.<br>○ Požadovat přístup k zprávám/certifikátům třetích stran, které potvrzují dodržování kontrolních opatření souvisejících s poskytováním služeb nebo dodávkami produktů. |
| **Dodržování** | • Dodavatel je povinen řádně využívat veškerá práva duševního vlastnictví a autorská práva společnosti Nemak a třetích stran.<br><br>• Dodavatel nese vůči společnosti Nemak odpovědnost za jakékoli porušení svých povinností uvedených v těchto bezpečnostních pokynech.<br><br>• Nedodržení těchto bezpečnostních pokynů dodavatelem nebo jakýmkoli jeho subdodavatelem může mít za následek sankce stanovené ve smlouvě a platných zákonech. |

- Dodavatel souhlasí s tím, že v případě jakéhokoli nároku vyplývajícího z porušení těchto bezpečnostních pokynů odškodní, bude hájit a zbaví společnost Nemak veškeré odpovědnosti.
- Tyto bezpečnostní pokyny mohou být čas od času aktualizovány. Dodavatel je povinen dodržovat tyto bezpečnostní pokyny po celou dobu trvání obchodního vztahu se společností Nemak.

**Kontaktní informace** Máte-li jakékoli dotazy nebo připomínky týkající se těchto pokynů, můžete se obrátit na oddělení informační bezpečnosti společnosti Nemak na adreseisec.suppliers@nemak.com .

**Revize**

| Verze | Datum | Žadatel | Popis změn |
|---|---|---|---|
| 1.0 | Červenec/2022 | Ricardo Serrano | Vytvoření pokynů |
| 2.0 | srpen/2022 | Edwin Macias | Formát dokumentu změněn na pokyny |
| 3.0 | Březen/2023 | Edwin Macias | Změna v části *Logická kontrola přístupu*:<br>Byl upřesněn text týkající se ukončení služeb dodavatele nebo subdodavatelských třetích stran. |
| 4.0 | Leden/2024 | Omar Duran | Přidána část *Používání cloudových služeb* |
| 4.0 | Leden/2025 | Omar Duran | Recenze dokončena. Nebyly zjištěny žádné změny. Žádná změna ve verzi dokumentu<br>Odstraněn ruský překlad. |
| 5.0 | Leden/2026 | Gerardo Vasquez | Část Úvod a účel byla nahrazena částí Cíl<br>Obsah části Cíl byl aktualizován |

Tento dokument se řídí obecným procesem správy dokumentů popsaným v:

NPO-GBL-SEC-10 Zásady správy dokumentů

**Schváleno**

| Verze | Datum | Jméno schvalovatele |
|---|---|---|
| 1.0 | Červenec/2022 | Edwin Macias |
| 2.0 | Srpen/2022 | Alejandro Valdes Flores |
| 3.0 | Březen/2023 | Alejandro Valdes Flores |
| 4.0 | Leden/2024 | Edwin Macias |
| 4.0 | Leden/2025 | Edwin Macias |
| 5.0 | Leden/2026 | Edwin Macias |

**Tento dokument byl vytvořen pomocí překladatelského nástroje.**

# Požiadavky na bezpečnosť informácií pre dodávateľov

**Január 2026**

**Cieľ**

Definovať všetky bezpečnostné pokyny, ktoré je potrebné dodržiavať na ochranu informácií zverejnených spoločnosťou Nemak.

Tieto bezpečnostné pokyny tvoria neoddeliteľnú súčasť akejkoľvek zmluvy uzavretej medzi spoločnosťou Nemak a dodávateľom a dodávateľ je povinný ich dodržiavať s cieľom chrániť dôvernosť a integritu informácií. Tieto požiadavky môžu byť doplnené ďalšími bezpečnostnými požiadavkami, akoukoľvek dohodou o úrovni služieb alebo akýmkoľvek iným dokumentom dohodnutým medzi spoločnosťou Nemak a dodávateľom.

**Rozsah**

Tento dokument sa vzťahuje na všetkých dodávateľov, ktorí majú alebo môžu mať prístup k akémukoľvek typu informácií, ktoré vlastní a/alebo zverejňuje spoločnosť Nemak.

**Výnimky**

V prípade, že nie je možné splniť bezpečnostnú požiadavku, je potrebné o tom informovať spoločnosť Nemak na nasledujúcej e-mailovej adrese, aby mohla vykonať príslušné posúdenie: isec.suppliers@nemak.com

**Definície**

***Nemak***
Nemak, S.A.B. de C.V. a jej dcérske spoločnosti.

***Dohoda***
Akákoľvek dohoda, objednávka, nominačný list alebo iný dokument, v ktorom sú stanovené podmienky, za ktorých sa majú produkty a/alebo služby dodávať a/alebo poskytovať spoločnosti Nemak.

***CSIRT** (tím pre reakciu na incidenty v oblasti kybernetickej bezpečnosti)*
Tím spoločnosti Nemak na riešenie incidentov v oblasti kybernetickej bezpečnosti.

***Informácie***
Všetky dôverné a proprietárne informácie, ktoré vlastní spoločnosť Nemak alebo jej podniky, klienti, dodávatelia alebo akákoľvek tretia strana, alebo ktoré sa akýmkoľvek spôsobom týkajú spoločnosti Nemak alebo jej podnikov, klientov, dodávateľov alebo akejkoľvek tretej strany.

***Audit***
Pravidelné hodnotenie výkonnosti dodávateľa a dodržiavania akejkoľvek zmluvy.

***Dodávateľ***
Akákoľvek fyzická alebo právnická osoba, ktorá poskytuje produkty a/alebo služby spoločnosti Nemak.

***Infraštruktúrne platformy a služby***
Systémy, aplikácie a/alebo sieťové prvky a databázy spoločnosti Nemak.

***Fyzické zdroje***
Hardvér alebo fyzické zariadenia používané výlučne na účely poskytovania služieb alebo dodávania produktov (napr. počítače, tlačiarne, servery, monitory, mobilné zariadenia, vymeniteľné pamäťové médiá atď.

***Logické zdroje***
Softvér, systémy alebo aplikácie, ku ktorým je prístup povolený výlučne na účely poskytovania služieb alebo dodávania produktov.

***SLA***
Dohoda o úrovni služieb

| | |
|---|---|
| **Úlohy a zodpovednosti** | ***Nemak:***<br>Komunikuje príslušné predpisy a opatrenia spoločnosti Nemak tretím stranám<br>***Dodávateľ:***<br>Zabezpečuje dodržiavanie požiadaviek na bezpečnosť informácií |
| **Všeobecné požiadavky** | • Dodávateľ prijme všetky potrebné opatrenia na ochranu akýchkoľvek informácií, ku ktorým má prístup, vrátane platforiem a služieb infraštruktúry spoločnosti Nemak, či už vyplývajúcich z poskytovania služieb alebo dodávok produktov, alebo z akéhokoľvek iného dôvodu, pre ktorý dodávateľ vyžaduje prístup k informáciám, platforme a/alebo infraštruktúrnym službám spoločnosti Nemak.<br>• Dodávateľ je povinný dodržiavať bezpečnostné pokyny uvedené v tomto dokumente a zabezpečiť, aby ich dodržiavali aj všetci subdodávatelia, a je povinný uchovávať dôkazy, ktoré preukazujú takéto dodržiavanie.<br>• Vždy dodržiavajte tieto bezpečnostné pokyny, aj keď bol rozsah služieb upravený spoločnosťou Nemak a dodávateľom.<br>• Podpíšte Globálny obchodný kódex spoločnosti Nemak pre dodávateľov, pričom platí, že na dodávateľa sa vzťahujú iba tie bezpečnostné pokyny, ktoré sa týkajú služieb, ktoré majú byť poskytované. |
| **Dôvernosť** | • Dodávateľ berie na vedomie, že informácie zverejnené spoločnosťou Nemak, ku ktorým má alebo bude mať prístup dodávateľ, jeho zamestnanci alebo subdodávatelia, sú majetkom spoločnosti Nemak, jej klientov, dodávateľov a/alebo tretích strán a sú chránené záväzkami dôvernosti.<br>• Dodávateľ zavedie politiky, postupy a kontroly, aby zabránil akémukoľvek neoprávnenému zverejneniu informácií zo strany zamestnancov alebo subdodávateľov, ktorí majú prístup k informáciám.<br>• Prístup k informáciám a k infraštruktúrnej platforme a službám sa poskytuje len tým zamestnancom a/alebo subdodávateľom dodávateľa, ktorí to potrebujú vedieť, a to výlučne v súvislosti s poskytovaním služieb alebo dodávkou produktov.<br>• Dodávateľ vyhlasuje a zaručuje, že osobné údaje alebo dôverné informácie môžu byť použité iba na obchodné účely a v prísnom súlade s akýmikoľvek dohodami medzi stranami, ako aj s akýmikoľvek politikami spoločnosti Nemak a platnými zákonmi.<br>• Dodávateľ zabezpečí dôvernosť informácií, ku ktorým má prístup, uzavretím jednej alebo viacerých dohôd o mlčanlivosti.<br>• Dodávateľ prijme proaktívne opatrenia na správnu ochranu osobných údajov alebo dôverných informácií, ktoré mu boli poskytnuté na účely dodávky produktov a/alebo služieb. |
| **Fyzická bezpečnosť** | • Dodávateľ zabezpečí, aby k osobným údajom a dôverným informáciám mali prístup iba oprávnení zamestnanci, ktorí ich potrebujú poznať.<br>• Dodávateľ prijme potrebné opatrenia na ochranu svojich vlastných zariadení a IT vybavenia a infraštruktúry.<br>• Dodávateľ a/alebo subdodávatelia musia vždy dodržiavať politiky a postupy spoločnosti Nemak v oblasti fyzickej bezpečnosti. |
| **Personál dodávateľa** | • Personál dodávateľa sa musí vyhýbať akýmkoľvek konfliktom záujmov, ako je stanovené v Globálnom obchodnom kódexe spoločnosti Nemak pre dodávateľov. |

| | |
|---|---|
| | • Dodávateľ bude zodpovedný za to, že jeho zamestnanci sú kompetentní a/alebo certifikovaní na poskytovanie služieb a že si túto úroveň udržia počas trvania zmluvy. Kompetentnosť a/alebo certifikácia zamestnancov musí byť preukázaná spôsobom, ktorý uspokojí spoločnosť Nemak.<br>• Dodávateľ písomne informuje svoj personál o obsahu tohto dokumentu. V prípade potreby môže spoločnosť Nemak požiadať dodávateľa, aby písomne potvrdil, že informoval svoj personál o obsahu tohto dokumentu, a dodávateľ zabezpečí, aby jeho personál alebo akýkoľvek subdodávateľský personál tento dokument prísne dodržiaval a riadil sa ním. |
| **Politika prijateľného používania IT infraštruktúry** | • Dodávateľ musí vždy správne využívať fyzické a logické zdroje poskytované spoločnosťou Nemak. |
| **Logická kontrola prístupu** | • Zamestnanci a/alebo subdodávatelia dodávateľa musia akceptovať požiadavky na bezpečnosť informácií. Dôkaz o akceptovaní týchto podmienok musí byť k dispozícii, ak to vyžaduje audit alebo akékoľvek iné účely.<br>• Dodávateľ súhlasí s tým, že bude mať vo svojich vlastných infraštruktúrnych systémoch politiku týkajúcu sa hesiel s nasledujúcimi kritériami:<br>○ Minimálna dĺžka 10 znakov, s aspoň jedným znakom z každej z 3-znakových skupín (malé písmená, veľké písmená, čísla).<br>○ Systémy by mali byť nakonfigurované tak, aby vyžadovali zmenu hesla aspoň raz za 12 mesiacov alebo okamžite, ak existuje aj len najmenší náznak, že heslo bolo akýmkoľvek spôsobom kompromitované, alebo ak existuje podozrenie, že ho môže poznať tretia strana.<br>• Po ukončení služieb alebo zmluvy dodávateľ deaktivuje alebo zruší účty zamestnancov alebo tretích strán na používanie IT infraštruktúry dodávateľa.<br>• Ak spoločnosť Nemak poskytuje účty a heslá na pripojenie k systémom spoločnosti Nemak, nesmú byť zverejnené a/alebo zdieľané s treťou stranou alebo zamestnancami dodávateľa, ktorí nie sú súčasťou poskytovania služieb alebo dodávok produktov. Individuálne účty udelené spoločnosťou Nemak nesmú byť zverejnené a/alebo zdieľané medzi zamestnancami, aj keď sú súčasťou poskytovania služieb alebo dodávok produktov.<br>• Dodávateľ je zodpovedný za akúkoľvek činnosť vykonávanú s účtami a heslami poskytnutými spoločnosťou Nemak zamestnancom dodávateľa.<br>• Spoločnosť Nemak ukončí prístup dodávateľa k informáciám, ak:<br>○ Účel bol splnený.<br>○ dodávateľ poruší tieto bezpečnostné pokyny.<br>○ Bude zistená akákoľvek podozrivá činnosť.<br>○ Keď to spoločnosť Nemak považuje za vhodné.<br>• V prípade, že spoločnosť Nemak poskytne používateľské účty (napr. účty Active Directory, prístup VPN, e-mail atď.) dodávateľovi alebo subdodávateľom dodávateľa, dodávateľ musí okamžite informovať spoločnosť Nemak, ak nastane niektorá z nasledujúcich situácií:<br>○ Zamestnanec alebo subdodávateľská tretia strana bola prepustená alebo už nemá zmluvný vzťah s dodávateľom. |

- Zamestnanec alebo subdodávateľská tretia strana už neposkytuje služby spoločnosti Nemak.

Oznámenia musia byť zaslané manažérovi pre styk s dodávateľmi spoločnosti Nemak a oddeleniu informačnej bezpečnosti spoločnosti Nemak: isec.suppliers@nemak.com

**Správa IT infraštruktúry**

*Prístup k sieti*

- Sieť dodávateľa musí byť chránená firewallmi a prístup k nej môžu mať len zamestnanci dodávateľa.
- Zamestnanci dodávateľa musia na pripojenie k sieti používať používateľa aktívneho adresára.

*Bezpečné vymazanie*

- Po ukončení obchodného vzťahu so spoločnosťou Nemak alebo na žiadosť spoločnosti Nemak, podľa toho, čo nastane skôr, dodávateľ vykoná bezpečné vymazanie informácií, aby zabezpečil riadne vymazanie (alebo vrátenie, ak je to vhodné) informácií.

*Ochrana proti malvéru*

- Dodávateľ bude udržiavať produkty a zariadenia používané na poskytovanie služieb alebo dodávku produktov s najnovšími verziami a aktualizáciami antimalwaru poskytovanými výrobcom. Firewall v počítačových zariadeniach musí byť aktivovaný, aby blokoval akékoľvek pokusy o škodlivý softvér.

*Správa zraniteľnosti*

- Dodávateľ bude vyhľadávať zraniteľnosti v rámci IT infraštruktúry s cieľom zistiť, oznámiť a odstrániť zraniteľnosti zistené pri poskytovaní služieb alebo dodávaní produktov, ako aj v zariadeniach dodávateľa používaných na poskytovanie služieb alebo dodávanie produktov.
- Dodávateľ musí v prípade akýchkoľvek zraniteľností implementovať nápravný plán.

*Opravy systémov*

- Dodávateľ zabezpečí, aby boli servery, používateľské počítače a mobilné zariadenia opravené najneskôr do 60 dní od vydania opravy.

*Odstránenie prístupu cez VPN*

- Dodávateľ súhlasí s tým, že na pripojenie k svojim zariadeniam bude používať VPN iba s overením Active Directory a bez iných možností pripojenia. Ak je to možné, dodávateľ bude používať viacfaktorové overenie s VPN.
- Prístup k VPN nesmie byť zdieľaný medzi jednotlivcami.

**Používanie cloudových služieb**

V prípade poskytovateľov cloudových služieb dodávateľ súhlasí so zahrnutím nasledujúcich ustanovení na ochranu údajov spoločnosti Nemak a dostupnosti služieb:

- Poskytovať špecializovanú podporu v prípade incidentu týkajúceho sa bezpečnosti informácií v prostredí cloudových služieb.
- Podporovať organizáciu pri zhromažďovaní digitálnych dôkazov, pričom zohľadní zákony a nariadenia týkajúce sa digitálnych dôkazov v rôznych jurisdikciách.

| | |
|---|---|
| | • Poskytovať požadované zálohovanie údajov a konfiguračných informácií a bezpečne spravovať zálohy podľa potreby.<br>• Poskytovať a vrátiť informácie, ako sú konfiguračné súbory, zdrojový kód, protokoly a údaje, ktoré sú vlastníctvom organizácie, ak o to bude požiadaný počas poskytovania služby alebo pri ukončení služby.<br>Poskytovateľ cloudových služieb musí vždy oznámiť:<br>• Zmeny technickej infraštruktúry (napr. presťahovanie, rekonfigurácia alebo zmeny hardvéru alebo softvéru), ktoré ovplyvňujú alebo menia ponuku cloudových služieb.<br>• Spracovanie alebo ukladanie informácií v novej geografickej alebo právnej jurisdikcii.<br>• Použitie poskytovateľov cloudových služieb alebo iných subdodávateľov (vrátane zmeny existujúcich alebo použitia nových strán). |
| **Povedomie o bezpečnosti informácií** | • Dodávateľ zavedie programy zvyšovania povedomia a vzdelávania (pre všetkých svojich zamestnancov) v oblasti informačnej bezpečnosti, prijímania preventívnych opatrení a implementácie politík, postupov a kontrol týkajúcich sa klasifikácie a správy informácií.<br>• Dodávateľ musí svojim zamestnancom poskytovať základné bezpečnostné školenia najmenej raz ročne, aby sa uistil, že sú si vedomí:<br>○ Rizikách phishingu<br>○ Bezpečnosti svojich hesiel<br>○ Používanie silných hesiel<br>○ Sociálneho inžinierstva<br>○ Sociálnych médií |
| **Riziká kybernetickej bezpečnosti a riadenie incidentov** | • Dodávateľ identifikuje riziká kybernetickej bezpečnosti a prijme primerané opatrenia na prevenciu akýchkoľvek bezpečnostných incidentov.<br>• V prípade, že dodávateľ je zapojený do bezpečnostného incidentu, ktorý ovplyvňuje spoločnosť Nemak, dodávateľ v koordinácii s CSIRT spolupracuje na obnovení normálneho prevádzky.<br>• Dodávateľ je povinný bezodkladne informovať spoločnosť Nemak o akomkoľvek skutočnom alebo potenciálnom incidente v oblasti kybernetickej bezpečnosti a porušení ochrany údajov. |
| **Kontinuita podnikania** | • Dodávateľ vypracuje plány kontinuity činnosti pre kritické systémy. Tieto plány musia obsahovať, okrem iného, postupy na obnovu po havárii, ktoré sa testujú najmenej raz ročne. |
| **Audit** | • Spoločnosť Nemak má právo:<br>○ Auditovať výkonnosť dodávateľa a dodržiavanie týchto bezpečnostných usmernení.<br>○ Požiadať o prístup k správam/certifikátom tretích strán, ktoré potvrdzujú dodržiavanie kontrolných mechanizmov súvisiacich s poskytovaním služieb alebo dodávkou produktov. |
| **Dodržiavanie** | • Dodávateľ je povinný riadne využívať všetky práva duševného vlastníctva a autorské práva spoločnosti Nemak a tretích strán.<br>• Dodávateľ bude zodpovedný spoločnosti Nemak za akékoľvek porušenie svojich povinností uvedených v týchto bezpečnostných pokynoch. |

- Nedodržanie týchto bezpečnostných pokynov zo strany dodávateľa alebo akéhokoľvek jeho subdodávateľa môže mať za následok sankcie uvedené v zmluve a príslušných zákonoch.
- Dodávateľ súhlasí s tým, že v prípade akéhokoľvek nároku vyplývajúceho z porušenia týchto bezpečnostných pokynov odškodní, bude brániť a ochráni spoločnosť Nemak.
- Tieto bezpečnostné pokyny môžu byť čas od času aktualizované. Dodávateľ je povinný dodržiavať tieto bezpečnostné pokyny po celú dobu trvania obchodného vzťahu so spoločnosťou Nemak.

**Kontaktné informácie** Ak máte otázky alebo pripomienky týkajúce sa týchto pokynov, môžete sa obrátiť na oddelenie informačnej bezpečnosti spoločnosti Nemak na adreseisec.suppliers@nemak.com .

**Revízie**

| Verzia | Dátum | Žiadateľ | Popis zmien |
|---|---|---|---|
| 1.0 | Júl/2022 | Ricardo Serrano | Vytvorenie usmernenia |
| 2.0 | august/2022 | Edwin Macias | Formát dokumentu zmenený na usmernenie |
| 3.0 | marec/2023 | Edwin Macias | Zmena v časti *Logická kontrola prístupu*:<br>Text týkajúci sa ukončenia služieb dodávateľa alebo subdodávateľov bol preformulovaný. |
| 4.0 | Január/2024 | Omar Duran | Pridaná časť *Používanie cloudových služieb* |
| 4.0 | Január/2025 | Omar Duran | Recenzia dokončená. Neboli zistené žiadne zmeny. Žiadna zmena vo verzii dokumentu<br>Odstránený ruský preklad |
| 5.0 | Január/2026 | Gerardo Vasquez | Časť Úvod a účel bola nahradená časťou Cieľ<br>Obsah časti „Cieľ“ bol aktualizovaný |

Tento dokument sa riadi všeobecným procesom správy dokumentov opísaným v:

NPO-GBL-SEC-10 Politika správy dokumentov

**Schválené**

| Verzia | Dátum | Meno schvaľovateľa |
|---|---|---|
| 1.0 | Júl/2022 | Edwin Macias |
| 2.0 | August/2022 | Alejandro Valdes Flores |
| 3,0 | marec/2023 | Alejandro Valdes Flores |
| 4,0 | Január/2024 | Edwin Macias |
| 4,0 | Január/2025 | Edwin Macias |
| 5,0 | Január/2026 | Edwin Macias |

**Tento dokument bol vytvorený pomocou prekladateľského nástroja.**

# Wymagania dotyczące bezpieczeństwa informacji dla dostawców

**Styczeń 2026**

**Cel**

Określenie wszystkich wytycznych dotyczących bezpieczeństwa, których należy przestrzegać w celu ochrony informacji ujawnionych przez Nemak.

Niniejsze wytyczne dotyczące bezpieczeństwa stanowią integralną część każdej umowy zawartej między firmą Nemak a dostawcą, a dostawca jest zobowiązany do ich przestrzegania w celu ochrony poufności i integralności informacji. Wymagania te mogą być uzupełnione innymi wymaganiami dotyczącymi bezpieczeństwa, umową o gwarantowanym poziomie usług lub innym dokumentem uzgodnionym między firmą Nemak a dostawcą.

**Zakres**

Niniejszy dokument ma zastosowanie do wszystkich dostawców, którzy mają lub mogą mieć dostęp do wszelkiego rodzaju informacji będących własnością i/lub ujawnionych przez Nemak.

**Wyjątki**

W przypadku niemożności spełnienia wymogu bezpieczeństwa należy powiadomić o tym firmę Nemak, wysyłając wiadomość e-mail na poniższy adres w celu dokonania odpowiedniej oceny: isec.suppliers@nemak.com

**Definicje**

***Nemak***
Nemak, S.A.B. de C.V. i jej spółki zależne.

***Umowa***
Każda umowa, zamówienie, pismo nominacyjne lub inny dokument określający warunki, na jakich produkty i/lub usługi mają być dostarczane i/lub świadczone na rzecz Nemak.

***CSIRT** (Zespół reagowania na incydenty związane z cyberbezpieczeństwem)*
Zespół reagowania na incydenty związane z cyberbezpieczeństwem firmy Nemak.

***Informacje***
Wszystkie poufne i zastrzeżone informacje posiadane przez firmę Nemak lub jej podmioty gospodarcze, klientów, dostawców lub osoby trzecie oraz wszelkie informacje z nimi związane.

***Audyt***
Okresowy przegląd wyników dostawcy i zgodności z umową.

***Dostawca***
Każda osoba fizyczna lub prawna, która dostarcza produkty i/lub świadczy usługi na rzecz Nemak.

***Platformy infrastrukturalne i usługi***
Systemy, aplikacje i/lub elementy sieciowe oraz bazy danych Nemak.

***Zasoby fizyczne***
Sprzęt lub urządzenia fizyczne wykorzystywane wyłącznie do świadczenia usług lub dostarczania produktów (np. komputery, drukarki, serwery, monitory, urządzenia mobilne, wymienne nośniki danych itp.

***Zasoby logiczne***
Oprogramowanie, systemy lub aplikacje, do których dostęp jest udzielany wyłącznie w celu świadczenia usług lub dostarczania produktów.

***SLA***
Umowa o gwarantowanym poziomie usług

| | |
|---|---|
| **Role i obowiązki** | ***Nemak:***<br>Przekazuje odpowiednie regulacje i środki Nemak stronom trzecim<br>***Dostawca:***<br>Zapewnia zgodność z wymogami bezpieczeństwa informacji |
| **Wymagania ogólne** | • Dostawca podejmuje wszelkie niezbędne środki w celu ochrony wszelkich informacji, do których ma dostęp, w tym platform i usług infrastruktury Nemak, niezależnie od tego, czy pochodzą one ze świadczenia usług lub dostawy produktów, czy też z jakiegokolwiek innego powodu, dla którego dostawca wymaga dostępu do informacji, platformy i/lub usług infrastruktury Nemak.<br>• Dostawca zobowiązuje się przestrzegać niniejszych wytycznych dotyczących bezpieczeństwa oraz zapewnić ich przestrzeganie przez podwykonawców, a także przechowywać dowody potwierdzające takie przestrzeganie.<br>• Należy zawsze przestrzegać niniejszych wytycznych dotyczących bezpieczeństwa, nawet jeśli zakres usług został zmodyfikowany przez Nemak i dostawcę.<br>• Należy podpisać Globalny Kodeks Biznesowy Nemak dla dostawców, przy czym rozumie się, że dostawca będzie zobowiązany do przestrzegania wyłącznie tych wytycznych dotyczących bezpieczeństwa, które odnoszą się do świadczonych usług. |
| **Poufność** | • Dostawca potwierdza, że informacje ujawnione przez Nemak, do których dostawca, jego pracownicy lub podwykonawcy mają lub będą mieli dostęp, są własnością Nemak, jego klientów, dostawców i/lub stron trzecich i są chronione zobowiązaniami do zachowania poufności.<br>• Dostawca ustanowi zasady, procedury i środki kontroli w celu zapobiegania nieuprawnionemu ujawnieniu informacji przez pracowników lub podwykonawców, którzy mają dostęp do tych informacji.<br>• Dostęp do informacji oraz do platformy infrastrukturalnej i usług będzie udzielany wyłącznie tym pracownikom i/lub personelowi podwykonawców dostawcy, którzy muszą mieć do nich dostęp, i wyłącznie w zakresie świadczenia usług lub dostawy produktów.<br>• Dostawca oświadcza i gwarantuje, że dane osobowe lub informacje poufne mogą być wykorzystywane wyłącznie do celów biznesowych i w ścisłej zgodności z umowami między stronami, a także z polityką Nemak i obowiązującym prawem.<br>• Dostawca zapewni poufność informacji, do których ma dostęp, poprzez zawarcie jednej lub kilku umów o zachowaniu poufności.<br>• Dostawca podejmuje proaktywne działania w celu prawidłowego zabezpieczenia danych osobowych lub informacji poufnych, które zostały mu ujawnione w celu dostawy produktów i/lub świadczenia usług. |
| **Bezpieczeństwo fizyczne** | • Dostawca zapewni, że dostęp do danych osobowych i informacji poufnych będą mieli wyłącznie upoważnieni pracownicy, którzy muszą znać te informacje.<br>• Dostawca podejmuje niezbędne środki w celu ochrony własnych obiektów oraz sprzętu i infrastruktury informatycznej.<br>• Dostawca i/lub personel podwykonawców zawsze przestrzega zasad i procedur Nemak dotyczących bezpieczeństwa fizycznego. |
| **Personel dostawcy** | • Personel dostawcy powinien unikać wszelkich konfliktów interesów określonych w Globalnym kodeksie biznesowym dla dostawców firmy Nemak. |

| | |
|---|---|
| | • Dostawca ponosi odpowiedzialność za to, aby jego personel posiadał kompetencje i/lub certyfikaty niezbędne do świadczenia usług oraz utrzymywał ten poziom przez cały okres obowiązywania Umowy. Kompetencje i/lub certyfikaty personelu muszą być możliwe do wykazania w sposób zadowalający dla firmy Nemak.<br>• Dostawca poinformuje swój personel na piśmie o treści niniejszego dokumentu. W razie potrzeby firma Nemak może zażądać od dostawcy pisemnego potwierdzenia, że poinformował swój personel o treści niniejszego dokumentu, a dostawca zapewni ścisłe przestrzeganie i zgodność z nim przez swój personel lub personel podwykonawców. |
| **Polityka dopuszczalnego użytkowania infrastruktury informatycznej** | • Dostawca powinien zawsze właściwie wykorzystywać zasoby fizyczne i logiczne dostarczone przez Nemak. |
| **Logiczna kontrola dostępu** | • Pracownicy i/lub personel podwykonawców dostawcy muszą zaakceptować wymagania dotyczące bezpieczeństwa informacji. Dowody akceptacji takich warunków powinny być dostępne na żądanie w przypadku audytu lub w innych celach.<br>• Dostawca zobowiązuje się do posiadania polityki dotyczącej haseł w swoich systemach infrastruktury, zgodnie z następującymi kryteriami:<br>  ○ Minimalna długość 10 znaków, z co najmniej jednym znakiem z każdej z 3 grup znaków (małe litery, wielkie litery, cyfry).<br>  ○ Systemy powinny być skonfigurowane tak, aby wymagały zmiany hasła co najmniej raz na 12 miesięcy lub natychmiast w przypadku najmniejszych oznak naruszenia bezpieczeństwa hasła lub podejrzenia, że osoba trzecia może je znać.<br>• Po zakończeniu świadczenia usług lub wygaśnięciu umowy dostawca wyłącza lub usuwa konta pracowników lub osób trzecich umożliwiające korzystanie z infrastruktury informatycznej dostawcy.<br>• Jeśli Nemak udostępnia konta i hasła umożliwiające połączenie się z systemami Nemak, nie mogą one być ujawniane ani udostępniane osobom trzecim lub pracownikom dostawcy, którzy nie są zaangażowani w świadczenie usług lub dostawę produktów. Indywidualne konta przyznane przez Nemak nie mogą być ujawniane ani udostępniane pracownikom, nawet jeśli są oni zaangażowani w świadczenie usług lub dostawę produktów.<br>• Dostawca ponosi odpowiedzialność za wszelkie działania wykonywane przy użyciu kont i haseł przekazanych pracownikom dostawcy przez Nemak.<br>• Nemak zablokuje dostęp Dostawcy do Informacji, gdy:<br>  ○ Cel zostanie osiągnięty.<br>  ○ Dostawca naruszy niniejsze wytyczne dotyczące bezpieczeństwa.<br>  ○ Wykryje jakiekolwiek podejrzane działania.<br>  ○ Nemak uzna to za stosowne.<br>• W przypadku, gdy Nemak udostępnia konta użytkowników (np. konta Active Directory, dostęp do VPN, pocztę elektroniczną itp.) dostawcy lub podwykonawcom dostawcy, dostawca musi niezwłocznie powiadomić Nemak, jeśli wystąpi którakolwiek z poniższych sytuacji:<br>  ○ Pracownik lub podwykonawca został zwolniony lub nie pozostaje już w stosunku umownym z dostawcą. |

- Pracownik lub podwykonawca nie świadczy już usług na rzecz Nemak.

Powiadomienia należy wysyłać do kierownika ds. kontaktów z dostawcami firmy Nemak oraz do działu bezpieczeństwa informacji firmy Nemak: isec.suppliers@nemak.com

**Zarządzanie infrastrukturą IT**

*Dostęp do sieci*

- Sieć dostawcy powinna być chroniona zaporami sieciowymi i dostęp do niej mogą mieć wyłącznie pracownicy dostawcy.
- Pracownicy dostawcy powinni korzystać z użytkownika Active Directory, aby połączyć się z siecią.

*Bezpieczne kasowanie*

- Po zakończeniu współpracy z Nemak lub na żądanie Nemak, w zależności od tego, co nastąpi wcześniej, dostawca ma obowiązek bezpiecznie usunąć informacje, żeby mieć pewność, że zostały one prawidłowo skasowane (lub zwrócone, jeśli to możliwe).

*Ochrona przed złośliwym oprogramowaniem*

- Dostawca będzie utrzymywał produkty i sprzęt wykorzystywane do świadczenia usług lub dostarczania produktów w stanie zgodnym z najnowszymi wersjami oprogramowania antywirusowego i aktualizacjami dostarczonymi przez producenta. Zapora sieciowa w sprzęcie komputerowym musi być włączona, aby blokować wszelkie próby ataku złośliwego oprogramowania.

*Zarządzanie podatnością*

- Dostawca będzie skanował infrastrukturę IT w celu wykrywania, zgłaszania i usuwania luk w zabezpieczeniach wykrytych podczas świadczenia usług lub dostarczania produktów, a także w sprzęcie dostawcy używanym do świadczenia usług lub dostarczania produktów.
- W przypadku wykrycia jakichkolwiek luk w zabezpieczeniach dostawca wdroży plan naprawczy.

*Aktualizacje systemów*

- Dostawca zapewni, że serwery, komputery użytkowników i urządzenia mobilne zostaną załatane w ciągu maksymalnie 60 dni od wydania poprawki.

*Usunięcie dostępu VPN*

- Dostawca zgadza się korzystać z VPN w celu połączenia się ze swoimi obiektami wyłącznie z uwierzytelnianiem Active Directory i bez innych opcji połączenia. Jeśli to możliwe, dostawca powinien stosować uwierzytelnianie wieloskładnikowe z VPN.
- Dostęp do VPN nie może być udostępniany innym osobom.

**Korzystanie z usług w chmurze**

W przypadku dostawców usług w chmurze dostawca zgadza się uwzględnić następujące postanowienia dotyczące ochrony danych Nemak i dostępności usług:

- Zapewnienie dedykowanego wsparcia w przypadku incydentu związanego z bezpieczeństwem informacji w środowisku usług w chmurze.
- Wspieranie organizacji w gromadzeniu dowodów cyfrowych, z uwzględnieniem przepisów i regulacji dotyczących dowodów cyfrowych w różnych jurysdykcjach.

| | |
|---|---|
| | • Zapewnienie wymaganej kopii zapasowej danych i informacji konfiguracyjnych oraz bezpieczne zarządzanie kopiami zapasowymi, stosownie do przypadku.<br>• Dostarczenie i zwrot informacji, takich jak pliki konfiguracyjne, kod źródłowy, logi i dane będące własnością organizacji, na żądanie podczas świadczenia usługi lub po jej zakończeniu.<br>Dostawca usług w chmurze musi zawsze powiadamiać o:<br>• O zmianach w infrastrukturze technicznej (np. przeniesienie, rekonfiguracja lub zmiany w sprzęcie lub oprogramowaniu), które mają wpływ na ofertę usług w chmurze lub ją zmieniają.<br>• Przetwarzaniu lub przechowywaniu informacji w nowej jurysdykcji geograficznej lub prawnej.<br>• Korzystanie z usług innych dostawców usług w chmurze lub innych podwykonawców (w tym zmiana istniejących lub korzystanie z nowych podmiotów). |
| **Świadomość bezpieczeństwa informacji** | • Dostawca wdroży programy uświadamiające i szkoleniowe (dla wszystkich swoich pracowników) w zakresie bezpieczeństwa informacji, podejmowania środków zapobiegawczych oraz wdrażania polityk, procedur i kontroli dotyczących klasyfikacji informacji i zarządzania nimi.<br>• Dostawca musi zapewnić swoim pracownikom podstawowe szkolenie w zakresie bezpieczeństwa co najmniej raz w roku, upewniając się, że są oni świadomi:<br>○ Ryzyko związane z phishingiem<br>○ Bezpiecznego przechowywania haseł<br>○ Stosowania silnych haseł<br>○ inżynierii społecznej<br>○ Media społecznościowe |
| **Ryzyko związane z cyberbezpieczeństwem i zarządzanie incydentami** | • Dostawca powinien zidentyfikować zagrożenia dla cyberbezpieczeństwa i podjąć odpowiednie działania w celu zapobiegania wszelkim incydentom związanym z bezpieczeństwem.<br>• W przypadku, gdy dostawca jest zaangażowany w incydent bezpieczeństwa, który ma wpływ na Nemak, wówczas dostawca, we współpracy z CSIRT, podejmuje działania mające na celu przywrócenie normalnego funkcjonowania.<br>• Dostawca niezwłocznie powiadamia Nemak o wszelkich rzeczywistych lub potencjalnych incydentach związanych z cyberbezpieczeństwem i naruszeniach danych. |
| **Ciągłość działania** | • Dostawca opracuje plany ciągłości działania dla systemów krytycznych. Plany te będą obejmowały między innymi procedury odzyskiwania danych po awarii, które będą testowane co najmniej raz w roku. |
| **Audyt** | • Nemak ma prawo do:<br>○ Przeprowadzania audytu wyników dostawcy i zgodności z niniejszymi wytycznymi bezpieczeństwa.<br>○ Żądania dostępu do raportów/certyfikatów stron trzecich, które potwierdzają zgodność z kontrolami związanymi ze świadczeniem usług lub dostawą produktów. |
| **Zgodność** | • Dostawca zobowiązuje się do właściwego korzystania z wszelkich praw własności intelektualnej i praw autorskich Nemak oraz stron trzecich.<br>• Dostawca ponosi odpowiedzialność wobec Nemak za wszelkie naruszenia obowiązków określonych w niniejszych wytycznych dotyczących bezpieczeństwa. |

- Nieprzestrzeganie niniejszych wytycznych dotyczących bezpieczeństwa przez dostawcę lub któregokolwiek z jego podwykonawców może skutkować karami określonymi w umowie i obowiązujących przepisach prawa.
- Dostawca zgadza się zwolnić firmę Nemak z odpowiedzialności, bronić jej i zabezpieczyć przed wszelkimi roszczeniami wynikającymi z naruszenia niniejszych wytycznych dotyczących bezpieczeństwa.
- Niniejsze wytyczne dotyczące bezpieczeństwa mogą być od czasu do czasu aktualizowane. Dostawca zobowiązuje się przestrzegać niniejszych wytycznych dotyczących bezpieczeństwa przez cały okres utrzymywania stosunków handlowych z Nemak.

**Dane kontaktowe** W przypadku pytań lub uwag dotyczących niniejszych wytycznych prosimy o kontakt z działem bezpieczeństwa informacji firmy Nemak pod adresemisec.suppliers@nemak.com .

**Zmiany**

| Wersja | Data | Wnioskodawca | Opis zmian |
|---|---|---|---|
| 1.0 | Lipiec 2022 | Ricardo Serrano | Opracowanie wytycznych |
| 2.0 | Sierpień/2022 | Edwin Macias | Format dokumentu zmieniono na wytyczne |
| 3.0 | Marzec 2023 | Edwin Macias | Zmieniono sekcję *„Logiczna kontrola dostępu”*:<br>Tekst dotyczący zakończenia świadczenia usług przez dostawcę lub podwykonawców został ponownie zdefiniowany. |
| 4.0 | Styczeń/2024 | Omar Duran | Dodano sekcję *„Korzystanie z usług w chmurze”.* |
| 4.0 | Styczeń/2025 | Omar Duran | Przegląd zakończony. Nie stwierdzono żadnych zmian. Brak zmian w wersji dokumentu<br>Usunięto rosyjskie tłumaczenie. |
| 5.0 | Styczeń/2026 | Gerardo Vasquez | Sekcja „Wprowadzenie i cel” została zastąpiona sekcją „Cel”.<br>Zaktualizowano treść sekcji „Cel”. |

Niniejszy dokument jest zgodny z ogólnym procesem zarządzania dokumentami opisanym w:

NPO-GBL-SEC-10 Polityka zarządzania dokumentami

**Zatwierdzono**

| Wersja | Data | Imię i nazwisko osoby zatwierdzającej |
|---|---|---|
| 1.0 | Lipiec 2022 | Edwin Macias |
| 2.0 | Sierpień 2022 | Alejandro Valdes Flores |
| 3,0 | Marzec/2023 | Alejandro Valdes Flores |

| | | |
|---|---|---|
| 4,0 | Styczeń/2024 | Edwin Macias |
| 4,0 | Styczeń/2025 | Edwin Macias |
| 5,0 | Styczeń/2026 | Edwin Macias |

**Ten dokument został utworzony przy użyciu narzędzia tłumaczeniowego.**

# Információbiztonsági követelmények a beszállítók számára

**2026. január**

**Cél**

Meghatározza az összes biztonsági irányelvet, amelyet be kell tartani a Nemak által közzétett információk védelme érdekében.

Ezek a biztonsági irányelvek a Nemak és a beszállító között létrejött bármely megállapodás szerves részét képezik, és a beszállító köteles ezeket betartani az információk titkosságának és integritásának védelme érdekében. Ezeket a követelményeket kiegészíthetik egyéb biztonsági követelmények, bármely szolgáltatási szintű megállapodás vagy bármely más, a Nemak és a beszállító között létrejött dokumentum.

**Hatály**

Ez a dokumentum minden olyan szállítóra vonatkozik, amely hozzáférhet vagy hozzáférhet bármilyen típusú, a Nemak tulajdonában lévő és/vagy általa közzétett információhoz.

**Kivételek**

Amennyiben egy biztonsági követelménynek nem lehet eleget tenni, azt a Nemaknak a következő e-mail címen kell jelezni, hogy az értékelje a helyzetet: isec.suppliers@nemak.com

**Fogalommeghatározások**

***Nemak***
A Nemak, S.A.B. de C.V. és leányvállalatai.

***Megállapodás***
Bármely megállapodás, megrendelés, kinevezési levél vagy egyéb dokumentum, amely meghatározza a Nemak számára történő termékek és/vagy szolgáltatások szállításának és/vagy nyújtásának feltételeit.

***CSIRT** (kiberbiztonsági incidenskezelő csapat)*
A Nemak kiberbiztonsági incidenskezelő csapata.

***Információ***
Minden bizalmas és védett információ, amely a Nemak vagy üzleti tevékenységei, ügyfelei, beszállítói vagy bármely harmadik fél birtokában van, vagy bármilyen módon kapcsolódik hozzájuk.

***Audit***
A beszállító teljesítményének és a megállapodások betartásának időszakos felülvizsgálata.

***Szállító***
Bármely természetes vagy jogi személy, amely termékeket és/vagy szolgáltatásokat nyújt a Nemak számára.

***Infrastruktúra platformok és szolgáltatások***
A Nemak rendszerei, alkalmazásai és/vagy hálózati elemei és adatbázisai.

***Fizikai erőforrások***
Kizárólag a szolgáltatások nyújtása vagy a termékek szállítása céljára használt hardver vagy fizikai berendezések (pl. számítógépek, nyomtatók, szerverek, monitorok, mobil eszközök, cserélhető adathordozók stb.

***Logikai erőforrások***
Szoftverek, rendszerek vagy alkalmazások, amelyekhez kizárólag a szolgáltatások nyújtása vagy a termékek szállítása céljából biztosítanak hozzáférést.

***SLA***
Szolgáltatási szintű megállapodás

| | |
|---|---|
| **Szerepek és felelősségek** | ***Nemak:***<br>Tájékoztatja a harmadik feleket a Nemak megfelelő szabályozásairól és intézkedéseiről<br>***Szállító:***<br>Biztosítja az információbiztonsági követelmények betartását |
| **Általános követelmények** | • A beszállító minden szükséges intézkedést megtesz az általa hozzáférhető információk védelme érdekében, ideértve a Nemak infrastruktúrájának platformjait és szolgáltatásait is, függetlenül attól, hogy azok szolgáltatásnyújtásból, termékellátásból vagy bármely más okból származnak, amely miatt a beszállítónak hozzáférése van a Nemak információihoz, platformjaihoz és/vagy infrastruktúra-szolgáltatásaihoz.<br>• A szállító köteles betartani, és alvállalkozóit is köteles rávenni a jelen dokumentumban meghatározott biztonsági irányelvek betartására, és köteles megőrizni a betartást igazoló bizonyítékokat.<br>• Mindig tartsa be ezeket a biztonsági irányelveket, még akkor is, ha a szolgáltatások hatókörét a Nemak és a szállító módosította.<br>• Írja alá a Nemak globális üzleti kódexét a beszállítók számára, azzal a megértéssel, hogy csak azok a biztonsági irányelvek alkalmazandók a beszállítóra, amelyek a nyújtandó szolgáltatásokra vonatkoznak. |
| **Titoktartás** | • A Szállító tudomásul veszi, hogy a Nemak által közzétett információk, amelyekhez a Szállító, alkalmazottai vagy alvállalkozói hozzáférnek és/vagy hozzáférni fognak, a Nemak, ügyfelei, beszállítói és/vagy harmadik felek tulajdonát képezik, és titoktartási kötelezettségek védik őket.<br>• A Szállító köteles olyan irányelveket, eljárásokat és ellenőrzési mechanizmusokat létrehozni, amelyek megakadályozzák az információkhoz hozzáféréssel rendelkező alkalmazottak vagy alvállalkozói személyzet által történő jogosulatlan közzétételét.<br>• Az információkhoz, valamint az infrastruktúra platformjához és szolgáltatásaihoz való hozzáférés csak azoknak a munkavállalóknak és/vagy alvállalkozói személyzetnek biztosítható, akiknek ez a tudás szükséges, és kizárólag a szolgáltatások nyújtása vagy a termékek szállítása céljából.<br>• A Szállító kijelenti és szavatolja, hogy a személyes adatok vagy bizalmas információk kizárólag üzleti célokra, a felek közötti megállapodásoknak, valamint a Nemak irányelveinek és az alkalmazandó jogszabályoknak szigorúan megfelelően használhatók fel.<br>• A Szállító egy vagy több titoktartási megállapodás megkötésével biztosítja az általa hozzáférhető információk titkosságát.<br>• A Szállító proaktív intézkedéseket hoz a termékek és/vagy szolgáltatások szállítása céljából neki átadott személyes adatok vagy bizalmas információk megfelelő védelme érdekében. |
| **Fizikai biztonság** | • A szállító biztosítja, hogy a személyes adatokhoz és a bizalmas információkhoz csak az arra jogosult személyzet férhessen hozzá, a szükséges mértékben.<br>• A szállító megteszi a szükséges intézkedéseket saját létesítményeinek, informatikai berendezéseinek és infrastruktúrájának védelme érdekében.<br>• A szállító és/vagy az alvállalkozói személyzetnek mindig be kell tartania a Nemak fizikai biztonsági irányelveit és eljárásait. |
| **A szállító személyzete** | • A szállító személyzete köteles elkerülni a Nemak globális üzleti kódexében a szállítók számára előírt összeférhetetlenségeket. |

| | |
|---|---|
| | • A szállító felelős azért, hogy személyzete kompetens és/vagy tanúsított legyen a szolgáltatások nyújtásához, és hogy ezt a szintet a megállapodás időtartama alatt fenntartsa. A személyzet kompetenciáját és/vagy tanúsítását a Nemak számára kielégítő módon kell igazolni.<br>• A szállító írásban tájékoztatja személyzetét a jelen dokumentum tartalmáról. Amennyiben szükséges, a Nemak írásban kérheti a szállítótól, hogy erősítse meg, hogy tájékoztatta személyzetét a jelen dokumentum tartalmáról, és a szállító köteles biztosítani, hogy személyzete vagy alvállalkozói szigorúan betartják és betartatják azt. |
| **IT-infrastruktúra elfogadható használati szabályzata** | • A szállító köteles a Nemak által biztosított fizikai és logikai erőforrásokat mindig megfelelően használni. |
| **Logikai hozzáférés-ellenőrzés** | • A szállító alkalmazottai és/vagy alvállalkozói kötelesek elfogadni az információbiztonsági követelményeket. Az ilyen feltételek elfogadásának bizonyítékát bármely audit vagy egyéb célból rendelkezésre kell bocsátani.<br>• A Szállító vállalja, hogy saját infrastruktúra-rendszereiben jelszó-politikát alkalmaz, amelynek kritériumai a következők:<br>○ Minimum 10 karakter hosszúság, legalább egy karakterrel mindhárom 3 karakteres csoportból (kisbetű, nagybetű, szám).<br>○ A rendszereket úgy kell konfigurálni, hogy legalább 12 havonta jelszóváltást igényeljenek, vagy azonnal, ha a legkisebb jel is utal arra, hogy a jelszó bármilyen módon kompromittálódott, vagy ha kétség merül fel, hogy egy harmadik fél ismerheti azt.<br>• A szolgáltatások vagy a szerződés megszűnése esetén a Szállító köteles letiltani vagy törölni a munkavállalók vagy harmadik felek fiókjait, amelyek a Szállító IT-infrastruktúráját használják.<br>• Ha a Nemak fiókokat és jelszavakat biztosít a Nemak rendszereihez való csatlakozáshoz, azokat nem szabad közölni és/vagy megosztani harmadik felekkel vagy a Szállító olyan alkalmazottaival, akik nem vesznek részt a szolgáltatások nyújtásában vagy a termékek szállításában. A Nemak által biztosított egyéni fiókokat nem szabad közölni és/vagy megosztani az alkalmazottak között, még akkor sem, ha azok részt vesznek a szolgáltatások nyújtásában vagy a termékek szállításában.<br>• A Szállító felelős minden olyan tevékenységért, amelyet a Nemak által a Szállító személyzetének biztosított fiókokkal és jelszavakkal végeznek.<br>• A Nemak megszünteti a Szállító hozzáférését az Információkhoz, ha:<br>○ A cél teljesült.<br>○ A Szállító megsérti ezeket a biztonsági irányelveket.<br>○ Bármilyen gyanús tevékenységet észlelnek.<br>○ A Nemak úgy ítéli meg, hogy az célszerű.<br>• Abban az esetben, ha a Nemak felhasználói fiókokat (pl. Active Directory fiókok, VPN-hozzáférés, e-mail stb.) biztosít a Szállító vagy a Szállító alvállalkozói számára, a Szállító köteles haladéktalanul értesíteni a Nemakot, ha az alábbiak bármelyike fennáll:<br>○ Az alkalmazott vagy alvállalkozói harmadik fél munkaviszonya megszűnik, vagy már nem áll szerződéses kapcsolatban a szállítóval. |

- Az alkalmazott vagy alvállalkozó harmadik fél már nem nyújt szolgáltatásokat a Nemaknak.

Az értesítéseket a Nemak beszállítói kapcsolattartó menedzserének és a Nemak információbiztonsági osztályának kell elküldeni: isec.suppliers@nemak.com

**IT-infrastruktúra menedzsment**

*Hálózati hozzáférés*

- A beszállítói hálózatot tűzfalakkal kell védeni, és csak a beszállító személyzete férhet hozzá.
- A beszállító személyzete aktív könyvtár felhasználóval csatlakozhat a hálózathoz.

*Biztonságos törlés*

- A Nemakkal fennálló üzleti kapcsolat megszűnésekor, vagy a Nemak kérésére, attól függően, hogy melyik következik be előbb, a szállító köteles az információk biztonságos törlését alkalmazni az információk megfelelő törlésének (vagy adott esetben visszajuttatásának) biztosítása érdekében.

*Rosszindulatú szoftverek elleni védelem*

- A Szállító a szolgáltatások nyújtásához vagy a termékek szállításához használt termékeket és berendezéseket a gyártó által biztosított legújabb kártevőirtó verziókkal és frissítésekkel tartja karban. A számítógépes berendezések tűzfalát engedélyezni kell, hogy blokkolja a kártevő szoftverek támadásait.

*Sebezhetőségkezelés*

- A szállító köteles az IT-infrastruktúrában sebezhetőségeket keresni, hogy felismerje, jelentsen és orvosolja a szolgáltatások nyújtása vagy a termékek szállítása során, valamint a szolgáltatások nyújtásához vagy a termékek szállításához használt berendezésekben talált sebezhetőségeket.
- A szállító köteles sebezhetőségek esetén javítási tervet végrehajtani.

*Rendszerjavítások*

- A szállító köteles gondoskodni arról, hogy a szerverek, a felhasználói számítógépek és a mobil eszközök legfeljebb 60 nappal a javítás kiadása után frissítésre kerüljenek.

*VPN-hozzáférés eltávolítása*

- A szállító vállalja, hogy VPN-hez való csatlakozáshoz kizárólag Active Directory hitelesítést használ, és más csatlakozási lehetőségeket nem. Ha lehetséges, a szállító többfaktoros hitelesítést használ a VPN-hez.
- A VPN-hozzáférés nem osztható meg más személyekkel.

**Felhőszolgáltatások használata**

Felhőszolgáltatók esetében a Szállító vállalja, hogy a Nemak adatainak védelme és a szolgáltatások rendelkezésre állása érdekében a következő rendelkezéseket alkalmazza:

- Dedikált támogatást nyújt a felhőszolgáltatási környezetben bekövetkező információbiztonsági incidensek esetén.
- Támogatja a szervezetet a digitális bizonyítékok gyűjtésében, figyelembe véve a különböző joghatóságok digitális bizonyítékokra vonatkozó törvényeit és rendeleteit.

| | |
|---|---|
| | • Biztosítja az adatok és konfigurációs információk szükséges biztonsági mentését, és a biztonsági mentéseket a vonatkozó előírásoknak megfelelően kezeli.<br>• A szolgáltatásnyújtás során vagy a szolgáltatás megszűnésekor kérésre biztosítja és visszajuttatja a szervezet tulajdonában lévő információkat, például konfigurációs fájlokat, forráskódokat, naplófájlokat és adatokat.<br>A felhőszolgáltató köteles minden esetben értesíteni:<br>• A technikai infrastruktúra olyan változásait (pl. áthelyezés, újrakonfigurálás, hardver- vagy szoftverváltozások), amelyek befolyásolják vagy megváltoztatják a felhőszolgáltatás kínálatát.<br>• Az információk feldolgozása vagy tárolása új földrajzi vagy jogi joghatóságban.<br>• Párhuzamos felhőszolgáltatók vagy más alvállalkozók igénybevétele (beleértve a meglévők cseréjét vagy új felek igénybevételét). |
| **Információbiztonsági tudatosság** | • A szállító köteles (minden alkalmazottja számára) tudatosságnövelő és oktatási programokat megvalósítani az információbiztonság, a megelőző intézkedések, valamint az információk osztályozására és kezelésére vonatkozó irányelvek, eljárások és ellenőrzések tekintetében.<br>• A szállító köteles legalább évente egyszer alapvető biztonsági képzést biztosítani alkalmazottai számára, biztosítva, hogy azok tisztában legyenek a következőekkel:<br>○ Az adathalászati kockázatok<br>○ Jelszavuk biztonságos tárolása<br>○ Erős jelszavak használata<br>○ Szociális mérnöki munka<br>○ Közösségi média |
| **Kiberbiztonsági kockázatok és incidenskezelés** | • A szállító köteles azonosítani a kiberbiztonsági kockázatokat és megtenni a megfelelő intézkedéseket a biztonsági incidensek megelőzése érdekében.<br>• Amennyiben a Szállító olyan biztonsági incidensbe keveredik, amely hatással van a Nemakra, akkor a Szállító a CSIRT-tel együttműködve köteles mindent megtenni a normális működés visszaállításához.<br>• A szállító köteles haladéktalanul értesíteni a Nemakot minden tényleges vagy potenciális kiberbiztonsági incidensről és adatvédelmi incidensről. |
| **Üzletmenet-folytonosság** | • A szállító köteles üzletmenet-folytonossági terveket kidolgozni a kritikus rendszerekre vonatkozóan. Ezeknek a terveknek tartalmazniuk kell, de nem kizárólagosan, legalább évente egyszer tesztelt katasztrófa-elhárítási eljárásokat. |
| **Audit** | • A Nemak jogosult:<br>○ A szállító teljesítményének és a biztonsági irányelvek betartásának ellenőrzése.<br>○ Hozzáférés kérése olyan harmadik felek jelentéseihez/tanúsítványaihoz, amelyek igazolják a szolgáltatások nyújtásával vagy termékek szállításával kapcsolatos ellenőrzések betartását. |
| **Megfelelés** | • A szállító köteles a Nemak és harmadik felek szellemi tulajdonjogait és szerzői jogait megfelelően használni.<br>• A szállító felelősséggel tartozik a Nemak felé a jelen biztonsági irányelvekben meghatározott kötelezettségeinek bármely megsértése esetén. |

- Ha a szállító vagy bármely alvállalkozója nem tartja be a biztonsági irányelveket, az a megállapodásban és az alkalmazandó jogszabályokban meghatározott szankciókat vonhat maga után.
- A szállító vállalja, hogy kártalanítja, védi és mentesíti a Nemakot minden olyan igény alól, amely a jelen biztonsági irányelvek megsértéséből ered.
- A jelen biztonsági irányelvek időről időre frissülhetnek. A szállító köteles betartani a jelen biztonsági irányelveket mindaddig, amíg üzleti kapcsolatban áll a Nemakkal.

**Kapcsolat** Ha kérdése vagy észrevétele van a jelen irányelvvel kapcsolatban, kérjük, forduljon a Nemak információbiztonsági osztályához aisec.suppliers@nemak.com e-mail címen.

**Módosítások**

| Verzió | Dátum | Kérő | A változások leírása |
|---|---|---|---|
| 1.0 | 2022. július | Ricardo Serrano | Irányelv kidolgozása |
| 2.0 | 2022. augusztus | Edwin Macias | A dokumentum formátuma irányelvre változott |
| 3.0 | 2023. március | Edwin Macias | A *logikai hozzáférés-vezérlés* szakasz módosítása:<br>A Szállító vagy alvállalkozói harmadik felek szolgáltatásainak megszűnésével kapcsolatos szöveg újra lett definiálva. |
| 4.0 | 2024. január | Omar Duran | *Felhőszolgáltatások használata* szakasz hozzáadva |
| 4.0 | 2025. január | Omar Duran | A felülvizsgálat befejeződött. Nincs azonosított változás. A dokumentum verziója nem változott.<br>Az orosz fordítás eltávolítva |
| 5.0 | 2026. január | Gerardo Vasquez | A Bevezetés és célkitűzés szakasz helyébe a Célkitűzés szakasz lépett. A Célkitűzés szakasz tartalma frissült |

Ez a dokumentum az alábbi dokumentumban leírt általános dokumentumkezelési folyamatot követi:

NPO-GBL-SEC-10 Dokumentumkezelési politika

**Jóváhagyta**

| Verzió | Dátum | Jóváhagyó neve |
|---|---|---|
| 1.0 | 2022. július | Edwin Macias |
| 2.0 | 2022. augusztus | Alejandro Valdes Flores |
| 3,0 | 2023. március | Alejandro Valdes Flores |
| 4,0 | 2024. január | Edwin Macias |
| 4,0 | Január/2025 | Edwin Macias |
| 5,0 | Január/2026 | Edwin Macias |

**Ez a dokumentum fordítóeszköz segítségével készült.**

# 供应商信息安全要求

**2026年1月**

| | |
|---|---|
| **目标** | 明确所有必须遵守的安全准则，以保护Nemak披露的信息。<br><br>这些安全准则构成Nemak与供应商之间签订的任何协议的组成部分，供应商应遵守这些准则以保护信息的机密性和完整性。这些要求可通过其他安全要求、任何服务级别协议或Nemak与供应商之间商定的任何其他文件进行补充。 |
| **适用范围** | 本文件适用于所有已接触或可能接触Nemak拥有及/或披露的任何类型信息的供应商。 |
| **例外情况** | 若无法满足某项安全要求，应通过以下邮箱通知Nemak进行相应评估：<br>isec.suppliers@nemak.com |
| **定义** | ***Nemak***<br>Nemak股份有限公司及其子公司。<br><br>***协议***<br>任何协议、采购订单、提名函或其他文件，其中规定向Nemak供应产品和/或提供服务的条款和条件。<br><br>***CSIRT（网络安全事件响应团队）***<br>Nemak 的网络安全事件响应团队。<br><br>***信息***<br>由Nemak持有或以任何形式关联于Nemak及其业务、客户、供应商或任何第三方之所有机密及专有信息。<br><br>***审计***<br>对供应商绩效及协议合规性的定期审查。<br><br>***供应商***<br>向Nemak提供产品和/或服务的任何自然人或法人实体。<br><br>***基础设施平台与服务***<br>Nemak的系统、应用程序和/或网络元素及数据库。<br><br>***物理资源***<br>仅用于提供服务或供应产品的硬件或物理设备（例如计算机、打印机、服务器、显示器、移动设备、可移动存储介质等）。<br><br>***逻辑资源***<br>仅为提供服务或供应产品而授予访问权限的软件、系统或应用程序。 |

| | |
|---|---|
| | ***SLA***<br>服务等级协议 |
| **角色与职责** | ***Nemak：***<br>向第三方传达Nemak的适用法规与措施<br>***供应商：***<br>确保信息安全要求的合规性 |
| **基本要求** | • 供应商应采取一切必要措施保护其接触到的任何信息，包括内马克基础设施的平台与服务。无论该信息源于服务提供、产品供应或其他任何需要访问内马克信息、平台及/或基础设施服务的情形。<br>• 供应商应遵守本文件规定的安全指南，并确保分包商遵守，同时保留证明合规性的证据。<br>• 即使Nemak与供应商修改了服务范围，仍须始终遵守本安全指南。<br>• 签署内马克《供应商全球商业守则》，但需理解仅与所提供服务相关的安全准则适用于供应商。 |
| **保密性** | • 供应商承认，由Nemak披露且供应商、其雇员或分包商人员已接触或将接触的信息，均属于Nemak、其客户、供应商及/或第三方所有，并受保密承诺保护。<br>• 供应商应制定政策、程序和控制措施，防止接触信息的员工或分包人员擅自披露信息。<br>• 只有供应商根据需要知情，且仅限于提供服务或供应产品，才可授予其员工和/或分包人员访问信息、基础设施平台和服务。<br>• 供应商声明并保证，个人数据或保密信息仅可用于商业目的，并严格遵守双方之间的任何协议、Nemak 的任何政策以及适用法律。<br>• 供应商应通过签署一项或多项保密协议，确保其接触到的信息保密。<br>• 供应商应采取主动措施，正确保护为供应产品和/或服务而向其披露的个人数据或机密信息。 |
| **物理安全** | • 供应商应确保个人数据和机密信息仅在需要知情的基础上由授权人员访问。<br>• 供应商应采取必要措施保护其自身设施、IT 设备和基础设施。<br>• 供应商和/或分包商人员应始终遵守 Nemak 的物理安全政策和程序。 |
| **供应商人员** | • 供应商人员应避免任何与Nemak《全球供应商商业行为准则》所述利益冲突的情况。<br>• 供应商须确保其员工具备提供服务的资质和/或认证，并在协议有效期内维持该资质水平。员工资质和/或认证须能向Nemak提供令人满意的证明。 |

| | |
|---|---|
| | • 供应商须以书面形式向其人员传达本文件内容。若Nemak提出要求，供应商应书面确认已向人员传达本文件内容，并确保其人员或分包人员严格遵守本文件规定。 |
| **IT基础设施可接受使用政策** | • 供应商须始终善用Nemak提供的物理及逻辑资源 |
| **逻辑访问控制** | • 供应商员工及/或分包人员必须接受信息安全要求。若审计或其他目的需要，应能提供接受此类条款和条件的证明。<br>• 供应商承诺在其自有基础设施系统中制定密码政策，具体标准如下：<br>  ○ 密码长度至少10位，且必须包含以下三类字符各一位：小写字母、大写字母、数字。<br>  ○ 系统应配置为要求密码至少每12个月更改一次，或在出现任何密码泄露迹象时立即更改，或当存在第三方可能知晓密码的疑虑时立即更改。<br>• 服务或合同终止时，供应商应停用或注销员工及第三方访问供应商IT基础设施的账户。<br>• 若Nemak提供连接其系统的账户及密码，该信息不得向任何第三方或非服务/产品供应环节的供应商员工披露及/或共享。对于Nemak授予的个人账户，即使涉及服务/产品供应环节，亦不得在员工间披露及/或共享。<br>• 供应商应对使用Nemak提供给其员工的账户及密码所进行的任何活动承担责任。<br>• 当出现以下情形时，Nemak将终止供应商对信息的访问权限：<br>  ○ 使用目的已达成。<br>  ○ 供应商违反本安全指南。<br>  ○ 检测到任何可疑活动时。<br>  ○ 当Nemak认为合适时。<br>• 若Nemak向供应商或其分包第三方提供用户账户（如Active Directory账户、VPN访问权限、电子邮箱等），当出现以下任一情况时，供应商须立即通知Nemak：<br>  ○ 该员工或分包第三方已被解雇或与供应商终止合同关系。<br>  ○ 该员工或分包第三方不再为Nemak提供服务。<br>  通知须同时发送至Nemak供应商联络经理及信息安全部门：isec.suppliers@nemak.com |
| **IT基础设施管理** | *网络访问*<br>供应商网络应受防火墙保护，仅允许供应商人员访问。 |

- 供应商网络应受防火墙保护，仅限供应商人员访问。
- 供应商人员应使用活动目录用户连接网络。

*安全擦除*

- 在与 Nemak 的业务关系终止时，或 Nemak 提出要求时（以先发生者为准），供应商应执行信息安全擦除，确保信息被正确删除（或返还，如适用）。

*反恶意软件保护*

- 供应商须确保用于提供服务或供应产品的设备及系统始终安装制造商提供的最新反恶意软件版本及更新。计算机设备中的防火墙必须处于启用状态，以阻断任何恶意软件入侵企图。

*漏洞管理*

- 供应商应扫描IT基础设施中的漏洞，以检测、通知并修复在提供服务或供应产品过程中发现的漏洞，以及在供应商用于提供服务或供应产品的设备中发现的漏洞。
- 供应商应制定漏洞修复方案以应对任何漏洞问题。

*系统补丁更新*

- 供应商应确保服务器、用户个人电脑及移动设备在补丁发布后60天内完成补丁安装。

*移除VPN访问权限*

- 供应商同意仅通过Active Directory身份验证使用VPN连接其设施，不得采用其他连接方式。在条件允许的情况下，供应商应启用VPN的多因素身份验证。
- VPN访问权限不得在个人间共享。

**云服务使用**

针对云服务提供商，供应商同意纳入以下条款以保障Nemak数据安全及服务可用性：

- 在云服务环境发生信息安全事件时提供专属支持。
- 协助组织收集数字证据，同时考虑不同司法管辖区对数字证据的法律法规要求。
- 按需提供数据及配置信息的备份，并确保备份的安全管理。
- 在服务期间或终止服务时，应要求提供并归还组织拥有的配置文件、源代码、日志及数据等信息。

云服务提供商必须及时通知：

- 影响或变更云服务的技术基础设施变更（如迁移、重组或软硬件变更）。

| | |
|---|---|
| | • 在新的地理区域或法律管辖区处理或存储信息。<br>• 使用同类云服务提供商或其他分包商（包括变更现有合作方或引入新合作方）。 |
| **信息安全意识** | • 供应商应针对信息安全实施员工培训计划，涵盖预防措施的落实，并制定信息分类与管理的相关政策、流程及管控措施。<br>• 供应商必须每年至少为员工提供一次基础安全培训，确保其了解：<br>○ 网络钓鱼风险<br>○ 密码安全防护<br>○ 使用强密码<br>○ 社会工程学攻击<br>○ 社交媒体 |
| **网络安全风险与事件管理** | • 供应商应识别网络安全风险，并采取适当措施防止任何安全事件发生。<br>• 若供应商涉及影响Nemak的安全事件，则应协同CSIRT共同恢复正常运营。<br>• 供应商应立即向Nemak通报任何实际或潜在的网络安全事件及数据泄露。 |
| **业务连续性** | • 供应商应为关键系统制定业务连续性计划。这些计划应包括但不限于每年至少测试一次的灾难恢复程序。 |
| **审计** | • Nemak有权：<br>○ 审核供应商的绩效及对本《安全指南》的遵守情况。<br>○ 要求查阅第三方出具的报告/证书，以验证其在提供服务或供应产品过程中所实施的控制措施是否符合要求。 |
| **合规** | • 供应商应善用Nemak及第三方拥有的任何知识产权和著作权。<br>• 供应商须对违反本安全指南所述责任的行为向Nemak承担责任。<br>• 供应商或其分包人员未遵守本安全准则，可能导致协议和适用法律规定的处罚。<br>• 供应商同意，若因违反本安全准则引发任何索赔，将赔偿、辩护并使Nemak免受损害。<br>• 本安全指南可能不时更新。供应商在与 Nemak 保持业务关系期间，应遵守本安全指南。 |
| **联系方式** | 如对本指南有任何疑问或意见，请通过isec.suppliers@nemak.com 联系 Nemak 信息安全部门。 |

**修订**

| 版本 | 日期 | 申请者 | 变更说明 |
|---|---|---|---|
| 1.0 | 2022年7月 | 里卡多·塞拉诺 | 指南的制定 |
| 2.0 | 2022年8月 | 埃德温·马西亚斯 | 文档格式更改为指南 |
| 3.0 | 2023年3月 | 埃德温·马西亚斯 | *逻辑访问控制*章节变更：<br>关于供应商或分包第三方终止服务的条款已重新定义。 |
| 4.0 | 2024年1月 | 奥马尔·杜兰 | 新增*云服务使用*章节 |
| 4.0 | 2025年1月 | 奥马尔·杜兰 | 审核完成。未发现需修改之处。文档版本保持不变<br>移除俄语译文 |
| 5.0 | 2026年1月 | 赫拉尔多·瓦斯奎兹 | "引言与目的"章节已替换为"目标"章节<br>目标部分内容已更新 |

本文件遵循以下文件所述的通用文档管理流程：

NPO-GBL-SEC-10 文件管理政策

**批准人**

| 版本 | 日期 | 审批人姓名 |
|---|---|---|
| 1.0 | 2022年7月 | 埃德温·马西亚斯 |
| 2.0 | 2022年8月 | 亚历杭德罗·瓦尔德斯·弗洛雷斯 |
| 3.0 | 2023年3月 | 亚历杭德罗·瓦尔德斯·弗洛雷斯 |
| 4.0 | 2024年1月 | 埃德温·马西亚斯 |
| 4.0 | 2025年1月 | 埃德温·马西亚斯 |
| 5.0 | 2026年1月 | 埃德温·马西亚斯 |

**本文件由翻译工具生成**

# Tedarikçiler için Bilgi Güvenliği Gereklilikleri

**Ocak 2026**

**Amaç**

Nemak tarafından açıklanan bilgileri korumak için uyulması gereken tüm Güvenlik Yönergelerini tanımlamak.

Bu Güvenlik Yönergeleri, Nemak ve Tedarikçi arasında yapılan herhangi bir anlaşmanın ayrılmaz bir parçasını oluşturur ve Tedarikçi, Bilgilerin gizliliğini ve bütünlüğünü korumak için bunlara uymakla yükümlüdür. Bu gereklilikler, diğer güvenlik gereklilikleri, herhangi bir hizmet seviyesi anlaşması veya Nemak ve Tedarikçi arasında mutabık kalınan diğer belgelerle desteklenebilir.

**Kapsam**

Bu belge, Nemak'ın sahip olduğu ve/veya ifşa ettiği her türlü bilgiye erişimi olan veya olabilecek tüm Tedarikçiler için geçerlidir.

**İstisnalar**

Bir güvenlik gerekliliğine uymak mümkün değilse, ilgili değerlendirme için Nemak'a aşağıdaki e-posta adresinden bildirimde bulunulmalıdır: isec.suppliers@nemak.com

**Tanım**

***Nemak***
Nemak, S.A.B. de C.V. ve bağlı şirketleri.

***Anlaşma***
Nemak'a ürün ve/veya hizmetlerin tedarik edileceği ve/veya sunulacağı şart ve koşulları belirleyen herhangi bir anlaşma, satın alma siparişi, adaylık mektubu veya diğer belgeler.

***CSIRT** (Siber Güvenlik Olaylarına Müdahale Ekibi)*
Nemak'ın Siber Güvenlik Olaylarına Müdahale Ekibi.

***Bilgi***
Nemak veya işleri, müşterileri, tedarikçileri veya herhangi bir üçüncü taraf tarafından sahip olunan ve herhangi bir şekilde bunlarla ilgili tüm gizli ve özel bilgiler.

***Denetim***
Tedarikçinin performansının ve herhangi bir Anlaşmaya uygunluğunun periyodik olarak gözden geçirilmesi.

***Tedarikçi***
Nemak'a ürün ve/veya hizmet sağlayan herhangi bir gerçek veya tüzel kişi.

***Altyapı Platformları ve Hizmetleri***
Nemak'ın sistemleri, uygulamaları ve/veya ağ öğeleri ve veritabanları.

***Fiziksel Kaynaklar***
Yalnızca hizmetlerin sağlanması veya ürünlerin tedariki amacıyla kullanılan donanım veya fiziksel ekipman (ör. bilgisayarlar, yazıcılar, sunucular, monitörler, mobil cihazlar, çıkarılabilir depolama ortamları vb.

***Mantıksal Kaynaklar***
Yalnızca hizmetlerin sağlanması veya ürünlerin tedariki amacıyla erişim izni verilen yazılımlar, sistemler veya uygulamalar.

***SLA***
Hizmet Seviyesi Anlaşması

| | |
|---|---|
| **Roller ve Sorumluluklar** | ***Nemak:***<br>Nemak'ın uygun düzenlemelerini ve önlemlerini üçüncü taraflara iletir.<br>***Tedarikçi:***<br>Bilgi güvenliği gerekliliklerine uyulmasını sağlar |
| **Genel Gereklilikler** | • Tedarikçi, hizmetlerin sağlanması veya ürünlerin tedarikinden kaynaklanan veya Tedarikçinin Nemak'ın Bilgi, Platform ve/veya Altyapı Hizmetlerine erişmesi gereken diğer herhangi bir nedenden kaynaklanan, Nemak Altyapısının Platformları ve Hizmetleri dahil olmak üzere erişimi olan tüm Bilgileri korumak için gerekli tüm önlemleri alacaktır.<br>• Tedarikçi, burada belirtilen Güvenlik Yönergelerine uyacak ve alt yüklenicilerin de uymasını sağlayacak ve bu uyumu gösteren kanıtları saklayacaktır.<br>• Hizmetlerin kapsamı Nemak ve Tedarikçi tarafından değiştirilmiş olsa bile, bu Güvenlik Yönergelerine her zaman uyun.<br>• Nemak'ın Tedarikçiler için Küresel İş Kuralları'nı imzalayın; ancak, yalnızca sunulacak hizmetlerle ilgili Güvenlik Yönergeleri Tedarikçi için geçerli olacaktır. |
| **Gizlilik** | • Tedarikçi, Tedarikçi, çalışanları veya alt yüklenici personelinin erişimi olan ve/veya erişimi olacak Nemak tarafından açıklanan Bilgilerin Nemak, müşterileri, tedarikçileri ve/veya üçüncü şahısların mülkiyeti olduğunu ve gizlilik taahhütleri ile korunduğunu kabul eder.<br>• Tedarikçi, Bilgiye erişimi olan çalışanları veya alt yüklenici personeli tarafından Bilginin yetkisiz olarak ifşa edilmesini önlemek için politikalar, prosedürler ve kontroller oluşturacaktır.<br>• Bilgiye ve Altyapı Platformu ile Hizmetlere erişim, yalnızca Tedarikçi tarafından alt yüklenici olarak görevlendirilen çalışanlara ve/veya personele, bilmesi gerekenler temelinde ve yalnızca hizmetlerin sağlanması veya ürünlerin tedariki ile ilgili olarak verilecektir.<br>• Tedarikçi, kişisel verilerin veya gizli bilgilerin yalnızca iş amaçları için ve taraflar arasındaki Anlaşmalar ile Nemak politikaları ve geçerli yasalarla tam uyum içinde kullanılabileceğini beyan ve taahhüt eder.<br>• Tedarikçi, bir veya birkaç gizlilik anlaşması imzalayarak erişimi olan Bilgilerin gizliliğini sağlayacaktır.<br>• Tedarikçi, ürün ve/veya hizmetlerin tedariki amacıyla kendisine ifşa edilen kişisel verileri veya gizli bilgileri doğru bir şekilde korumak için proaktif önlemler alacaktır. |
| **Fiziksel Güvenlik** | • Tedarikçi, kişisel verilere ve gizli bilgilere yalnızca ihtiyaç duyduğu ölçüde yetkili personelin erişebilmesini sağlayacaktır.<br>• Tedarikçi, kendi tesislerini, BT ekipmanlarını ve altyapısını korumak için gerekli önlemleri alacaktır.<br>• Tedarikçi ve/veya alt yüklenici personeli, Nemak'ın Fiziksel Güvenlik politikalarına ve prosedürlerine her zaman uymalıdır. |
| **Tedarikçinin Personeli** | • Tedarikçinin personeli, Nemak'ın Tedarikçiler için Küresel İş Kuralları'nda belirtilen çıkar çatışmalarından kaçınmalıdır.<br>• Tedarikçi, personelinin hizmetlerin sağlanması için yetkin ve/veya sertifikalı olmasını ve Sözleşme süresince bu seviyeyi korumayı garanti eder. Personelin yetkinliği ve/veya sertifikası, Nemak'ı tatmin edecek şekilde kanıtlanabilmelidir. |

| | |
|---|---|
| | • Tedarikçi, personelini bu belgenin içeriği hakkında yazılı olarak bilgilendirmelidir. Gerekirse, Nemak Tedarikçiden personelini bu belgenin içeriği hakkında bilgilendirdiğini yazılı olarak teyit etmesini isteyebilir ve Tedarikçi, personelinin veya alt yüklenicilerinin bu belgeye sıkı sıkıya bağlı kalmasını ve uymasını sağlamalıdır. |
| **BT Altyapısı Kabul Edilebilir Kullanım Politikası** | • Tedarikçi, Nemak tarafından sağlanan Fiziksel ve Mantıksal Kaynakları her zaman iyi bir şekilde kullanmalıdır. |
| **Mantıksal Erişim Kontrolü** | • Tedarikçi tarafından alt yüklenici olarak görevlendirilen çalışanlar ve/veya personel, Bilgi Güvenliği gerekliliklerini kabul etmelidir. Bu şart ve koşulların kabul edildiğine dair kanıt, herhangi bir denetim veya başka bir amaçla talep edilmesi halinde sunulmalıdır.<br>• Tedarikçi, kendi altyapı sistemlerinde aşağıdaki kriterlere sahip bir şifre politikası uygulamayı kabul eder:<br>○ En az 10 karakter uzunluğunda, 3 karakterlik grupların her birinden (küçük harf, büyük harf, rakamlar) en az bir karakter içermelidir.<br>○ Sistemler, en az 12 ayda bir şifre değişikliği gerektirecek şekilde yapılandırılmalıdır veya şifrenin herhangi bir şekilde ele geçirildiğine dair en ufak bir işaret olması durumunda veya üçüncü bir tarafın şifreyi bildiğinden şüphe duyulması durumunda derhal şifre değişikliği yapılmalıdır.<br>• Hizmetlerin veya sözleşmenin sona ermesi üzerine, Tedarikçi, Tedarikçinin BT Altyapısını kullanmak üzere çalışan veya üçüncü taraf hesaplarını devre dışı bırakacak veya silecektir.<br>• Nemak, Nemak'ın sistemlerine bağlanmak için hesaplar ve şifreler sağlarsa, bunlar hizmetlerin sağlanması veya ürünlerin tedarikinde yer almayan üçüncü şahıslara veya Tedarikçinin personeline ifşa edilmeyecek ve/veya paylaşılmayacaktır. Nemak tarafından verilen kişiselleştirilmiş hesaplar, hizmetlerin sağlanması veya ürünlerin tedarikinde yer alsalar bile personel arasında ifşa edilmeyecek ve/veya paylaşılmayacaktır.<br>• Tedarikçi, Nemak tarafından Tedarikçi personeline sağlanan hesaplar ve şifrelerle gerçekleştirilen tüm faaliyetlerden sorumludur.<br>• Nemak, aşağıdaki durumlarda Tedarikçinin Bilgilere erişimini sonlandıracaktır:<br>○ Amaç yerine getirildiğinde.<br>○ Tedarikçi tarafından bu Güvenlik Yönergelerinin ihlali söz konusu olduğunda.<br>○ Herhangi bir şüpheli faaliyet tespit edildiğinde.<br>○ Nemak uygun gördüğü zaman.<br>• Nemak'ın Tedarikçiye veya Tedarikçinin alt yüklenicisi olan üçüncü taraflara kullanıcı hesapları (ör. Active Directory hesapları, VPN erişimi, e-posta vb.) sağlaması durumunda, aşağıdaki durumlardan herhangi biri geçerli olduğunda Tedarikçi derhal Nemak'a bildirimde bulunmalıdır:<br>○ Çalışan veya alt yüklenici üçüncü tarafın işine son verilmişse veya Tedarikçi ile sözleşme ilişkisi kalmamışsa.<br>○ Çalışan veya alt yüklenici üçüncü taraf artık Nemak'a hizmet sunmamaktadır.<br>Bildirimler, Nemak'ın Tedarikçi ilişki yöneticisine ve Nemak'ın Bilgi Güvenliği departmanına gönderilmelidir: isec.suppliers@nemak.com |

| | |
|---|---|
| **BT Altyapı Yönetimi** | *Ağ Erişimi*<br>• Tedarikçi ağı güvenlik duvarları ile korunacak ve yalnızca Tedarikçinin personeli tarafından erişilebilecektir.<br>• Tedarikçinin personeli, ağa bağlanmak için aktif dizin kullanıcısı kullanmalıdır.<br>*Güvenli Silme*<br>• Nemak ile iş ilişkisinin sona ermesi veya Nemak'ın talebi üzerine, hangisi önce gerçekleşirse, Tedarikçi, Bilgilerin uygun şekilde silinmesini (veya varsa iade edilmesini) sağlamak için bilgilerin güvenli silme işlemini uygulayacaktır.<br>*Kötü Amaçlı Yazılım Koruması*<br>• Tedarikçi, hizmetlerin sağlanması veya ürünlerin tedariki için kullanılan ürünleri ve ekipmanları, üretici tarafından sağlanan en son kötü amaçlı yazılımdan koruma sürümleri ve güncellemeleri ile bakımını yapacaktır. Bilgisayar ekipmanındaki güvenlik duvarı, herhangi bir kötü amaçlı yazılım girişimini engellemek için etkinleştirilmelidir.<br>*Güvenlik Açığı Yönetimi*<br>• Tedarikçi, hizmetlerin sağlanması veya ürünlerin tedarikinde ve ayrıca hizmetlerin sağlanması veya ürünlerin tedarikinde kullanılan Tedarikçinin ekipmanında bulunan güvenlik açıklarını tespit etmek, bildirmek ve gidermek için BT Altyapısı içinde güvenlik açıklarını tarayacaktır.<br>• Tedarikçi, herhangi bir güvenlik açığı durumunda bir düzeltme planı uygulamalıdır.<br>*Sistem Yama Uygulaması*<br>• Tedarikçi, sunucuların, kullanıcı bilgisayarlarının ve mobil cihazların yama yayınlandıktan sonra en geç 60 gün içinde yamalanmasını sağlayacaktır.<br>*VPN Erişiminin Kaldırılması*<br>• Tedarikçi, tesislerine bağlanmak için yalnızca Active Directory kimlik doğrulaması ile VPN kullanmayı ve başka hiçbir bağlantı seçeneğini kullanmamayı kabul eder. Mümkünse, Tedarikçi VPN ile Çok Faktörlü Kimlik Doğrulama kullanmalıdır.<br>• VPN erişimi kişiler arasında paylaşılmamalıdır. |
| **Bulut Hizmetlerinin Kullanımı** | Bulut hizmeti sağlayıcıları durumunda, Tedarikçi, Nemak'ın verilerinin korunması ve hizmetlerin kullanılabilirliği için aşağıdaki hükümleri dahil etmeyi kabul eder:<br>• Bulut hizmeti ortamında bir bilgi güvenliği olayı meydana gelmesi durumunda özel destek sağlamak.<br>• Farklı yargı bölgelerindeki dijital kanıtlarla ilgili yasa ve düzenlemeleri dikkate alarak, dijital kanıtların toplanmasında kuruluşa destek olmak.<br>• Gerekli veri ve yapılandırma bilgilerinin yedeklemesini sağlamak ve yedeklemeleri uygun şekilde güvenli bir şekilde yönetmek.<br>• Hizmet sunumu sırasında veya hizmetin sona ermesi durumunda talep edildiğinde, kuruluşa ait yapılandırma dosyaları, kaynak kodu, günlükler ve veriler gibi bilgileri sağlamak ve iade etmek. |

| | |
|---|---|
| | Bulut hizmeti sağlayıcısı her zaman aşağıdakileri bildirmelidir:<br>• Bulut hizmeti sunumunu etkileyen veya değiştiren teknik altyapıdaki değişiklikler (ör. taşınma, yeniden yapılandırma veya donanım veya yazılımdaki değişiklikler).<br>• Yeni bir coğrafi veya yasal yargı alanında bilgilerin işlenmesi veya depolanması.<br>• Eş bulut hizmeti sağlayıcılarının veya diğer alt yüklenicilerin kullanımı (mevcut tarafların değiştirilmesi veya yeni tarafların kullanılması dahil). |
| **Bilgi Güvenliği Farkındalığı** | • Tedarikçi, bilgi güvenliği, önleyici tedbirlerin alınması ve bilgilerin sınıflandırılması ve yönetilmesine ilişkin politikalar, prosedürler ve kontrollerle ilgili olarak (tüm çalışanlarına yönelik) farkındalık ve öğrenme programları uygulamalıdır.<br>• Tedarikçi, çalışanlarına yılda en az bir kez temel güvenlik eğitimi vererek aşağıdaki konularda farkındalıklarını sağlamalıdır:<br>○ Kimlik avı riskleri<br>○ Şifrelerini güvende tutma<br>○ Güçlü şifrelerin kullanımı<br>○ Sosyal mühendislik<br>○ Sosyal medya |
| **Siber güvenlik riskleri ve olay yönetimi** | • Tedarikçi, siber güvenlik risklerini belirlemeli ve herhangi bir güvenlik olayını önlemek için uygun önlemleri almalıdır.<br>• Tedarikçinin Nemak'ı etkileyen bir Güvenlik Olayına karışması durumunda, Tedarikçi CSIRT ile koordineli olarak normal faaliyetlere dönmek için birlikte çalışmalıdır.<br>• Tedarikçi, gerçek veya potansiyel siber güvenlik olaylarını ve veri ihlallerini derhal Nemak'a bildirmelidir. |
| **İş Sürekliliği** | • Tedarikçi, kritik sistemler için iş sürekliliği planları geliştirmelidir. Bu planlar, yılda en az bir kez test edilen felaket kurtarma prosedürlerini içermelidir, ancak bunlarla sınırlı değildir. |
| **Denetim** | • Nemak aşağıdaki haklara sahip olacaktır:<br>○ Tedarikçinin performansını ve bu Güvenlik Yönergelerine uygunluğunu denetlemek.<br>○ Hizmetlerin sağlanması veya ürünlerin tedarikiyle ilgili kontrollere uyumu doğrulayan üçüncü tarafların raporlarına/sertifikalarına erişim talep etmek. |
| **Uyum** | • Tedarikçi, Nemak ve üçüncü tarafların Fikri Mülkiyet Haklarını ve Telif Haklarını iyi bir şekilde kullanacaktır.<br>• Tedarikçi, bu Güvenlik Yönergelerinde belirtilen sorumluluklarının ihlali durumunda Nemak'a karşı sorumludur.<br>• Tedarikçinin veya alt yüklenicilerinin bu Güvenlik Yönergelerine uymaması, Sözleşmede ve ilgili yasalarda belirtilen cezaların uygulanmasına neden olabilir.<br>• Tedarikçi, bu Güvenlik Yönergelerinin ihlalinden kaynaklanan herhangi bir talepte Nemak'ı tazmin etmeyi, savunmayı ve zarar görmemesini sağlamayı kabul eder.<br>• Bu Güvenlik Yönergeleri zaman zaman güncellenebilir. Tedarikçi, Nemak ile iş ilişkisini sürdürdüğü sürece bu Güvenlik Yönergelerine uymakla yükümlüdür. |
| **İletişim Bilgileri** | Bu kılavuzla ilgili sorularınız veya yorumlarınız varsa, sorularınızıisec.suppliers@nemak.com adresinden Nemak Bilgi Güvenliği birimine iletebilirsiniz. |

**Revizyonlar**

| Sürüm | Tarih | Talep Eden | Değişikliklerin Açıklaması |
|---|---|---|---|
| 1.0 | Temmuz/2022 | Ricardo Serrano | Kılavuzun oluşturulması |
| 2.0 | Ağustos/2022 | Edwin Macias | Belge formatı kılavuza değiştirildi |
| 3.0 | Mart/2023 | Edwin Macias | Bölüm *Mantıksal Erişim Kontrolü* değiştirildi:<br>Tedarikçi veya Alt Yüklenici Üçüncü Tarafların hizmetlerinin sona ermesiyle ilgili metin yeniden tanımlandı. |
| 4.0 | Ocak/2024 | Omar Duran | *Bulut Hizmetlerinin Kullanımı* bölümü eklendi. |
| 4. | Ocak/2025 | Omar Duran | İnceleme tamamlandı. Herhangi bir değişiklik tespit edilmedi. Belge sürümünde değişiklik yok<br>Rusça çeviri kaldırıldı. |
| 5.0 | Ocak/2026 | Gerardo Vasquez | Giriş ve Amaç bölümü, Hedef bölümü ile değiştirildi<br>Amaç bölümünün içeriği güncellendi |

Bu belge, aşağıda açıklanan genel belge yönetim sürecini takip etmektedir:

NPO-GBL-SEC-10 Belge Yönetimi Politikası

**Onaylayan**

| Sürüm | Tarih | Onaylayan Kişinin Adı |
|---|---|---|
| 1.0 | Temmuz/2022 | Edwin Macias |
| 2.0 | Ağustos/2022 | Alejandro Valdes Flores |
| 3 | Mart/2023 | Alejandro Valdes Flores |
| 4.0 | Ocak/2024 | Edwin Macias |
| 4.0 | Ocak/2025 | Edwin Macias |
| 5 | Ocak/2026 | Edwin Macias |

**Bu belge bir çeviri aracı kullanılarak oluşturulmuştur.**