Information Security Requirements for Suppliers

January 2024

Introduction and Purpose

These guidelines set forth the information security requirements (hereinafter "Security Guidelines") to be complied by all Suppliers of customer (hereinafter "Nemak").

The purpose of these Security Guidelines is to protect any Information. The 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

Objective

Inform the Supplier about all the Security Guidelines that it must comply with in order to protect the Information disclosed by Nemak.

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:*** Communicate the appropriate regulations and measures of Nemak to third parties ***Supplier:*** Ensure 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. • 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. • Always comply with these Security Guidelines, even if the scope of the services has been modified by Nemak and Supplier. • 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. • 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. • 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. • 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. • Supplier shall ensure the confidentiality of the Information to which it has access to by executing one or several non-disclosure agreements. • 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. • Supplier shall take the necessary measures to protect its own facilities and IT equipment and infrastructure. • 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. • 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. • Supplier agrees to have a policy for passwords in its own infrastructure systems, with the following criteria: ○ Minimum length of 10 characters, with at least one character from each of the 3-character groups (lowercase, uppercase, numbers). ○ 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. • Upon termination of services or contract, Supplier shall disable or eliminate employee or third-party accounts to use Supplier's IT Infrastructure. • 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. • Supplier shall be responsible for any activity carried out with the accounts and passwords provided by Nemak to Supplier personnel. • Nemak will terminate Supplier's access to the Information when: ○ The purpose has been fulfilled. ○ There is a breach by Supplier of these Security Guidelines. ○ Any suspicious activity is detected. ○ When Nemak deems it convenient. • 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: ○ The employee or subcontracted third party is terminated or is no longer having a contractual relation with the Supplier. ○ The employee or subcontracted third party is no longer providing services to Nemak. 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. • Processing or storing information in a new geographical or legal jurisdiction. • 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. • Supplier must provide its employees with basic security training at least once a year, ensuring they are aware of: ○ Phishing risks ○ Keeping safe their password ○ Use of strong passwords ○ Social engineering ○ Social media
Cybersecurity Risks and Incident Management	• Supplier shall identify cybersecurity risks and take appropriate action towards preventing any security incidents. • 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. • 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: ○ Audit Supplier's performance and compliance with these Security Guidelines. ○ 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. • Supplier shall be liable to Nemak with respect to any breach of its responsibilities stated in these Security Guidelines. • 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. • Supplier agrees to indemnify, defend and hold Nemak harmless in the event of any claim arising from any breach of these Security Guidelines. • 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: 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

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

Requisitos de seguridad de la información para proveedores

Enero de 2024

Introducción y finalidad

Estas directrices establecen los requisitos de seguridad de la información (en adelante, "Directrices de Seguridad") que deben cumplir todos los Proveedores del cliente (en adelante, "Nemak").

El propósito de estas Directrices de Seguridad es proteger cualquier Información. Las Directrices de Seguridad forman parte integrante de cualquier acuerdo suscrito entre Nemak y el Proveedor, y el Proveedor deberá cumplirlas para proteger la confidencialidad e integridad de la Información. Estos requisitos pueden ser complementados por medio de otros requisitos de seguridad, cualquier acuerdo de nivel de servicio o cualquier otro documento acordado entre Nemak y el Proveedor.

Alcance

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

Excepciones

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

Objetivo

Informar al Proveedor sobre todas las Pautas de Seguridad que debe cumplir para proteger la Información divulgada por Nemak.

Definiciones

Nemak
Nemak, S.A.B. de C.V. y sus filiales.

Acuerdo
Cualquier acuerdo, orden de compra, carta de nominación u otro documento que establezca los términos y condiciones bajo los cuales los productos y/o servicios deben ser suministrados y/o prestados 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 de propiedad en poder de, y relacionada de alguna manera con, Nemak o sus negocios, clientes, proveedores o cualquier tercero.

Auditoría
Revisión periódica de la actuación 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
Sistemas, aplicaciones y/o elementos de red y bases de datos de Nemak.

Recursos materiales
Hardware o equipos físicos utilizados exclusivamente para la prestación de los servicios o el suministro de los productos (por ejemplo, ordenadores, impresoras, servidores, monitores, dispositivos móviles, soportes de almacenamiento extraíbles, etc.).

Recursos lógicos
Programas informáticos, sistemas o aplicaciones a los que se concede acceso únicamente a efectos de la prestación de los servicios o el suministro de los productos.

	SLA Acuerdo de nivel de servicio
Funciones y responsabilidades	***Nemak:*** Comunicar a terceros las normas y medidas adecuadas de Nemak ***Proveedor:*** Garantizar 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, incluyendo las Plataformas y 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 acceder a la Información, Plataforma y/o Servicios de la Infraestructura de Nemak. • El Proveedor cumplirá, y hará que los subcontratistas cumplan, las Directrices de Seguridad establecidas en el presente documento, y mantendrá pruebas que demuestren dicho cumplimiento. • Cumpla siempre con estas Directrices de Seguridad, incluso si el alcance de los servicios ha sido modificado por Nemak y el Proveedor. • Firme el Código Global de Negocio de Nemak para Proveedores, entendiéndose que sólo serán de aplicación al Proveedor aquellas Directrices de Seguridad que guarden relación con los servicios que se vayan a prestar.
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. • El Proveedor establecerá políticas, procedimientos y controles para evitar cualquier divulgación no autorizada de la Información por parte de empleados o personal subcontratado que tenga acceso a la Información. • El acceso a la Información y a la Plataforma de Infraestructuras y Servicios se concederá únicamente a aquellos empleados y/o personal subcontratado por el Proveedor en función de la necesidad de conocimiento y únicamente con respecto a la prestación de los servicios o suministro de productos. • El Proveedor declara y garantiza que los datos personales o la información confidencial sólo podrán ser utilizados con fines comerciales y en estricta consonancia con cualquier Acuerdo entre las partes, así como con cualquier política de Nemak y la legislación aplicable. • El Proveedor garantizará la confidencialidad de la Información a la que tenga acceso mediante la firma de uno o varios acuerdos de confidencialidad. • El proveedor tomará medidas proactivas para salvaguardar correctamente los datos personales o la información confidencial que se le revele con el fin de suministrar productos y/o servicios.
Seguridad física	• El proveedor se asegurará de que sólo el personal autorizado tenga acceso a los datos personales y a la información confidencial cuando sea necesario. • El Proveedor tomará las medidas necesarias para proteger sus propias instalaciones y equipos e infraestructuras informáticas.

	• El personal del proveedor y/o subcontratado deberá cumplir siempre con las políticas y procedimientos de Seguridad Física de Nemak.
Personal del proveedor	• El personal del Proveedor evitará cualquier conflicto de intereses según lo establecido en el Código Global de Negocios 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. • El Proveedor informará por escrito a su personal sobre el contenido de este documento. En caso de que así 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 garantizará la estricta adhesión y cumplimiento del mismo por parte de su personal o de cualquier personal subcontratado.
Política de uso aceptable de la infraestructura informática	• 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 deberán aceptar los requisitos de Seguridad de la Información. La prueba de la aceptación de dichos términos y condiciones deberá estar disponible si así lo requiere cualquier auditoría o para cualquier otro fin.
	• El proveedor se compromete a tener una política de contraseñas en sus propios sistemas de infraestructura, con los siguientes criterios:
	  ○ Longitud mínima de 10 caracteres, con al menos un carácter de cada uno de los grupos de 3 caracteres (minúsculas, mayúsculas, números).
	  ○ Los sistemas deben configurarse para exigir un cambio de contraseña al menos una vez cada 12 meses, o inmediatamente si hay el menor indicio de que la contraseña se ha visto comprometida de algún modo, o si hay dudas de que un tercero pueda conocerla.
	• A la finalización de los servicios o del contrato, el Proveedor deberá desactivar o eliminar las cuentas de empleados o terceros para utilizar la Infraestructura de TI del Proveedor.
	• En caso de que Nemak proporcione cuentas y contraseñas para conectarse a los sistemas de Nemak, éstas no deberán ser reveladas y/o compartidas con ningún tercero o personal del Proveedor que no forme parte de la prestación de los servicios o suministro de productos. En el caso de cuentas individualizadas otorgadas por Nemak, las mismas no deberán ser divulgadas y/o compartidas entre el personal aunque forme parte de la prestación de los servicios o suministro de productos.
	• El Proveedor será responsable de cualquier actividad realizada con las cuentas y contraseñas facilitadas por Nemak al personal del Proveedor.
	• Nemak dará por terminado el acceso del Proveedor a la Información cuando:
	  ○ El propósito se ha cumplido.
	  ○ El proveedor incumple las presentes directrices de seguridad.
	  ○ Se detecta cualquier actividad sospechosa.

- Cuando Nemak lo estime conveniente.

- 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, el Proveedor deberá notificar inmediatamente a Nemak si se da alguna de las siguientes circunstancias:
  - El empleado o tercero subcontratado es despedido o deja de tener relación contractual con el Proveedor.
  - El empleado o tercero subcontratado deja de prestar servicios a Nemak.

  Las notificaciones deben enviarse al responsable de enlace con proveedores de Nemak y a Seguridad de la Información de Nemak: isec.suppliers@nemak.com

Gestión de infraestructuras informáticas

Acceso a la red

- La red del proveedor estará protegida por cortafuegos y sólo podrá acceder a ella el personal del proveedor.
- El personal del proveedor utilizará un usuario de directorio activo para conectarse a la red.

Borrado seguro

- A la finalización de la relación comercial con Nemak o cuando Nemak lo solicite, lo que ocurra primero, el Proveedor aplicará el borrado seguro de la información para garantizar la correcta eliminación (o devolución, en su caso) de la Información.

Protección antimalware

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

Gestión de vulnerabilidades

- El Proveedor escaneará en busca de vulnerabilidades dentro de la Infraestructura de TI para detectar, notificar y remediar las vulnerabilidades encontradas en la prestación de los servicios o suministro de productos, así como en los equipos del Proveedor utilizados para la prestación de los servicios o suministro de productos.
- El proveedor aplicará un plan de corrección en caso de que se detecten vulnerabilidades.

Parcheado de sistemas

- El proveedor garantizará que los servidores, los PC de los usuarios y los dispositivos móviles se parcheen en un plazo máximo de 60 días tras la publicación del parche.

Eliminar el acceso VPN

- El Proveedor acepta utilizar la VPN para conectarse a sus instalaciones únicamente con autenticación de Active Directory y ninguna otra opción de conexión. Si es posible, el Proveedor utilizará la autenticación multifactor con VPN.
- El acceso a la VPN no se compartirá entre particulares.

Uso de servicios en nube	En caso de 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: • Proporcionar apoyo específico en caso de incidente de seguridad de la información en el entorno de servicios en nube. • Apoyar a la organización en la recopilación de pruebas digitales, teniendo en cuenta las leyes y normativas sobre pruebas digitales de las distintas jurisdicciones. • Proporcionar las copias de seguridad necesarias de los datos y la información de configuración y gestionar de forma segura las copias de seguridad, según proceda. • 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 a la finalización del mismo. El proveedor de servicios en nube debe notificarlo siempre: • 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 nube. • Tratamiento o almacenamiento de información en una nueva jurisdicción geográfica o jurídica. • Uso de proveedores de servicios en la nube homólogos u otros subcontratistas (incluido el cambio de los existentes o el uso de nuevas partes).
Concienciación sobre la seguridad de la información	• El proveedor implementará programas de concienciación y aprendizaje (entre 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. • El proveedor debe proporcionar a sus empleados formación básica sobre seguridad al menos una vez al año, asegurándose de que son conscientes de: ○ Riesgos de phishing ○ Mantener a salvo su contraseña ○ Uso de contraseñas seguras ○ Ingeniería social ○ 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. • En caso de que el Proveedor se vea involucrado en un Incidente de Seguridad que afecte a Nemak, entonces el Proveedor, en coordinación con el CSIRT, trabajará conjuntamente para volver a la normalidad de las operaciones. • El Proveedor notificará inmediatamente a Nemak cualquier incidente real o potencial de ciberseguridad y violación de datos.
Continuidad de las actividades	• El proveedor desarrollará planes de continuidad de negocio para los sistemas críticos. Estos planes incluirán, entre otros, procedimientos de recuperación en caso de catástrofe que se probarán al menos una vez al año.
Auditoría	• Nemak tendrá derecho a: ○ Auditar la actuación del Proveedor y el cumplimiento de estas Directrices de Seguridad. ○ Solicitar acceso a informes/certificados de terceros que validen el cumplimiento de los controles vinculados a la prestación de los servicios o suministro de productos.

Conformidad

- El Proveedor hará buen uso de los Derechos de Propiedad Intelectual y Derechos de Autor de Nemak y de terceros.
- El Proveedor será responsable ante Nemak con respecto a cualquier incumplimiento de sus responsabilidades establecidas en estas Directrices de Seguridad.
- El incumplimiento por parte del Proveedor o de cualquiera de sus subcontratados de las presentes Directrices de Seguridad podrá dar lugar a las sanciones especificadas en el Contrato y en la legislación aplicable.
- El proveedor se compromete a indemnizar, defender y mantener indemne a Nemak en caso de cualquier reclamación derivada de cualquier incumplimiento de estas Directrices de Seguridad.
- Estas Directrices de Seguridad podrán ser actualizadas periódicamente. El Proveedor deberá cumplir estas Directrices de Seguridad mientras mantenga una relación comercial con Nemak.

Información de contacto

Si tiene preguntas o comentarios con respecto a esta directriz, puede ponerse en contacto con Seguridad de la Información de Nemak con su consulta en isec.suppliers@nemak.com.

Revisiones

Versión	Fecha	Solicitante	Descripción de los cambios
1.0	Julio/2022	Ricardo Serrano	Creación de una directriz
2.0	Agosto/2022	Edwin Macías	El formato del documento ha cambiado a directriz
3.0	Marzo/2023	Edwin Macías	Sección *Control de Acceso Lógico* modificada: Se redefinió el texto relativo a 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*

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 de la persona autorizada
1.0	Julio/2022	Edwin Macías
2.0	Agosto/2022	Alejandro Valdés Flores
3.0	Marzo/2023	Alejandro Valdés Flores
4.0	Enero/2024	Edwin Macías

Este documento se ha creado utilizando una herramienta de traducción

Anforderungen an die Informationssicherheit für Lieferanten

Januar 2024

Einführung und Zweck

Diese Richtlinien legen die Anforderungen an die Informationssicherheit (im Folgenden "Sicherheitsrichtlinien") fest, die von allen Lieferanten des Kunden (im Folgenden "Nemak") einzuhalten sind.

Der Zweck dieser Sicherheitsrichtlinien ist der Schutz von Informationen. Die Sicherheitsrichtlinien sind integraler Bestandteil eines jeden zwischen Nemak und dem Lieferanten geschlossenen Vertrages, und der Lieferant muss sie einhalten, um die Vertraulichkeit und Integrität der Informationen zu schützen. Diese Anforderungen können durch andere Sicherheitsanforderungen, ein Service Level Agreement oder ein anderes zwischen Nemak und dem Lieferanten vereinbartes Dokument ergänzt werden.

Umfang

Dieses Dokument gilt für alle Lieferanten, die Zugang zu Informationen jeglicher Art haben oder haben könnten, die Nemak gehören 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 mitgeteilt werden, damit eine entsprechende Bewertung vorgenommen werden kann: isec.suppliers@nemak.com

Zielsetzung

den Lieferanten über alle Sicherheitsrichtlinien zu informieren, die er einhalten muss, um die von Nemak weitergegebenen Informationen zu schützen.

Definitionen

Nemak
Nemak, S.A.B. de C.V. und ihre Tochtergesellschaften.

Vereinbarung
Jeder Vertrag, jede Bestellung, jeder Nominierungsbrief oder jedes andere Dokument, das die Bedingungen festlegt, unter denen die Produkte und/oder Dienstleistungen an Nemak geliefert und/oder erbracht werden sollen.

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

Informationen
Alle vertraulichen und urheberrechtlich geschützten Informationen, die sich im Besitz von Nemak oder seinen Unternehmen, Kunden, Lieferanten oder Dritten befinden und sich in irgendeiner Weise auf diese beziehen.

Prüfung
Regelmäßige Überprüfung der Leistung des Lieferanten und der Einhaltung der Vereinbarung.

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

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

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

Logische Ressourcen

	Software, Systeme oder Anwendungen, zu denen der Zugang ausschließlich für die Erbringung der Dienstleistungen oder die Lieferung der Produkte gewährt wird. ***SLA*** Service Level Agreement
Rollen und Zuständigkeiten	***Nemak:*** die entsprechenden Vorschriften und Maßnahmen von Nemak an Dritte weitergeben ***Lieferant:*** Sicherstellung der Einhaltung der Anforderungen an die Informationssicherheit
Allgemeine Anforderungen	• Der Lieferant ergreift alle erforderlichen Maßnahmen zum Schutz der Informationen, zu denen er Zugang hat, einschließlich der Plattformen und Dienste der Nemak-Infrastruktur, unabhängig davon, ob diese aus der Erbringung von Dienstleistungen oder der Lieferung von Produkten oder aus einem anderen Grund stammen, aus dem der Lieferant Zugang zu den Informationen, Plattformen und/oder Infrastrukturdiensten von Nemak benötigt. • Der Lieferant muss die hierin festgelegten Sicherheitsrichtlinien einhalten und alle Unterauftragnehmer dazu veranlassen, diese einzuhalten, und muss Nachweise aufbewahren, die eine solche Einhaltung belegen. • Halten Sie diese Sicherheitsrichtlinien immer ein, auch wenn der Umfang der Dienstleistungen von Nemak und dem Lieferanten geändert wurde. • Unterschreiben Sie den Globalen Geschäftskodex für Lieferanten von Nemak, wobei nur die Sicherheitsrichtlinien, die sich auf die zu erbringenden Dienstleistungen beziehen, für den Lieferanten gültig sind.
Vertraulichkeit	• Der Lieferant erkennt an, dass die von Nemak weitergegebenen Informationen, zu denen der Lieferant, seine Mitarbeiter oder das von ihm beauftragte Personal Zugang haben und/oder haben werden, Eigentum von Nemak, seinen Kunden, Lieferanten und/oder Dritten sind und durch Vertraulichkeitsverpflichtungen geschützt sind. • Der Lieferant muss Richtlinien, Verfahren und Kontrollen einführen, um eine unbefugte Offenlegung der Informationen durch Angestellte oder Mitarbeiter von Unterauftragnehmern, die Zugang zu den Informationen haben, zu verhindern. • Der Zugang zu den Informationen, zur Infrastrukturplattform und zu den Diensten wird nur denjenigen Mitarbeitern und/oder dem Personal gewährt, die vom Lieferanten auf einer Need-to-know-Basis und ausschließlich im Hinblick auf die Erbringung der Dienstleistungen oder die Lieferung von Produkten unter Vertrag genommen werden. • Der Lieferant sichert zu und gewährleistet, dass personenbezogene Daten oder vertrauliche Informationen nur für geschäftliche Zwecke und in strikter Übereinstimmung mit den zwischen den Parteien geschlossenen Verträgen sowie mit den Richtlinien von Nemak und dem geltenden Recht verwendet werden dürfen. • Der Lieferant gewährleistet die Vertraulichkeit der Informationen, zu denen er Zugang hat, durch den Abschluss einer oder mehrerer Geheimhaltungsvereinbarungen. • Der Lieferant ergreift proaktiv Maßnahmen zum korrekten Schutz personenbezogener Daten oder vertraulicher Informationen, die ihm zum Zwecke der Lieferung von Produkten und/oder Dienstleistungen mitgeteilt werden.
Physische Sicherheit	• Der Lieferant stellt sicher, dass personenbezogene Daten und vertrauliche Informationen nur von befugtem Personal nach dem Grundsatz "Kenntnis nur, wenn nötig" eingesehen werden können.

	• Der Lieferant ergreift die erforderlichen Maßnahmen zum Schutz seiner eigenen Einrichtungen, IT-Ausrüstung und Infrastruktur. • Der Lieferant und/oder das von ihm beauftragte Personal müssen stets die Richtlinien und Verfahren für die physische Sicherheit von Nemak einhalten.
Personal des Lieferanten	• Das Personal des Lieferanten muss jegliche Interessenkonflikte vermeiden, wie sie im Globalen Geschäftskodex für Lieferanten von Nemak festgelegt sind. • Der Lieferant ist dafür verantwortlich, dass sein Personal für die Erbringung der Dienstleistungen kompetent und/oder zertifiziert ist und dass es dieses Niveau während der Laufzeit des Vertrags beibehält. Die Kompetenz und/oder Zertifizierung des Personals muss zur Zufriedenheit von Nemak nachgewiesen werden können. • Der Lieferant muss sein Personal schriftlich über den Inhalt dieses Dokuments informieren. Auf Wunsch kann Nemak den Lieferanten auffordern, schriftlich zu bestätigen, dass er sein Personal über den Inhalt dieses Dokuments informiert hat, und der Lieferant muss die strikte Einhaltung und Befolgung dieses Dokuments durch sein Personal oder das Personal von Unterauftragnehmern sicherstellen.
Richtlinie zur akzeptablen Nutzung der IT-Infrastruktur	• Der Lieferant wird die von Nemak zur Verfügung gestellten physischen und logischen Ressourcen immer gut nutzen.

Logische Zugangskontrolle	• Die Mitarbeiter und/oder das Personal, das der Lieferant als Unterauftragnehmer einsetzt, müssen die Informationssicherheitsanforderungen akzeptieren. Ein Nachweis über die Zustimmung zu diesen Bedingungen muss verfügbar sein, falls dies für ein Audit oder für andere Zwecke erforderlich ist.
	• Der Lieferant erklärt sich bereit, für seine eigenen Infrastruktursysteme eine Kennwortpolitik mit den folgenden Kriterien zu verfolgen:
	  ○ Mindestlänge von 10 Zeichen, davon mindestens ein Zeichen aus jeder der 3 Zeichengruppen (Kleinbuchstaben, Großbuchstaben, Zahlen).
	  ○ Die Systeme sollten so konfiguriert werden, dass das Passwort mindestens alle 12 Monate geändert werden muss, oder sofort, wenn es den geringsten Hinweis darauf gibt, dass das Passwort in irgendeiner Weise kompromittiert wurde, oder wenn der Verdacht besteht, dass eine dritte Partei es kennen könnte.
	• Bei Beendigung der Dienstleistungen oder des Vertrags muss der Lieferant die Konten von Mitarbeitern oder Dritten zur Nutzung der IT-Infrastruktur des Lieferanten deaktivieren oder löschen.
	• Wenn Nemak Konten und Passwörter für den Zugang zu den Systemen von Nemak zur Verfügung stellt, dürfen diese nicht an Dritte oder Mitarbeiter des Lieferanten, die nicht an der Erbringung der Dienstleistungen oder der Lieferung von Produkten beteiligt sind, weitergegeben und/oder mit ihnen geteilt werden. Für von Nemak gewährte individuelle Konten gilt, dass sie nicht an Mitarbeiter weitergegeben und/oder mit ihnen geteilt werden dürfen, auch wenn diese an der Erbringung der Dienstleistungen oder der Lieferung von Produkten beteiligt sind.
	• Der Lieferant ist für alle Aktivitäten verantwortlich, die mit den Konten und Passwörtern durchgeführt werden, die Nemak dem Personal des Lieferanten zur Verfügung stellt.
	• Nemak wird den Zugang des Lieferanten zu den Informationen beenden, wenn:

- Der Zweck ist erfüllt.
- Es liegt ein Verstoß des Lieferanten gegen diese Sicherheitsrichtlinien vor.
- Jede verdächtige Aktivität wird erkannt.
- Wenn Nemak es für richtig hält.

- Falls Nemak dem Lieferanten oder von ihm 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 Arbeitnehmer oder der beauftragte Dritte wird entlassen oder steht nicht mehr in einem Vertragsverhältnis mit dem Lieferanten.
  - Der Mitarbeiter oder der beauftragte Dritte erbringt keine Dienstleistungen mehr für Nemak.

  Die Meldungen müssen an den Verbindungsmanager für Lieferanten von Nemak und an die Informationssicherheit von Nemak gesendet werden: isec.suppliers@nemak.com

Verwaltung der IT-Infrastruktur

Netzzugang

- Das Netz des Lieferanten muss durch Firewalls geschützt sein und darf nur vom Personal des Lieferanten betreten werden.
- Das Personal des Lieferanten muss einen Active-Directory-Benutzer verwenden, um sich mit dem Netz zu verbinden.

Sicheres Löschen

- Bei Beendigung der Geschäftsbeziehung mit Nemak oder auf Verlangen von Nemak, je nachdem, was zuerst eintritt, wendet der Lieferant die sichere Datenlöschung an, um die ordnungsgemäße Löschung (oder Rückgabe, falls zutreffend) der Informationen zu gewährleisten.

Anti-Malware-Schutz

- Der Auftragnehmer wird die Produkte und Geräte, die für die Erbringung der Dienstleistungen oder die Lieferung der Produkte verwendet werden, mit den neuesten Anti-Malware-Versionen und den vom Hersteller bereitgestellten Updates pflegen. Die Firewall in der Computerausrüstung muss aktiviert sein, um jegliche Malware-Versuche zu blockieren.

Schwachstellen-Management

- Der Auftragnehmer sucht nach Schwachstellen in der IT-Infrastruktur, um die bei der Erbringung der Dienstleistungen oder der Lieferung von Produkten gefundenen Schwachstellen zu erkennen, zu melden und zu beheben, ebenso wie die bei der Erbringung der Dienstleistungen oder der Lieferung von Produkten verwendeten Geräte des Auftragnehmers.
- Der Lieferant muss im Falle von Schwachstellen einen Plan zur Behebung des Problems erstellen.

System-Patching

- Der Lieferant stellt sicher, dass Server, Benutzer-PCs und mobile Geräte innerhalb von höchstens 60 Tagen nach der Veröffentlichung des Patches gepatcht werden.

	VPN-Zugang entfernen • Der Lieferant erklärt sich damit einverstanden, VPN für die Verbindung zu seinen Einrichtungen nur mit Active Directory-Authentifizierung und keinen anderen Verbindungsoptionen zu verwenden. Wenn möglich, muss der Lieferant Multifaktor-Authentifizierung mit VPN verwenden. • Der VPN-Zugang darf nicht von mehreren Personen gemeinsam genutzt werden.
Nutzung von Cloud-Diensten	Im Falle von Anbietern von Cloud-Diensten verpflichtet sich der Lieferant, die folgenden Bestimmungen zum Schutz der Daten von Nemak und zur Verfügbarkeit der Dienste aufzunehmen: • Bereitstellung engagierter Unterstützung im Falle eines Informationssicherheitsvorfalls in der Cloud-Service-Umgebung. • Unterstützung der Organisation bei der Sammlung digitaler Beweise unter Berücksichtigung der Gesetze und Vorschriften für digitale Beweise in den verschiedenen Gerichtsbarkeiten. • Bereitstellung der erforderlichen Sicherungskopien von Daten und Konfigurationsinformationen und ggf. sichere Verwaltung der Sicherungskopien. • Bereitstellung und Rückgabe von Informationen wie Konfigurationsdateien, Quellcode, Protokolle und Daten, die Eigentum der Organisation sind, wenn sie während der Bereitstellung des Dienstes oder bei Beendigung des Dienstes angefordert werden. Der Anbieter des Cloud-Dienstes ist immer meldepflichtig: • 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. • Verarbeitung oder Speicherung von Informationen in einer neuen geografischen oder rechtlichen Zuständigkeit. • Nutzung von Peer-Cloud-Dienstleistern oder anderen Unterauftragnehmern (einschließlich des Wechsels bestehender oder des Einsatzes neuer Parteien).
Sensibilisierung für Informationssicherheit	• Der Lieferant muss Sensibilisierungs- und Lernprogramme (für alle seine Mitarbeiter) in Bezug auf die Informationssicherheit einführen, Präventivmaßnahmen ergreifen und Richtlinien, Verfahren und Kontrollen für die Klassifizierung und Verwaltung von Informationen einführen. • Der Lieferant muss seinen Mitarbeitern mindestens einmal jährlich eine grundlegende Sicherheitsschulung zukommen lassen, die sicherstellt, dass sie über die folgenden Punkte informiert sind: ○ Phishing-Risiken ○ Ihr Passwort sicher aufbewahren ○ Verwendung von sicheren Passwörtern ○ Social Engineering ○ Soziale Medien
Cybersicherheitsrisiken und Management von Vorfällen	• Der Lieferant muss Cybersicherheitsrisiken erkennen und geeignete Maßnahmen zur Verhinderung von Sicherheitsvorfällen ergreifen. • Falls der Lieferant in einen Sicherheitsvorfall verwickelt ist, der Nemak betrifft, wird der Lieferant in Abstimmung mit dem CSIRT zusammenarbeiten, um zum normalen Betrieb zurückzukehren.

	• Der Lieferant ist verpflichtet, Nemak unverzüglich über jeden tatsächlichen oder potenziellen Vorfall im Bereich der Cybersicherheit und jede Datenverletzung zu informieren.
Geschäftskontinuität	• Der Lieferant muss Pläne zur Aufrechterhaltung des Geschäftsbetriebs für kritische Systeme entwickeln. Diese Pläne müssen unter anderem Verfahren zur Wiederherstellung im Katastrophenfall umfassen, die mindestens einmal jährlich getestet werden.
Prüfung	• Nemak hat das Recht dazu: ○ Prüfung der Leistung des Lieferanten und der Einhaltung dieser Sicherheitsrichtlinien. ○ Zugang zu Berichten/Bescheinigungen Dritter zu verlangen, die die Einhaltung der Kontrollen im Zusammenhang mit der Erbringung von Dienstleistungen oder der Lieferung von Produkten bestätigen.
Einhaltung der Vorschriften	• Der Lieferant wird alle geistigen Eigentumsrechte und Urheberrechte von Nemak und Dritten in angemessener Weise nutzen. • Der Lieferant haftet Nemak gegenüber für jeden Verstoß gegen seine in diesen Sicherheitsrichtlinien genannten Pflichten. • Die Nichteinhaltung dieser Sicherheitsrichtlinien durch den Lieferanten oder eines seiner Unterauftragnehmer kann Sanktionen nach Maßgabe des Abkommens und der geltenden Gesetze nach sich ziehen. • Der Lieferant erklärt sich damit einverstanden, Nemak zu entschädigen, zu verteidigen und schadlos zu halten im Falle von Ansprüchen, die sich aus einem Verstoß gegen diese Sicherheitsrichtlinien ergeben. • Diese Sicherheitsrichtlinien können von Zeit zu Zeit aktualisiert werden. Der Lieferant muss diese Sicherheitsrichtlinien einhalten, solange er eine Geschäftsbeziehung mit Nemak unterhält.
Kontaktinformationen	Wenn Sie Fragen oder Anmerkungen zu dieser Richtlinie haben, können Sie sich mit Ihrer Anfrage an die Informationssicherheit von Nemak wenden: isec.suppliers@nemak.com.

Überarbeitungen

Version	Datum	Antragsteller	Beschreibung der Änderungen
1.0	Juli/2022	Ricardo Serrano	Erstellung eines Leitfadens
2.0	August/2022	Edwin Macias	Dokumentformat in Leitfaden geändert
3.0	März/2023	Edwin Macias	Abschnitt *Logische Zugriffskontrolle* geändert: Der Text, der sich auf die Beendigung der Dienstleistungen des Lieferanten oder unterbeauftragter Dritter bezieht, wurde neu definiert.
4.0	Januar/2024	Omar Duran	Abschnitt über *die Nutzung von Cloud-Diensten* hinzugefügt

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

NPO-GBL-SEC-10 Richtlinie zur Dokumentenverwaltung

Genehmigt durch

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

Dieses Dokument wurde mit einem Übersetzungsprogramm erstellt

Requisitos de segurança da informação para fornecedores

Janeiro de 2024

Introdução e objetivo

Estas diretrizes estabelecem os requisitos de segurança da informação (doravante denominados "Diretrizes de segurança") a serem cumpridos por todos os fornecedores do cliente (doravante denominados "Nemak").

O objetivo destas Diretrizes de segurança é proteger qualquer Informação. As Diretrizes de Segurança são parte integrante de qualquer contrato firmado entre a Nemak e o Fornecedor, e o Fornecedor deverá 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.

Escopo

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

Exceções

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

Objetivo

Informar o Fornecedor sobre todas as Diretrizes de Segurança que ele deve cumprir para proteger as Informações divulgadas pela Nemak.

Definições

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

Acordo
Qualquer contrato, 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 seus negócios, clientes, fornecedores ou terceiros, e relacionadas de alguma forma a eles.

Auditoria
Revisão periódica do desempenho e da conformidade do Fornecedor com qualquer Contrato.

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 usado exclusivamente para fins de prestação dos serviços ou fornecimento dos produtos (por exemplo, computadores, impressoras, servidores, monitores, dispositivos móveis, mídia de armazenamento removível, 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 Contrato de nível de serviço
Funções e responsabilidades	***Nemak:*** Comunicar os regulamentos e medidas apropriados da Nemak a terceiros ***Fornecedor:*** Garantir a conformidade com os requisitos de segurança da informação
Requisitos gerais	• O Fornecedor deverá tomar todas as medidas necessárias para proteger quaisquer Informações às quais tenha acesso, incluindo as Plataformas e Serviços da Infraestrutura da Nemak, sejam elas derivadas da prestação de serviços ou do fornecimento de produtos ou por qualquer outro motivo pelo qual o Fornecedor necessite acessar as Informações, a Plataforma e/ou os Serviços de Infraestrutura da Nemak. • O Fornecedor deverá cumprir e fazer com que todos os subcontratados cumpram as Diretrizes de Segurança aqui estabelecidas e deverá manter evidências que demonstrem essa conformidade. • Sempre cumpra estas Diretrizes de segurança, mesmo que o escopo dos serviços tenha sido modificado pela Nemak e pelo Fornecedor. • Assinar o Global Business Code for Suppliers da Nemak, entendendo-se que somente 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 de propriedade da Nemak, de seus clientes, fornecedores e/ou terceiros, e estão protegidas por compromissos de confidencialidade. • O Fornecedor deverá estabelecer políticas, procedimentos e controles para evitar qualquer divulgação não autorizada das Informações por funcionários ou pessoal subcontratado que tenha acesso às Informações. • O acesso às Informações e à Plataforma de Infraestrutura e aos Serviços deverá ser concedido somente aos funcionários e/ou pessoal subcontratado pelo Fornecedor com base na necessidade de conhecimento e somente com relação à prestação dos serviços ou fornecimento de produtos. • O Fornecedor declara e garante que os dados pessoais ou informações confidenciais somente poderão ser utilizados para fins comerciais e em estrito alinhamento com quaisquer Contratos entre as partes, bem como com quaisquer políticas da Nemak e com a legislação aplicável. • O Fornecedor deverá garantir a confidencialidade das Informações às quais tem acesso por meio da assinatura de um ou vários acordos de não divulgação. • O Fornecedor deverá tomar medidas proativas para proteger corretamente os dados pessoais ou as informações confidenciais que lhe forem divulgadas para fins de fornecimento de produtos e/ou serviços.
Segurança física	• O fornecedor deve garantir que os dados pessoais e as informações confidenciais sejam acessados apenas por pessoal autorizado, de acordo com a necessidade de conhecimento. • O Fornecedor deve tomar as medidas necessárias para proteger suas próprias instalações, equipamentos e infraestrutura de TI.

	• O pessoal do fornecedor e/ou subcontratado deve sempre cumprir as políticas e os procedimentos de segurança física da Nemak.
Pessoal do fornecedor	• O pessoal do fornecedor deve evitar quaisquer conflitos de interesse, conforme estabelecido no Código Comercial Global para Fornecedores da Nemak. • O Fornecedor será responsável pelo fato de que sua equipe é competente e/ou certificada para a prestação dos serviços e que mantém esse nível durante a vigência do Contrato. A competência e/ou certificação da equipe deve poder ser demonstrada de forma satisfatória para a Nemak. • O Fornecedor deverá informar seu pessoal por escrito sobre o conteúdo deste documento. Caso seja necessário, a Nemak poderá solicitar ao Fornecedor que confirme por escrito que informou seu pessoal sobre o conteúdo deste documento, e o Fornecedor deverá garantir a estrita adesão e cumprimento do mesmo por seu pessoal ou por 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 evidência da aceitação de tais termos e condições deverá estar disponível caso seja exigida por qualquer auditoria ou para quaisquer outros fins.
	• O fornecedor concorda em ter uma política para senhas em seus próprios sistemas de infraestrutura, com os seguintes critérios:
	  ○ Comprimento mínimo de 10 caracteres, com pelo menos um caractere de cada um dos grupos de 3 caracteres (minúsculas, maiúsculas, números).
	  ○ Os sistemas devem ser configurados para exigir a alteração da senha pelo menos uma vez a cada 12 meses, ou imediatamente, caso haja a menor indicação de que a senha tenha sido comprometida de alguma forma, ou se houver dúvida de que um terceiro possa conhecê-la.
	• Após a rescisão dos serviços ou do contrato, o Fornecedor deverá desativar ou eliminar as contas de funcionários ou de terceiros para usar a infraestrutura de TI do Fornecedor.
	• 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 do fornecimento de produtos. Para contas individualizadas concedidas pela Nemak, elas não devem ser divulgadas e/ou compartilhadas entre funcionários, mesmo que façam parte da prestação dos serviços ou do fornecimento de produtos.
	• O fornecedor será responsável por qualquer atividade realizada com as contas e senhas fornecidas pela Nemak ao pessoal do fornecedor.
	• A Nemak encerrará o acesso do Fornecedor às Informações quando:
	  ○ O propósito foi cumprido.
	  ○ O Fornecedor violou estas Diretrizes de Segurança.
	  ○ Qualquer atividade suspeita é detectada.
	  ○ Quando Nemak achar conveniente.

- Caso a Nemak forneça 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 situações a seguir:
  - O funcionário ou terceiro subcontratado for demitido ou não tiver mais uma relação contratual com o Fornecedor.
  - O funcionário ou terceiro subcontratado não está mais prestando serviços à Nemak.

  As notificações devem ser enviadas ao gerente de contato com o fornecedor da Nemak e à 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 de diretório ativo para se conectar à rede.

Apagamento seguro

- Após o término do relacionamento 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 usados para a prestação dos serviços ou fornecimento dos produtos com as versões e atualizações antimalware mais recentes fornecidas pelo fabricante. O firewall do equipamento de informática deve estar ativado para bloquear qualquer tentativa de malware.

Gerenciamento de vulnerabilidades

- O Fornecedor deverá procurar vulnerabilidades na Infraestrutura de TI para detectar, notificar e remediar as vulnerabilidades encontradas na prestação dos serviços ou no fornecimento de produtos, bem como nos equipamentos do Fornecedor usados para a prestação dos serviços ou fornecimento de produtos.
- O fornecedor deve implementar um plano de correção em caso de vulnerabilidades.

Patching de sistemas

- O fornecedor deve garantir que servidores, PCs de usuários e dispositivos móveis sejam corrigidos no prazo máximo de 60 dias após o lançamento da correção.

Remover acesso à VPN

- O Fornecedor concorda em usar a VPN para se conectar às suas instalações somente com a autenticação do Active Directory e nenhuma outra opção de conexão. Se possível, o Fornecedor deverá usar a autenticação multifator com a VPN.
- O acesso à 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 no caso de um incidente de segurança da informação no ambiente do serviço de nuvem. • Apoiar a organização na coleta de evidências digitais, levando em consideração as leis e os regulamentos para evidências digitais em diferentes jurisdições. • Fornecer o backup necessário de dados e informações de configuração e gerenciar com segurança os backups, conforme aplicável. • Fornecer e devolver informações, como arquivos de configuração, código-fonte, registros e dados de propriedade da organização, quando solicitado durante a prestação do serviço ou ao término do serviço. O provedor de serviços em nuvem sempre deve notificar: • Alterações na infraestrutura técnica (por exemplo, realocação, reconfiguração ou alterações em hardware ou software) que afetem ou alterem a oferta de serviços em nuvem. • Processamento ou armazenamento de informações em uma nova jurisdição geográfica ou legal. • Uso de provedores de serviços de nuvem de pares ou outros subcontratados (incluindo a alteração de partes existentes ou o uso de novas partes).
Conscientização sobre segurança da informação	• O Fornecedor deve implementar programas de conscientização e aprendizado (entre seus funcionários) com relação à segurança das informações, tomando medidas preventivas e implementando políticas, procedimentos e controles sobre como classificar e gerenciar informações. • O fornecedor deve fornecer aos seus funcionários treinamento básico de segurança pelo menos uma vez por ano, garantindo que eles estejam cientes: ○ Riscos de phishing ○ Manter sua senha segura ○ Uso de senhas fortes ○ Engenharia social ○ Mídia social
Riscos de segurança cibernética e gerenciamento de incidentes	• O fornecedor deve identificar os riscos de segurança cibernética e tomar as medidas adequadas para evitar incidentes de segurança. • 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. • O Fornecedor deve 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 de negócios para sistemas críticos. Esses planos devem incluir, entre outros, procedimentos de recuperação de desastres que sejam testados pelo menos uma vez por ano.
Auditoria	• A Nemak terá o direito de: ○ Auditar o desempenho e a conformidade do Fornecedor com estas Diretrizes de Segurança. ○ Solicitar acesso a relatórios/certificados de terceiros que validem a conformidade com os controles vinculados à prestação dos serviços ou ao fornecimento de produtos.

Conformidade

- O Fornecedor deverá fazer bom uso de todos os direitos de propriedade intelectual e direitos autorais da Nemak e de terceiros.
- O fornecedor será responsável perante a Nemak em relação a qualquer violação de suas responsabilidades estabelecidas nestas Diretrizes de segurança.
- O não cumprimento destas Diretrizes de Segurança pelo Fornecedor ou por qualquer de seus funcionários subcontratados poderá resultar em penalidades, conforme especificado no Contrato e nas leis aplicáveis.
- O fornecedor concorda em indenizar, defender e isentar a Nemak de responsabilidade no caso de qualquer reclamação decorrente de violação destas Diretrizes de segurança.
- Estas Diretrizes de Segurança podem ser atualizadas periodicamente. O Fornecedor deverá cumprir estas Diretrizes de Segurança enquanto mantiver um relacionamento comercial com a Nemak.

Informações de contato

Em caso de dúvidas ou comentários sobre esta diretriz, entre em contato com a Nemak's Information Security pelo e-mail isec.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	A seção *Controle de acesso lógico* foi alterada: O texto relacionado ao término dos serviços do Fornecedor ou de Terceiros Subcontratados foi redefinido.
4.0	Janeiro/2024	Omar Duran	Adicionada a seção *Uso de serviços em nuvem*

Este documento segue o processo geral de gerenciamento 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

Este documento foi criado usando uma ferramenta de tradução

Požadavky na zabezpečení informací pro dodavatele

leden 2024

Úvod a účel	Tyto pokyny stanoví požadavky na bezpečnost informací (dále jen "bezpečnostní pokyny"), které musí dodržovat všichni dodavatelé zákazníka (dále jen "Nemak"). Účelem těchto bezpečnostních pokynů je chránit veškeré informace. Bezpečnostní pokyny tvoří nedílnou součást každé smlouvy uzavřené mezi společností Nemak a Dodavatelem a Dodavatel je povinen je dodržovat, aby chránil důvěrnost a integritu Informací. Tyto požadavky mohou být doplněny prostřednictvím dalších bezpečnostních požadavků, jakékoli dohody o úrovni služeb nebo jiného dokumentu dohodnutého mezi společností Nemak a Dodavatelem.
Oblast působnosti	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 to oznámit společnosti Nemak na následující e-mailovou adresu pro jeho odpovídající vyhodnocení: isec.suppliers@nemak.com.
Cíl	informovat dodavatele o všech bezpečnostních pokynech, které musí dodržovat, aby ochránil informace zveřejněné společností Nemak.
Definice	***Nemak*** Nemak, S.A.B. de C.V. a její dceřiné společnosti. ***Dohoda*** Jakákoli smlouva, objednávka, nominační dopis nebo jiný dokument, který stanoví podmínky, za nichž mají být společnosti Nemak dodávány a/nebo poskytovány produkty a/nebo služby. ***CSIRT*** *(Cyber Security Incident Response Team)* Nemakův tým pro řešení kybernetických bezpečnostních incidentů. ***Informace*** Veškeré důvěrné a vlastnické informace, které má společnost Nemak nebo její podniky, klienti, dodavatelé nebo jakákoli třetí strana k dispozici a které se jí jakýmkoli způsobem týkají. ***Audit*** Pravidelná kontrola výkonu dodavatele a jeho souladu s jakoukoli dohodou. ***Dodavatel*** Jakákoli fyzická nebo právnická osoba, která společnosti Nemak poskytuje produkty a/nebo služby. ***Platformy a služby infrastruktury*** systémy, aplikace a/nebo síťové prvky a databáze společnosti Nemak. ***Fyzické zdroje*** Hardware nebo fyzické vybavení používané výhradně pro účely poskytování služeb nebo dodávek produktů (např. počítače, tiskárny, servery, monitory, mobilní zařízení, výměnná paměťová média atd.). ***Logické zdroje*** Software, systémy nebo aplikace, ke kterým je přístup udělen výhradně pro účely poskytování služeb nebo dodávek produktů. ***SLA*** Dohoda o úrovni služeb

Role a odpovědnosti	***Nemak:*** Sdělování příslušných předpisů a opatření společnosti Nemak třetím stranám. ***Dodavatel:*** Zajištění souladu s požadavky na bezpečnost informací
Obecné požadavky	• Dodavatel je povinen přijmout veškerá nezbytná opatření k ochraně všech informací, ke kterým má přístup, včetně platforem a služeb infrastruktury společnosti Nemak, ať už vyplývají z poskytování služeb nebo dodávek produktů nebo z jakéhokoli jiného důvodu, pro který Dodavatel potřebuje přístup k informacím, platformě a/nebo službám infrastruktury společnosti Nemak. • Dodavatel je povinen dodržovat bezpečnostní pokyny stanovené v tomto dokumentu a zajistit, aby je dodržovali i jeho subdodavatelé, a uchovávat doklady, které toto dodržování prokazují. • Vždy dodržujte tyto bezpečnostní pokyny, a to i v případě, že rozsah služeb byl společností Nemak a dodavatelem upraven. • Podepište Globální obchodní kodex společnosti Nemak pro dodavatele, přičemž se rozumí, že na dodavatele se vztahují pouze ty bezpečnostní pokyny, které se týkají poskytovaných služeb.
Důvěrnost	• Dodavatel bere na vědomí, že informace sdělené společností Nemak, ke kterým mají a/nebo budou mít přístup dodavatel, jeho zaměstnanci nebo subdodavatelé, jsou majetkem společnosti Nemak, jejích klientů, dodavatelů a/nebo třetích stran a jsou chráněny závazky mlčenlivosti. • Dodavatel zavede zásady, postupy a kontrolní mechanismy, které zabrání neoprávněnému vyzrazení informací zaměstnanci nebo subdodavateli, kteří mají k informacím přístup. • Přístup k informacím a k platformě infrastruktury a službám bude umožněn pouze těm zaměstnancům a/nebo pracovníkům, které dodavatel najal jako subdodavatele, a to na základě potřeby vědět a výhradně v souvislosti s poskytováním služeb nebo dodávkami produktů. • Dodavatel prohlašuje a zaručuje, že osobní údaje nebo důvěrné informace mohou být použity pouze pro obchodní účely a v přísném souladu se všemi dohodami mezi stranami, jakož i se všemi zásadami společnosti Nemak a platnými právními předpisy. • Dodavatel zajistí důvěrnost informací, ke kterým má přístup, uzavřením jedné nebo více dohod o mlčenlivosti. • Dodavatel přijme proaktivní opatření k řádnému zabezpečení osobních údajů nebo důvěrných informací, které mu byly sděleny za účelem dodávky výrobků a/nebo služeb.
Fyzická bezpečnost	• Dodavatel zajistí, aby k osobním údajům a důvěrným informacím měli přístup pouze oprávnění pracovníci na základě zásady "need-to-know". • Dodavatel přijme nezbytná opatření k ochraně svých vlastních zařízení a IT vybavení a infrastruktury. • Dodavatel a/nebo subdodavatelský personál musí vždy dodržovat zásady a postupy fyzické bezpečnosti společnosti Nemak.
Personál dodavatele	• Zaměstnanci dodavatele se musí vyvarovat jakéhokoli střetu zájmů, jak je uvedeno v Globálním obchodním kodexu pro dodavatele společnosti Nemak.

	• Dodavatel odpovídá za to, že jeho zaměstnanci jsou způsobilí a/nebo certifikovaní pro poskytování služeb a že si tuto úroveň udrží po celou dobu trvání Smlouvy. Způsobilost a/nebo certifikaci personálu musí být možné prokázat ke spokojenosti společnosti Nemak. • Dodavatel je povinen písemně informovat své zaměstnance o obsahu tohoto dokumentu. V případě potřeby může společnost Nemak požádat dodavatele, aby písemně potvrdil, že informoval své zaměstnance o obsahu tohoto dokumentu, a dodavatel zajistí, aby jej jeho zaměstnanci nebo zaměstnanci subdodavatelů důsledně dodržovali.
Zásady přijatelného používání infrastruktury IT	• Dodavatel musí vždy řádně využívat fyzické a logické zdroje poskytnuté společností Nemak.

Logické řízení přístupu	• Zaměstnanci a/nebo pracovníci najatí subdodavatelem musí akceptovat požadavky na bezpečnost informací. Důkaz o přijetí těchto podmínek musí být k dispozici, pokud to vyžaduje jakýkoli audit nebo pro jiné účely.
	• Dodavatel souhlasí s tím, že bude mít politiku pro hesla ve svých vlastních infrastrukturních systémech, která bude splňovat následující kritéria:
	  ○ Minimální délka je 10 znaků, přičemž každý ze tří skupin znaků (malá písmena, velká písmena, číslice) musí obsahovat alespoň jeden znak.
	  ○ Systémy by měly být nakonfigurovány tak, aby vyžadovaly změnu hesla alespoň jednou za 12 měsíců nebo okamžitě, pokud se objeví sebemenší náznak, že heslo bylo jakýmkoli způsobem prozrazeno, nebo pokud existuje pochybnost, že by ho mohla znát třetí strana.
	• Po ukončení služeb nebo smlouvy dodavatel zakáže nebo zruší účty zaměstnanců nebo třetích stran pro používání IT infrastruktury dodavatele.
	• Pokud společnost Nemak poskytne účty a hesla pro připojení k systémům společnosti Nemak, nesmějí být zpřístupněny a/nebo sdíleny s žádnou třetí stranou nebo zaměstnanci dodavatele, kteří se nepodílejí na poskytování služeb nebo dodávkách produktů. V případě individuálních účtů poskytnutých společností Nemak nesmí být tyto účty zveřejněny a/nebo sdíleny mezi zaměstnanci, i když jsou součástí poskytování služeb nebo dodávek produktů.
	• Dodavatel odpovídá za veškeré činnosti prováděné pomocí účtů a hesel, které společnost Nemak poskytla pracovníkům dodavatele.
	• Společnost Nemak ukončí přístup Dodavatele k Informacím, pokud:
	  ○ Účel byl splněn.
	  ○ Dodavatel porušil tyto bezpečnostní pokyny.
	  ○ Zjistí se jakákoli podezřelá aktivita.
	  ○ Když to Nemak uzná za vhodné.
	• V případě, že společnost Nemak poskytuje uživatelské účty (např. účty Active Directory, přístup k VPN, e-mail atd.) dodavateli nebo třetím stranám, které si dodavatel najal jako subdodavatele, musí dodavatel neprodleně informovat společnost Nemak, pokud nastane některá z následujících situací:
	  ○ Zaměstnanec nebo subdodavatelská třetí strana je propuštěn nebo již není ve smluvním vztahu s dodavatelem.

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

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

Správa infrastruktury IT

Přístup k síti

- Síť dodavatele musí být chráněna firewally a přístup k ní mohou mít pouze zaměstnanci dodavatele.
- Pracovníci dodavatele musí pro připojení k síti používat uživatele aktivního adresáře.

Bezpečné vymazání

- Po ukončení obchodního vztahu se společností Nemak nebo na žádost společnosti Nemak, podle toho, co nastane dříve, Dodavatel použije bezpečný výmaz informací, aby zajistil řádné vymazání (nebo případně vrácení) Informací.

Ochrana proti malwaru

- Dodavatel bude udržovat produkty a zařízení používané pro poskytování služeb nebo dodávku produktů s nejnovějšími verzemi antimalwaru a aktualizacemi poskytovanými výrobcem. Firewall v počítačovém vybavení musí být povolen tak, aby blokoval jakýkoli pokus o škodlivý software.

Správa zranitelností

- Dodavatel je povinen vyhledávat zranitelnosti v rámci IT infrastruktury, odhalovat, oznamovat a odstraňovat zranitelnosti zjištěné při poskytování služeb nebo dodávkách produktů, jakož i v zařízeních dodavatele používaných při poskytování služeb nebo dodávkách produktů.
- Dodavatel zavede plán nápravy v případě jakýchkoli zranitelností.

Záplatování systémů

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

Odebrání přístupu k síti VPN

- Dodavatel se zavazuje používat pro připojení ke svým zařízením pouze VPN s ověřením Active Directory a bez jiných možností připojení. Pokud je to možné, musí dodavatel používat vícefaktorové ověřování pomocí VPN.
- Přístup do sítě VPN nesmí být sdílen mezi jednotlivci.

Používání cloudových služeb

V případě poskytovatelů cloudových služeb se dodavatel zavazuje zahrnout následující ustanovení o ochraně dat společnosti Nemak a dostupnosti služeb:

- Poskytování specializované podpory v případě incidentu v oblasti bezpečnosti informací v prostředí cloudových služeb.
- Podporovat organizaci při shromažďování digitálních důkazů s ohledem na zákony a předpisy pro digitální důkazy v různých jurisdikcích.
- Zajišťování požadovaného zálohování dat a informací o konfiguraci a případná bezpečná správa záloh.

	• Poskytnout a vrátit informace, jako jsou konfigurační soubory, zdrojový kód, protokoly a data, které jsou ve vlastnictví organizace, pokud o to organizace požádá během poskytování služby nebo při jejím ukončení. Poskytovatel cloudových služeb musí vždy informovat: • Změny technické infrastruktury (např. přemístění, rekonfigurace nebo změny hardwaru či softwaru), které ovlivňují nebo mění nabídku cloudových služeb. • Zpracování nebo ukládání informací v nové zeměpisné nebo právní jurisdikci. • Využívání rovnocenných poskytovatelů cloudových služeb nebo jiných subdodavatelů (včetně změny stávajících nebo využití nových stran).
Informovanost o bezpečnosti informací	• Dodavatel musí zavést programy zvyšování povědomí a vzdělávání (pro všechny své zaměstnance), pokud jde o bezpečnost informací, přijímání preventivních opatření a zavádění zásad, postupů a kontrolních mechanismů pro klasifikaci a správu informací. • Dodavatel musí svým zaměstnancům alespoň jednou ročně poskytnout základní bezpečnostní školení a zajistit, aby byli seznámeni s: ○ Rizika phishingu ○ Udržování hesla v bezpečí ○ Používání silných hesel ○ Sociální inženýrství ○ Sociální média
Rizika kybernetické bezpečnosti a řízení incidentů	• Dodavatel musí identifikovat rizika kybernetické bezpečnosti a přijmout vhodná opatření k předcházení bezpečnostním incidentům. • V případě, že je dodavatel zapojen do bezpečnostního incidentu, který ovlivní společnost Nemak, bude dodavatel v koordinaci s CSIRT spolupracovat na obnovení běžného provozu. • Dodavatel je povinen neprodleně informovat společnost Nemak o jakémkoli skutečném nebo potenciálním kybernetickém bezpečnostním incidentu a narušení bezpečnosti dat.
Kontinuita podnikání	• Dodavatel vypracuje plány kontinuity provozu pro kritické systémy. Tyto plány musí mimo jiné zahrnovat postupy obnovy po havárii, které se testují alespoň jednou ročně.
Audit	• Společnost Nemak má právo: ○ auditovat výkonnost dodavatele a dodržování těchto bezpečnostních pokynů. ○ Vyžádat si přístup ke zprávám/certifikátům třetích stran, které potvrzují soulad s kontrolami souvisejícími s poskytováním služeb nebo dodávkami výrobků.
Dodržování předpisů	• Dodavatel je povinen řádně využívat veškerá práva duševního vlastnictví a autorská práva společnosti Nemak a třetích stran. • Dodavatel je odpovědný společnosti Nemak za jakékoli porušení svých povinností uvedených v těchto bezpečnostních pokynech. • Nedodržení těchto bezpečnostních pokynů ze strany dodavatele nebo jeho subdodavatelů může být důvodem k sankcím uvedeným ve smlouvě a platných zákonech. • Dodavatel se zavazuje odškodnit společnost Nemak, hájit ji a zbavit ji odpovědnosti v případě jakýchkoli nároků vyplývajících z porušení těchto bezpečnostních pokynů.

- 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

Pokud máte dotazy nebo připomínky k tomuto pokynu, můžete se obrátit na oddělení bezpečnosti informací společnosti Nemak na adrese isec.suppliers@nemak.com.

Revize

Verze	Datum	Žadatel	Popis změn
1.0	červenec/2022	Ricardo Serrano	Vytvoření pokynů
2.0	srpen/2022	Edwin Macias	Změna formátu dokumentu na pokyny
3.0	březen/2023	Edwin Macias	Sekce *Řízení logického přístupu* změněna: Text týkající se ukončení služeb dodavatele nebo subdodavatelských třetích stran byl nově definován.
4.0	leden/2024	Omar Duran	Přidána sekce *Používání cloudových služeb*

Tento dokument se řídí obecným postupem 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

Tento dokument byl vytvořen pomocí překladače.

Požiadavky na bezpečnosť informácií pre dodávateľov

január 2024

Úvod a účel

Tieto pokyny stanovujú požiadavky na bezpečnosť informácií (ďalej len "bezpečnostné pokyny"), ktoré musia dodržiavať všetci dodávatelia zákazníka (ďalej len "Nemak").

Účelom týchto bezpečnostných pokynov je chrániť akékoľvek informácie. Bezpečnostné pokyny tvoria neoddeliteľnú súčasť každej 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 prostredníctvom ďalších bezpečnostných požiadaviek, akejkoľvek dohody o úrovni služieb alebo akéhokoľvek iného dokumentu dohodnutého medzi spoločnosťou Nemak a Dodávateľom.

Rozsah pôsobnosti

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 ju oznámiť spoločnosti Nemak na nasledujúci e-mail, aby ju mohla príslušne vyhodnotiť: isec.suppliers@nemak.com

Cieľ

Informovať Dodávateľa o všetkých Bezpečnostných pokynoch, ktoré musí dodržiavať, aby ochránil Informácie zverejnené spoločnosťou Nemak.

Definície

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

Dohoda
Akákoľvek zmluva, objednávka, menovací dekrét alebo iný dokument, v ktorom sú stanovené podmienky, za ktorých sa majú spoločnosti Nemak dodávať a/alebo poskytovať výrobky a/alebo služby.

CSIRT *(Cyber Security Incident Response Team)*
Tím Nemak pre riešenie kybernetických bezpečnostných incidentov.

Informácie
Všetky dôverné a vlastnícke informácie, ktoré má spoločnosť Nemak alebo jej podniky, klienti, dodávatelia alebo akákoľvek tretia strana a ktoré sa jej akýmkoľvek spôsobom týkajú.

Audit
Pravidelná kontrola výkonu a dodržiavania akejkoľvek dohody zo strany dodávateľa.

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

Platformy a služby infraštruktúry
systémy, aplikácie a/alebo sieťové prvky a databázy spoločnosti Nemak.

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

Logické zdroje
Softvér, systémy alebo aplikácie, ku ktorým je prístup udelený výlučne na účely poskytovania služieb alebo dodávky produktov.

	SLA Dohoda o úrovni služieb
Úlohy a zodpovednosti	***Nemak:*** oznamovanie príslušných predpisov a opatrení spoločnosti Nemak tretím stranám ***Dodávateľ:*** Zabezpečenie súladu s požiadavkami na bezpečnosť informácií
Všeobecné požiadavky	• Dodávateľ je povinný prijať všetky potrebné opatrenia na ochranu všetkých informácií, ku ktorým má prístup, vrátane platforiem a služieb infraštruktúry spoločnosti Nemak, či už vyplývajú z poskytovania služieb alebo dodávok produktov, alebo z akéhokoľvek iného dôvodu, pre ktorý Dodávateľ potrebuje prístup k informáciám, platforme a/alebo službám infraštruktúry spoločnosti Nemak. • Dodávateľ je povinný dodržiavať a zabezpečiť, aby všetci subdodávatelia dodržiavali bezpečnostné usmernenia uvedené v tomto dokumente, a uchovávať dôkazy, ktoré preukazujú toto dodržiavanie. • Vždy dodržiavajte tieto bezpečnostné pokyny, a to aj v prípade, že spoločnosť Nemak a Dodávateľ upravili rozsah služieb. • Podpíšte Globálny obchodný kódex spoločnosti Nemak pre dodávateľov, pričom sa rozumie, že na dodávateľa sa vzťahujú len tie bezpečnostné pokyny, ktoré sa týkajú služieb, ktoré sa majú poskytnúť.
Dôvernosť	• Dodávateľ berie na vedomie, že Informácie zverejnené spoločnosťou Nemak, ku ktorým majú a/alebo budú mať prístup Dodávateľ, jeho zamestnanci alebo subdodávatelia, sú majetkom spoločnosti Nemak, jej klientov, dodávateľov a/alebo tretích strán a sú chránené záväzkami mlčanlivosti. • Dodávateľ zavedie zásady, postupy a kontrolné mechanizmy, aby zabránil akémukoľvek neoprávnenému zverejneniu informácií zamestnancami alebo subdodávateľmi, ktorí majú prístup k informáciám. • Prístup k informáciám a k infraštruktúrnej platforme a službám bude umožnený len tým zamestnancom a/alebo personálu, ktorých dodávateľ najal ako subdodávateľov, a to na základe potreby poznať informácie a výlučne v súvislosti s poskytovaním služieb alebo dodávkou produktov. • Dodávateľ vyhlasuje a zaručuje, že osobné údaje alebo dôverné informácie sa môžu používať len na obchodné účely a v prísnom súlade so všetkými dohodami medzi stranami, ako aj so všetkými zásadami spoločnosti Nemak a platnými právnymi predpismi. • Dodávateľ zabezpečí dôvernosť informácií, ku ktorým má prístup, uzavretím jednej alebo viacerých dohôd o mlčanlivosti. • Dodávateľ prijme proaktívne opatrenia na správne zabezpečenie osobných údajov alebo dôverných informácií, ktoré mu boli poskytnuté na účely dodávky výrobkov a/alebo služieb.
Fyzická bezpečnosť	• Dodávateľ zabezpečí, aby k osobným údajom a dôverným informáciám mali prístup len oprávnení pracovníci na základe zásady "need-to-know". • Dodávateľ prijme potrebné opatrenia na ochranu svojich vlastných zariadení a IT zariadení a infraštruktúry. • Dodávateľ a/alebo subdodávateľský personál musí vždy dodržiavať zásady a postupy fyzickej bezpečnosti spoločnosti Nemak.

Personál dodávateľa	• Zamestnanci dodávateľa sa musia vyhýbať akýmkoľvek konfliktom záujmov, ako je stanovené v Globálnom obchodnom kódexe pre dodávateľov spoločnosti Nemak. • Dodávateľ zodpovedá za to, že jeho zamestnanci sú kompetentní a/alebo certifikovaní na poskytovanie služieb a že si túto úroveň udržia počas trvania Zmluvy. Spôsobilosť a/alebo certifikáciu personálu musí byť možné preukázať k spokojnosti spoločnosti Nemak. • Dodávateľ písomne informuje svojich zamestnancov o obsahu tohto dokumentu. V prípade, že si to Nemak vyžiada, môže požiadať Dodávateľa o písomné potvrdenie, že informoval svojich zamestnancov o obsahu tohto dokumentu, a Dodávateľ zabezpečí jeho prísne dodržiavanie a súlad s ním zo strany svojich zamestnancov alebo všetkých zamestnancov subdodávateľov.
Zásady prijateľného používania IT infraštruktúry	• Dodávateľ musí vždy riadne využívať fyzické a logické zdroje poskytnuté spoločnosťou Nemak

Logické riadenie prístupu	• Zamestnanci a/alebo zamestnanci subdodávateľov Dodávateľa musia akceptovať požiadavky na bezpečnosť informácií. Dôkaz o prijatí týchto podmienok musí byť k dispozícii, ak to vyžaduje akýkoľvek audit alebo na iné účely.
	• Dodávateľ súhlasí s tým, že bude mať politiku pre heslá vo svojich vlastných infraštruktúrnych systémoch s týmito kritériami:
	  ○ Minimálna dĺžka 10 znakov, pričom z každej skupiny 3 znakov (malé, veľké písmená, čísla) musí byť aspoň jeden znak.
	  ○ Systémy by mali byť nakonfigurované tak, aby vyžadovali zmenu hesla aspoň raz za 12 mesiacov alebo okamžite, ak sa objaví čo i len najmenší náznak, že heslo bolo akýmkoľvek spôsobom kompromitované, alebo ak existuje pochybnosť, že by ho mohla poznať tretia strana.
	• Po ukončení služieb alebo zmluvy Dodávateľ zakáže alebo zruší účty zamestnancov alebo tretích strán na používanie IT infraštruktúry Dodávateľa.
	• Ak spoločnosť Nemak poskytne účty a heslá na pripojenie k systémom spoločnosti Nemak, nesmú byť zverejnené a/alebo poskytnuté žiadnej tretej strane alebo zamestnancom dodávateľa, ktorí nie sú súčasťou poskytovania služieb alebo dodávok produktov. V prípade individuálnych účtov poskytnutých spoločnosťou Nemak sa nesmú zverejniť a/alebo zdieľať medzi zamestnancami, aj keď sú súčasťou poskytovania služieb alebo dodávania produktov.
	• Dodávateľ je zodpovedný za všetky činnosti vykonávané pomocou účtov a hesiel, ktoré Nemak poskytol zamestnancom Dodávateľa.
	• Spoločnosť Nemak ukončí prístup Dodávateľa k Informáciám, keď:
	  ○ Účel bol splnený.
	  ○ Dodávateľ porušil tieto bezpečnostné pokyny.
	  ○ Zistí sa akákoľvek podozrivá aktivita.
	  ○ Keď to Nemak uzná za vhodné.
	• V prípade, že spoločnosť Nemak poskytuje používateľské účty (napr. účty Active Directory, prístup VPN, e-mail atď.) Dodávateľovi alebo tretím stranám, ktoré sú

subdodávateľmi Dodávateľa, Dodávateľ musí okamžite informovať spoločnosť Nemak, ak sa uplatní niektorý z nasledujúcich bodov:

- Zamestnanec alebo tretia strana, s ktorou bola uzatvorená subdodávateľská zmluva, ukončí pracovný pomer alebo už nie je v zmluvnom vzťahu s dodávateľom.
- Zamestnanec alebo subdodávateľská tretia strana už neposkytuje spoločnosti Nemak služby.

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

Riadenie IT infraštruktúry

Prístup k sieti

- Sieť dodávateľa musí byť chránená firewallom a prístup k nej môžu mať len zamestnanci dodávateľa.
- Pracovníci 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 použije bezpečný výmaz informácií, aby zabezpečil riadne vymazanie (prípadne vrátenie) Informácií.

Antimalvérová ochrana

- Dodávateľ bude udržiavať produkty a zariadenia používané na poskytovanie služieb alebo dodávku produktov s najnovšími verziami antimalvéru a aktualizáciami poskytovanými výrobcom. Firewall v počítačovom vybavení musí byť zapnutý tak, aby blokoval akýkoľvek pokus o škodlivý softvér.

Správa zraniteľností

- Dodávateľ je povinný skenovať zraniteľnosti v rámci IT infraštruktúry s cieľom odhaliť, 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 zaviesť plán nápravy.

Oprava systémov

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

Odstránenie prístupu do siete VPN

- Dodávateľ sa zaväzuje používať na pripojenie k svojim zariadeniam len sieť VPN s overením Active Directory a bez iných možností pripojenia. Ak je to možné, Dodávateľ použije viacfaktorovú autentifikáciu s VPN.
- Prístup do VPN sa nesmie zdieľať medzi jednotlivcami.

Používanie cloudových služieb

V prípade poskytovateľov cloudových služieb sa Dodávateľ zaväzuje zahrnúť nasledujúce ustanovenia týkajúce sa ochrany údajov spoločnosti Nemak a dostupnosti služieb:

	• Poskytovanie špecializovanej podpory v prípade incidentu informačnej bezpečnosti v prostredí cloudových služieb. • Podporujte organizáciu pri zhromažďovaní digitálnych dôkazov, pričom zohľadnite zákony a predpisy týkajúce sa digitálnych dôkazov v rôznych jurisdikciách. • Zabezpečenie požadovaného zálohovania údajov a informácií o konfigurácii a bezpečná správa záloh podľa potreby. • Poskytnutie a vrátenie informácií, ako sú konfiguračné súbory, zdrojový kód, protokoly a údaje, ktoré sú vo vlastníctve organizácie, na požiadanie počas poskytovania služby alebo pri ukončení služby. Poskytovateľ cloudových služieb musí vždy informovať: • zmeny technickej infraštruktúry (napr. premiestnenie, rekonfigurácia alebo zmeny hardvéru alebo softvéru), ktoré ovplyvňujú alebo menia ponuku cloudových služieb. • Spracovanie alebo uchovávanie informácií v novej geografickej alebo právnej jurisdikcii. • Používanie rovnocenných poskytovateľov cloudových služieb alebo iných subdodávateľov (vrátane zmeny existujúcich alebo využívania nových strán).
Informovanosť o informačnej bezpečnosti	• Dodávateľ musí zaviesť programy zvyšovania povedomia a vzdelávania (u všetkých svojich zamestnancov) v oblasti informačnej bezpečnosti, prijímania preventívnych opatrení a zavádzania politík, postupov a kontrolných mechanizmov, ako klasifikovať a spravovať informácie. • Dodávateľ musí svojim zamestnancom aspoň raz ročne poskytnúť základné bezpečnostné školenie a zabezpečiť, aby si boli vedomí: ○ Riziká phishingu ○ Udržiavanie hesla v bezpečí ○ Používanie silných hesiel ○ Sociálne inžinierstvo ○ Sociálne médiá
Riziká kybernetickej bezpečnosti a riadenie incidentov	• Dodávateľ identifikuje riziká kybernetickej bezpečnosti a prijme vhodné opatrenia na predchádzanie bezpečnostným incidentom. • V prípade, že je Dodávateľ zapojený do bezpečnostného incidentu, ktorý má vplyv na spoločnosť Nemak, Dodávateľ v koordinácii s CSIRT spolupracuje na obnovení normálnej prevádzky. • Dodávateľ je povinný bezodkladne informovať spoločnosť Nemak o akomkoľvek skutočnom alebo potenciálnom kybernetickom bezpečnostnom incidente a narušení bezpečnosti údajov.
Kontinuita podnikania	• Dodávateľ vypracuje plány kontinuity prevádzky pre kritické systémy. Tieto plány musia okrem iného zahŕňať postupy obnovy po havárii, ktoré sa testujú aspoň raz ročne.
Audit	• Nemak má právo: ○ Audit výkonu a dodržiavania týchto bezpečnostných pokynov zo strany dodávateľa. ○ požadovať prístup k správam/osvedčeniam tretích strán, ktoré potvrdzujú dodržiavanie kontrol súvisiacich s poskytovaním služieb alebo dodávkou výrobkov.
Dodržiavanie predpisov	• Dodávateľ je povinný riadne využívať všetky práva duševného vlastníctva a autorské práva spoločnosti Nemak a tretích strán.

- Dodávateľ zodpovedá spoločnosti Nemak za akékoľvek porušenie svojich povinností uvedených v týchto bezpečnostných pokynoch.
- Nedodržanie týchto bezpečnostných pokynov zo strany dodávateľa alebo ktoréhokoľvek z jeho subdodávateľov môže viesť k sankciám uvedeným v dohode a platných zákonoch.
- Dodávateľ sa zaväzuje odškodniť, brániť a chrániť spoločnosť Nemak v prípade akéhokoľvek nároku vyplývajúceho z porušenia týchto bezpečnostných pokynov.
- Tieto bezpečnostné pokyny sa môžu z času na čas aktualizovať. Dodávateľ je povinný dodržiavať tieto Bezpečnostné pokyny po celú dobu, kým udržiava obchodný vzťah so spoločnosťou Nemak.

Kontaktné informácie

Ak máte otázky alebo pripomienky týkajúce sa tohto usmernenia, môžete sa so svojou otázkou obrátiť na oddelenie informačnej bezpečnosti spoločnosti Nemak na adrese isec.suppliers@nemak.com.

Revízie

Verzia	Dátum	Žiadateľ	Popis zmien
1.0	júl/2022	Ricardo Serrano	Vytvorenie usmernenia
2.0	august/2022	Edwin Macias	Zmena formátu dokumentu na usmernenie
3.0	marec/2023	Edwin Macias	Sekcia *Logické riadenie prístupu* zmenená: Text týkajúci sa ukončenia služieb dodávateľa alebo subdodávateľských tretích strán bol nanovo definovaný.
4.0	január/2024	Omar Duran	Pridaná časť *Používanie cloudových služieb*

Tento dokument sa riadi všeobecným procesom správy dokumentov opísaným v:

NPO-GBL-SEC-10 Politika správy dokumentov

Schválil

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

Tento dokument bol vytvorený pomocou nástroja na prekladanie

Wymagania dotyczące bezpieczeństwa informacji dla dostawców

Styczeń 2024 r.

Wprowadzenie i cel

Niniejsze wytyczne określają wymogi bezpieczeństwa informacji (zwane dalej "Wytycznymi bezpieczeństwa"), które muszą być przestrzegane przez wszystkich Dostawców klienta (zwanych dalej "Nemak").

Celem niniejszych Wytycznych dotyczących bezpieczeństwa jest ochrona wszelkich Informacji. Wytyczne dotyczące bezpieczeństwa stanowią integralną część każdej umowy zawartej pomiędzy Nemak a Dostawcą, a Dostawca jest zobowiązany do ich przestrzegania w celu ochrony poufności i integralności Informacji. Wymogi te mogą zostać uzupełnione innymi wymogami bezpieczeństwa, umową o gwarantowanym poziomie usług lub innym dokumentem uzgodnionym między 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, gdy nie jest możliwe spełnienie wymogu bezpieczeństwa, należy powiadomić o tym Nemak na następujący adres e-mail w celu dokonania odpowiedniej oceny: isec.suppliers@nemak.com

Cel

Poinformować Dostawcę o wszystkich Wytycznych dotyczących bezpieczeństwa, których musi przestrzegać w celu ochrony Informacji ujawnionych przez Nemak.

Definicje

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

Umowa
Wszelkie umowy, zamówienia zakupu, listy nominacyjne lub inne dokumenty określające warunki, na jakich produkty i/lub usługi mają być dostarczane i/lub świadczone na rzecz Nemak.

***CSIRT** (zespół reagowania na incydenty bezpieczeństwa cybernetycznego)*
Zespół reagowania na incydenty bezpieczeństwa cybernetycznego firmy Nemak.

Informacje
Wszelkie informacje poufne i zastrzeżone będące w posiadaniu i w jakikolwiek sposób związane z firmą Nemak lub jej przedsiębiorstwami, klientami, dostawcami lub jakąkolwiek stroną trzecią.

Audyt
Okresowy przegląd wyników Dostawcy i zgodności z Umową.

Dostawca
Każda osoba fizyczna lub prawna, która dostarcza produkty i/lub usługi firmie Nemak.

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

Zasoby fizyczne
Sprzęt komputerowy lub fizyczny wykorzystywany wyłącznie w celu 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 przyznawany wyłącznie w celu świadczenia usług lub dostarczania produktów.

	SLA Umowa o gwarantowanym poziomie usług
Role i obowiązki	***Nemak:*** Przekazywanie odpowiednich regulacji i środków Nemak stronom trzecim ***Dostawca:*** Zapewnienie zgodności z wymogami bezpieczeństwa informacji
Wymagania ogólne	• Dostawca podejmie wszelkie niezbędne środki w celu ochrony wszelkich Informacji, do których ma dostęp, w tym Platform i Usług Infrastruktury Nemak, niezależnie od tego, czy wynikają 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. • Dostawca będzie przestrzegać i spowoduje, że wszyscy podwykonawcy będą przestrzegać Wytycznych dotyczących bezpieczeństwa określonych w niniejszym dokumencie, a także będzie przechowywać dowody potwierdzające ich przestrzeganie. • Należy zawsze przestrzegać niniejszych Wytycznych dotyczących bezpieczeństwa, nawet jeśli zakres usług został zmodyfikowany przez Nemak i Dostawcę. • Podpisać Globalny Kodeks Biznesowy Nemak dla Dostawców, przy czym rozumie się, że tylko te Wytyczne dotyczące bezpieczeństwa, które odnoszą się do usług, które mają być świadczone, będą miały zastosowanie do Dostawcy.
Poufność	• Dostawca przyjmuje do wiadomości, że Informacje ujawnione przez Nemak, do których Dostawca, jego pracownicy lub podwykonawcy mają i/lub będą mieli dostęp, stanowią własność Nemak, jej klientów, dostawców i/lub stron trzecich i są chronione zobowiązaniami do zachowania poufności. • Dostawca ustanowi zasady, procedury i mechanizmy kontroli w celu zapobiegania nieuprawnionemu ujawnieniu Informacji przez pracowników lub personel podwykonawców, którzy mają dostęp do Informacji. • Dostęp do Informacji oraz Platformy Infrastrukturalnej i Usług będzie udzielany wyłącznie tym pracownikom i/lub personelowi, którym Dostawca zlecił podwykonawstwo na zasadzie ograniczonego dostępu i wyłącznie w odniesieniu do świadczenia usług lub dostawy produktów. • Dostawca oświadcza i gwarantuje, że dane osobowe lub informacje poufne mogą być wykorzystywane wyłącznie do celów biznesowych i w ścisłej zgodności z wszelkimi Umowami między stronami, a także z wszelkimi politykami Nemak i obowiązującym prawem. • Dostawca zapewni poufność Informacji, do których ma dostęp, poprzez zawarcie jednej lub kilku umów o zachowaniu poufności. • Dostawca podejmie proaktywne środki w celu prawidłowego zabezpieczenia danych osobowych lub informacji poufnych, które zostaną mu ujawnione w celu dostarczenia produktów i/lub usług.
Bezpieczeństwo fizyczne	• Dostawca dopilnuje, aby dostęp do danych osobowych i informacji poufnych miał wyłącznie upoważniony personel, zgodnie z zasadą ograniczonego dostępu. • Dostawca podejmie niezbędne środki w celu ochrony własnych obiektów oraz sprzętu i infrastruktury IT. • Dostawca i/lub personel podwykonawcy muszą zawsze przestrzegać zasad i procedur bezpieczeństwa fizycznego Nemak.

Personel dostawcy	• Personel Dostawcy będzie unikać wszelkich konfliktów interesów zgodnie z Globalnym kodeksem biznesowym dla dostawców firmy Nemak. • Dostawca będzie odpowiedzialny za to, że jego personel jest kompetentny i/lub certyfikowany do świadczenia usług i że utrzyma ten poziom w okresie obowiązywania Umowy. Kompetencje i/lub certyfikacja personelu muszą być możliwe do wykazania w sposób satysfakcjonujący Nemak. • Dostawca poinformuje swój personel na piśmie o treści niniejszego dokumentu. W razie potrzeby Nemak może zażądać od Dostawcy pisemnego potwierdzenia, że poinformował on swój personel o treści niniejszego dokumentu, a Dostawca zapewni ścisłe przestrzeganie tego dokumentu przez swój personel lub personel podwykonawców.
Zasady dopuszczalnego użytkowania infrastruktury IT	• Dostawca będzie zawsze dobrze wykorzystywać Zasoby Fizyczne i Logiczne dostarczone przez Nemak
Logiczna kontrola dostępu	• Pracownicy i/lub personel podwykonawców Dostawcy muszą zaakceptować wymogi dotyczące bezpieczeństwa informacji. Dowód akceptacji takich warunków będzie dostępny, jeśli będzie to wymagane przez jakikolwiek audyt lub do jakichkolwiek innych celów. • Dostawca zgadza się posiadać politykę dotyczącą haseł we własnych systemach infrastruktury, obejmującą następujące kryteria: ○ Minimalna długość 10 znaków, w tym co najmniej jeden znak z każdej z 3 grup znaków (małe litery, duże litery, cyfry). ○ Systemy powinny być skonfigurowane tak, aby wymagały zmiany hasła co najmniej raz na 12 miesięcy lub natychmiast, jeśli istnieją najmniejsze oznaki, że hasło zostało w jakikolwiek sposób naruszone lub jeśli istnieją wątpliwości, że osoba trzecia może je znać. • Po zakończeniu świadczenia usług lub rozwiązaniu umowy Dostawca wyłączy lub usunie konta pracowników lub osób trzecich umożliwiające korzystanie z Infrastruktury IT Dostawcy. • Jeśli Nemak udostępnia konta i hasła do łączenia się z systemami Nemak, nie mogą one być ujawniane i/lub udostępniane osobom trzecim lub pracownikom Dostawcy, którzy nie uczestniczą w świadczeniu usług lub dostarczaniu produktów. W przypadku zindywidualizowanych kont przyznanych przez Nemak, nie wolno ich ujawniać i/lub udostępniać pracownikom, nawet jeśli uczestniczą oni w świadczeniu usług lub dostarczaniu produktów. • Dostawca ponosi odpowiedzialność za wszelkie działania wykonywane przy użyciu kont i haseł udostępnionych przez Nemak personelowi Dostawcy. • Nemak zakończy dostęp Dostawcy do Informacji, gdy: ○ Cel został osiągnięty. ○ Dostawca naruszył niniejsze Wytyczne dotyczące bezpieczeństwa. ○ Każda podejrzana aktywność jest wykrywana. ○ Kiedy Nemak uzna to za stosowne.

- W przypadku, gdy Nemak udostępnia konta użytkowników (np. konta Active Directory, dostęp VPN, pocztę e-mail itp.) Dostawcy lub podwykonawcom Dostawcy, Dostawca musi niezwłocznie powiadomić Nemak o wystąpieniu któregokolwiek z poniższych przypadków:
  - Pracownik lub osoba trzecia będąca podwykonawcą zostaje zwolniona lub nie pozostaje już w stosunku umownym z Dostawcą.
  - Pracownik lub podwykonawca nie świadczy już usług na rzecz Nemak.

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

Zarządzanie infrastrukturą IT

Dostęp do sieci

- Sieć Dostawcy będzie chroniona zaporami ogniowymi, a dostęp do niej będzie możliwy wyłącznie dla personelu Dostawcy.
- Personel Dostawcy powinien używać użytkownika Active Directory do łączenia się z siecią.

Bezpieczne usuwanie

- Po zakończeniu relacji biznesowych z Nemak lub na żądanie Nemak, w zależności od tego, co nastąpi wcześniej, Dostawca zastosuje bezpieczne usuwanie informacji, aby zapewnić prawidłowe usunięcie (lub zwrot, jeśli dotyczy) Informacji.

Ochrona przed złośliwym oprogramowaniem

- Dostawca będzie utrzymywać produkty i sprzęt wykorzystywany do świadczenia usług lub dostarczania produktów z najnowszymi wersjami oprogramowania antymalware i aktualizacjami dostarczonymi przez producenta. Firewall w sprzęcie komputerowym musi być włączony, aby blokować wszelkie próby złośliwego oprogramowania.

Zarządzanie podatnościami

- Dostawca przeprowadzi skanowanie w poszukiwaniu luk w zabezpieczeniach Infrastruktury IT w celu wykrycia, powiadomienia i usunięcia luk w zabezpieczeniach wykrytych podczas świadczenia usług lub dostarczania produktów, a także w sprzęcie Dostawcy wykorzystywanym do świadczenia usług lub dostarczania produktów.
- Dostawca wdroży plan naprawczy w przypadku wystąpienia jakichkolwiek luk w zabezpieczeniach.

Patchowanie systemów

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

Usuń dostęp VPN

- Dostawca zgadza się używać VPN do łączenia się ze swoimi obiektami wyłącznie z uwierzytelnianiem Active Directory i bez innych opcji połączenia. Jeśli to możliwe, Dostawca powinien używać uwierzytelniania wieloskładnikowego z VPN.
- Dostęp VPN nie może być współdzielony przez poszczególne osoby.

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 wymaganych kopii zapasowych danych i informacji konfiguracyjnych oraz bezpieczne zarządzanie kopiami zapasowymi. • Dostarczanie i zwracanie informacji, takich jak pliki konfiguracyjne, kod źródłowy, dzienniki i dane, które są własnością organizacji, na żądanie w trakcie świadczenia usługi lub po jej zakończeniu. Dostawca usług w chmurze zawsze musi o tym powiadomić: • Zmiany w infrastrukturze technicznej (np. przeniesienie, rekonfiguracja lub zmiany w sprzęcie lub oprogramowaniu), które wpływają na ofertę usług w chmurze lub ją zmieniają. • Przetwarzanie lub przechowywanie informacji w nowej jurysdykcji geograficznej lub prawnej. • Korzystanie z zewnętrznych dostawców usług w chmurze lub innych podwykonawców (w tym zmiana istniejących lub korzystanie z nowych podmiotów).
Świadomość bezpieczeństwa informacji	• Dostawca wdroży programy uświadamiające i edukacyjne (wśród swoich pracowników) w odniesieniu do bezpieczeństwa informacji, podejmowania środków zapobiegawczych oraz wdrażania polityk, procedur i kontroli w zakresie klasyfikowania informacji i zarządzania nimi. • Dostawca musi zapewnić swoim pracownikom podstawowe szkolenie w zakresie bezpieczeństwa co najmniej raz w roku, upewniając się, że są oni świadomi: ○ Zagrożenia związane z phishingiem ○ Przechowywanie bezpiecznego hasła ○ Korzystanie z silnych haseł ○ Inżynieria społeczna ○ Media społecznościowe
Ryzyko związane z cyberbezpieczeństwem i zarządzanie incydentami	• Dostawca zidentyfikuje zagrożenia dla cyberbezpieczeństwa i podejmie odpowiednie działania w celu zapobiegania wszelkim incydentom bezpieczeństwa. • W przypadku, gdy Dostawca jest zaangażowany w Incydent bezpieczeństwa, który ma wpływ na Nemak, Dostawca, w porozumieniu z CSIRT, będzie współpracować w celu przywrócenia normalnej działalności. • Dostawca niezwłocznie powiadomi Nemak o wszelkich faktycznych lub potencjalnych incydentach cyberbezpieczeństwa i naruszeniach danych.
Ciągłość działania	• Dostawca opracuje plany ciągłości działania dla krytycznych systemów. Plany te obejmują między innymi procedury odzyskiwania danych po awarii, które są testowane co najmniej raz w roku.
Audyt	• Nemak ma prawo do: ○ Audyt wyników Dostawcy i zgodności z niniejszymi Wytycznymi dotyczącymi bezpieczeństwa. ○ Żądanie dostępu do raportów/certyfikatów stron trzecich, które potwierdzają zgodność z kontrolami związanymi ze świadczeniem usług lub dostawą produktów.

Zgodność

- Dostawca będzie w należyty sposób korzystać z wszelkich praw własności intelektualnej i praw autorskich Nemak i osób trzecich.
- Dostawca ponosi odpowiedzialność wobec Nemak za wszelkie naruszenia swoich 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 zabezpieczyć, bronić i chronić firmę Nemak przed wszelkimi roszczeniami wynikającymi z naruszenia niniejszych Wytycznych dotyczących bezpieczeństwa.
- Niniejsze Wytyczne dotyczące bezpieczeństwa mogą być okresowo aktualizowane. Dostawca będzie przestrzegać niniejszych Wytycznych dotyczących bezpieczeństwa tak długo, jak długo będzie utrzymywać relacje biznesowe z Nemak.

Informacje kontaktowe

W przypadku pytań lub uwag dotyczących niniejszych wytycznych można skontaktować się z działem bezpieczeństwa informacji firmy Nemak pod adresem isec.suppliers@nemak.com .

Zmiany

Wersja	Data	Wnioskodawca	Opis zmian
1.0	Lipiec/2022 r.	Ricardo Serrano	Tworzenie wytycznych
2.0	Sierpień/2022 r.	Edwin Macias	Zmieniono format dokumentu na wytyczne
3.0	Marzec/2023 r.	Edwin Macias	Sekcja *Logiczna kontrola dostępu* została zmieniona: Tekst dotyczący zakończenia świadczenia usług przez Dostawcę lub Podwykonawcę został ponownie zdefiniowany.
4.0	Styczeń/2024 r.	Omar Duran	Dodano sekcję *Korzystanie z usług w chmurze*

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

NPO-GBL-SEC-10 Polityka zarządzania dokumentami

Zatwierdzony przez

Wersja	Data	Imię i nazwisko zatwierdzającego
1.0	Lipiec/2022 r.	Edwin Macias
2.0	Sierpień/2022 r.	Alejandro Valdes Flores
3.0	Marzec/2023 r.	Alejandro Valdes Flores
4.0	Styczeń/2024 r.	Edwin Macias

Niniejszy dokument został utworzony przy użyciu narzędzia tłumaczącego

Információbiztonsági követelmények a beszállítókkal szemben

január 2024

Bevezetés és cél

Ezek az irányelvek meghatározzák azokat az információbiztonsági követelményeket (a továbbiakban: "Biztonsági irányelvek"), amelyeket az ügyfél (a továbbiakban: "Nemak") valamennyi beszállítójának be kell tartania.

A jelen biztonsági irányelvek célja az információk védelme. A Biztonsági irányelvek a Nemak és a Beszállító között létrejött bármely megállapodás szerves részét képezik, és a Beszállító köteles betartani azokat az Információk bizalmas jellegének és integritásának védelme érdekében. Ezek a követelmények kiegészíthetők egyéb biztonsági követelményekkel, bármely szolgáltatási szintű megállapodással vagy a Nemak és a Beszállító között elfogadott bármely más dokumentummal.

Terjedelem

Ez a dokumentum minden olyan beszállítóra vonatkozik, aki a Nemak tulajdonában lévő és/vagy általa nyilvánosságra hozott bármilyen típusú információhoz hozzáfér vagy hozzáférhet.

Kivételek

Amennyiben valamely biztonsági követelménynek nem lehet megfelelni, azt a Nemaknak kell jelezni a következő e-mail címen a megfelelő értékelés érdekében: isec.suppliers@nemak.com.

Célkitűzés

Tájékoztatja a Szállítót az összes olyan biztonsági irányelvről, amelyet a Nemak által átadott információk védelme érdekében be kell tartania.

Fogalommeghatározások

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

Megállapodás
Bármilyen megállapodás, megrendelés, megbízólevél vagy egyéb dokumentum, amely meghatározza azokat a feltételeket, amelyek alapján a termékeket és/vagy szolgáltatásokat a Nemaknak kell szállítani és/vagy nyújtani.

***CSIRT** (Cyber Security Incident Response Team - Kiberbiztonsági incidensekre reagáló csoport)*
A Nemak kiberbiztonsági incidensekre reagáló csoportja.

Információ
Minden bizalmas és védett információ, amely a Nemak vagy annak vállalkozásai, ügyfelei, beszállítói vagy bármely harmadik fél birtokában van, és bármilyen módon kapcsolódik hozzá.

Auditálás
A Beszállító teljesítményének és a Megállapodásnak való megfelelésének rendszeres felülvizsgálata.

Beszállító
Bármely természetes vagy jogi személy, aki vagy amely termékeket és/vagy szolgáltatásokat nyújt a Nemaknak.

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

Fizikai erőforrások
Kizárólag a szolgáltatások nyújtásához vagy a termékek szállításához használt hardver vagy fizikai berendezések (pl. számítógépek, nyomtatók, szerverek, monitorok, mobil eszközök, cserélhető adathordozók stb.).

	Logikai erőforrások Olyan szoftverek, rendszerek vagy alkalmazások, amelyekhez kizárólag a szolgáltatások nyújtása vagy a termékek szállítása céljából biztosítanak hozzáférést. ***SLA*** Szolgáltatási szintű megállapodás
Szerepek és felelősségek	***Nemak:*** A Nemak megfelelő szabályozásának és intézkedéseinek közlése harmadik felekkel. ***Beszállító:*** Az információbiztonsági követelményeknek való megfelelés biztosítása
Általános követelmények	• A Szállító köteles minden szükséges intézkedést megtenni annak érdekében, hogy megvédjen minden olyan információt, amelyhez hozzáfér, beleértve a Nemak infrastruktúra platformjait és szolgáltatásait, függetlenül attól, hogy az a szolgáltatások nyújtásából vagy a termékek szállításából származik, vagy bármely más okból, amiért a Szállítónak szüksége van a Nemak információihoz, platformjához és/vagy infrastrukturális szolgáltatásaihoz való hozzáférésre. • A Szállító köteles betartani, és köteles az alvállalkozókat is betartatni az itt meghatározott biztonsági irányelvekkel, és köteles az ilyen megfelelést igazoló bizonyítékokat megőrizni. • Mindig tartsa be ezeket a biztonsági irányelveket, még akkor is, ha a Nemak és a Szállító módosította a szolgáltatások körét. • Aláírja a Nemak globális üzleti szabályzatát a beszállítók számára, azzal, hogy a Beszállítóra csak azok a biztonsági irányelvek vonatkoznak, amelyek a nyújtandó szolgáltatásokra vonatkoznak.
Bizalmasság	• A Beszállító tudomásul veszi, hogy a Nemak által közölt információk, amelyekhez a Beszállító, annak alkalmazottai vagy alvállalkozói hozzáférnek és/vagy hozzáférnek, a Nemak, ügyfelei, beszállítói és/vagy harmadik felek tulajdonát képezik, és titoktartási kötelezettségvállalás védi őket. • A Szállító köteles olyan irányelveket, eljárásokat és ellenőrzéseket kialakítani, amelyek megakadályozzák, hogy az információkhoz hozzáféréssel rendelkező alkalmazottak vagy alvállalkozók jogosulatlanul felfedjék az információkat. • Az információkhoz, valamint az infrastruktúra platformhoz és a szolgáltatásokhoz való hozzáférés csak a Szállító által alvállalkozói szerződéssel megbízott alkalmazottak és/vagy személyzet számára engedélyezett, a szükséges ismeretek alapján és kizárólag a szolgáltatások nyújtása vagy a termékek szállítása tekintetében. • A Szállító kijelenti és garantálja, hogy a személyes adatok vagy bizalmas információk kizárólag üzleti célokra és a felek közötti megállapodásokkal, valamint a Nemak szabályzatával és az alkalmazandó jogszabályokkal szigorúan összhangban használhatók fel. • A Szállító egy vagy több titoktartási megállapodás megkötésével biztosítja a számára hozzáférhető információk bizalmas kezelését. • A Szállítónak proaktív intézkedéseket kell tennie a termékek és/vagy szolgáltatások nyújtása céljából átadott személyes adatok vagy bizalmas információk megfelelő védelme érdekében.
Fizikai biztonság	• A szállító biztosítja, hogy a személyes adatokhoz és bizalmas információkhoz csak az arra felhatalmazott személyzet férjen hozzá, a szükséges ismeretek alapján.

	• A Szállító megteszi a szükséges intézkedéseket saját létesítményeinek, informatikai berendezéseinek és infrastruktúrájának védelme érdekében. • 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 az összeférhetetlenséget a Nemak Szállítókra vonatkozó globális üzleti kódexében meghatározottak szerint. • A Beszállító felelős azért, hogy személyzete rendelkezik a szolgáltatások nyújtásához szükséges szakértelemmel és/vagy képesítéssel, és hogy ezt a szintet a Megállapodás időtartama alatt fenntartja. A személyzet alkalmasságát és/vagy képesítését a Nemak számára kielégítően igazolni kell. • A Szállító írásban tájékoztatja személyzetét a jelen dokumentum tartalmáról. Amennyiben a Nemak kéri, a Szállító írásban kérheti a Szállítótól annak igazolását, hogy tájékoztatta személyzetét a jelen dokumentum tartalmáról, és a Szállító köteles biztosítani, hogy a saját vagy az alvállalkozói személyzet szigorúan betartsa és betartsa azt.
IT infrastruktúra elfogadható használatra vonatkozó szabályzat	• A Szállító mindig megfelelően használja a Nemak által biztosított fizikai és logikai erőforrásokat.
Logikai hozzáférés-szabályozás	• A Szállító által alkalmazott és/vagy alvállalkozói személyzetnek el kell fogadnia az információbiztonsági követelményeket. Az ilyen feltételek elfogadásának bizonyítékait rendelkezésre kell bocsátani, ha bármilyen ellenőrzés vagy egyéb célú ellenőrzés megköveteli. • A szállító vállalja, hogy saját infrastrukturális rendszereinek jelszavaira vonatkozóan a következő kritériumoknak megfelelő politikát alkalmaz: ○ Minimum 10 karakter hosszú, legalább egy karakter a 3 karaktercsoportból (kisbetűk, nagybetűk, számok). ○ A rendszereket úgy kell beállítani, hogy legalább 12 havonta egyszer jelszócserét írjanak elő, vagy azonnal, ha a legkisebb jele is van annak, hogy a jelszó bármilyen módon veszélybe került, vagy ha kétséges, hogy egy harmadik fél ismerheti azt. • A szolgáltatások vagy a szerződés megszűnésekor a Szállító köteles letiltani vagy megszüntetni a Szállító informatikai infrastruktúráját használó alkalmazottak vagy harmadik felek fiókjait. • Ha a Nemak a Nemak rendszereihez való csatlakozáshoz fiókokat és jelszavakat biztosít, ezeket nem lehet felfedni és/vagy megosztani harmadik féllel vagy a Szállító azon munkatársaival, akik nem vesznek részt a szolgáltatásnyújtásban vagy a termékértékesítésben. A Nemak által biztosított egyedi fiókok esetében azokat nem szabad felfedni és/vagy megosztani a személyzet között, még akkor sem, ha azok a szolgáltatások nyújtásában vagy a termékek szállításában részt vesznek. • A Beszállító felel minden olyan tevékenységért, amelyet a Nemak által a Beszállító személyzete számára biztosított fiókokkal és jelszavakkal végeznek. • A Nemak megszünteti a Szállító hozzáférését az információkhoz, ha: ○ A cél teljesült.

- A Szállító megsértette a jelen Biztonsági Irányelveket.
- Bármilyen gyanús tevékenységet észlel.
- Amikor Nemak úgy ítéli meg, hogy megfelelő.

- Abban az esetben, ha a Nemak felhasználói fiókokat (pl. Active Directory fiókokat, VPN hozzáférést, e-mailt stb.) biztosít a Szállító vagy a Szállító által alvállalkozóként megbízott harmadik felek számára, a Szállító köteles haladéktalanul értesíteni a Nemakot, ha az alábbiak bármelyike fennáll:
  - A munkavállaló vagy alvállalkozó harmadik fél megszűnik, vagy már nem áll szerződéses kapcsolatban a Szállítóval.
  - Az alkalmazott vagy alvállalkozó harmadik fél már nem nyújt szolgáltatást a Nemaknak.

  Az értesítéseket a Nemak beszállítói kapcsolattartójának és a Nemak információbiztonsági igazgatójának kell elküldeni: isec.suppliers@nemak.com.

IT infrastruktúra-menedzsment

Hálózati hozzáférés

- A szállítói hálózatot tűzfalakkal kell védeni, és ahhoz csak a szállító személyzete férhet hozzá.
- A szállító személyzete a hálózathoz való csatlakozáshoz aktív könyvtárfelhasználót használ.

Biztonságos törlés

- A Nemakkal fennálló üzleti kapcsolat megszűnésekor vagy a Nemak kérésére, attól függően, hogy melyik történik előbb, a Szállító alkalmazza az információk biztonságos törlését az információk megfelelő törlésének (vagy adott esetben visszaadásának) biztosítása érdekében.

Antimalware védelem

- A Szállító a szolgáltatások nyújtásához vagy a termékek szállításához használt termékeket és berendezéseket a gyártó által biztosított legújabb antimalware verziókkal és frissítésekkel tartja karban. A számítógépes berendezések tűzfalának engedélyezve kell lennie, hogy blokkolja a rosszindulatú szoftverek próbálkozásait.

Sebezhetőségkezelés

- A Beszállító köteles az informatikai infrastruktúrán belül a sebezhetőségeket vizsgálni, hogy a szolgáltatások nyújtása vagy a termékek szállítása során, valamint a Beszállító által a szolgáltatások nyújtásához vagy a termékek szállításához használt berendezésekben talált sebezhetőségeket felderítse, értesítse és orvosolja.
- A szállítónak javítási tervet kell végrehajtania a sebezhetőségek esetén.

Rendszerek foltozása

- A szállító biztosítja, hogy a szerverek, a felhasználói számítógépek és a mobil eszközök a javítás kiadását követő legfeljebb 60 napon belül javításra kerüljenek.

VPN hozzáférés eltávolítása

	• A szállító vállalja, hogy a VPN-t kizárólag Active Directory-hitelesítéssel és más csatlakozási lehetőség nélkül használja a létesítményeihez való csatlakozáshoz. Ha lehetséges, a Szállítónak a VPN mellett többfaktoros hitelesítést kell használnia. • A VPN-hozzáférés nem osztható meg magánszemélyek között.
Felhőszolgáltatások használata	A felhőszolgáltatók esetében a Szállító vállalja, hogy a Nemak adatainak védelme és a szolgáltatások rendelkezésre állása érdekében a következő rendelkezéseket tartalmazza: • Célzott támogatás nyújtása a felhőszolgáltatási környezetben bekövetkező információbiztonsági incidensek esetén. • Támogatja a szervezetet a digitális bizonyítékok összegyűjtésében, figyelembe véve a különböző joghatóságok digitális bizonyítékokra vonatkozó törvényeit és előírásait. • Az adatok és a konfigurációs információk szükséges biztonsági mentése és adott esetben a biztonsági mentések biztonságos kezelése. • A szolgáltatás nyújtása során vagy a szolgáltatás megszűnésekor kérésre a szervezet tulajdonát képező információkat, például konfigurációs fájlokat, forráskódot, naplókat és adatokat szolgáltasson és szolgáltasson vissza. A felhőszolgáltatónak mindig értesítenie kell: • A műszaki infrastruktúrában bekövetkező olyan változások (pl. áthelyezés, átkonfigurálás, vagy a hardver vagy szoftver módosítása), amelyek befolyásolják vagy megváltoztatják a felhőszolgáltatási ajánlatot. • Az információk feldolgozása vagy tárolása egy új földrajzi vagy jogi joghatóságban. • Egyenrangú felhőszolgáltatók vagy más alvállalkozók használata (beleértve a meglévő felek cseréjét vagy újak igénybevételét).
Információbiztonsági tudatosság	• A szállítónak tudatossági és tanulási programokat kell végrehajtania (alkalmazottai körében) az információbiztonsággal, a megelőző intézkedések meghozatalával, valamint az információk osztályozására és kezelésére vonatkozó irányelvek, eljárások és ellenőrzések végrehajtásával kapcsolatban. • A szállítónak legalább évente egyszer alapvető biztonsági képzésben kell részesítenie alkalmazottait, biztosítva, hogy tisztában legyenek a következőkkel: ○ Adathalász kockázatok ○ A jelszó biztonságban tartása ○ Erős jelszavak használata ○ Társadalmi mérnöki tevékenység ○ Közösségi média
Kiberbiztonsági kockázatok és incidenskezelés	• A szállító azonosítja a kiberbiztonsági kockázatokat, és megfelelő intézkedéseket tesz a biztonsági incidensek megelőzése érdekében. • Amennyiben a Beszállító olyan biztonsági incidensben érintett, amely érinti a Nemakot, a Beszállító a CSIRT-tel együttműködve dolgozik a normál működés helyreállításán. • A Szállító köteles haladéktalanul értesíteni a Nemakot minden tényleges vagy potenciális kiberbiztonsági incidensről és adatvédelmi incidensről.
Üzletmenet-folytonosság	• A szállítónak üzletmenet-folytonossági terveket kell kidolgoznia a kritikus rendszerekre. Ezeknek a terveknek tartalmazniuk kell többek között, de nem kizárólagosan, katasztrófa utáni helyreállítási eljárásokat, amelyeket legalább évente egyszer tesztelnek.

Auditálás	• A Nemak jogosult: ○ Ellenőrzi a Beszállító teljesítményét és a jelen Biztonsági Irányelveknek való megfelelését. ○ hozzáférést kérhet a harmadik féltől származó olyan jelentésekhez/tanúsítványokhoz, amelyek igazolják a szolgáltatások nyújtásához vagy a termékek szállításához kapcsolódó ellenőrzéseknek való megfelelést.
Megfelelés	• A Szállító köteles a Nemak és harmadik felek szellemi tulajdonjogait és szerzői jogait megfelelően felhasználni. • A Szállító felelős a Nemakkal szemben a jelen Biztonsági irányelvekben foglalt kötelezettségeinek megszegéséért. • Ha a Szállító vagy bármely alvállalkozója nem tartja be a jelen biztonsági irányelveket, az a Megállapodásban és az alkalmazandó jogszabályokban meghatározott szankciókat vonhat maga után. • A Beszállító vállalja, hogy kártalanítja, védi és mentesíti a Nemakot a jelen Biztonsági Irányelvek megsértéséből eredő bármely követelés esetén. • Ezek a biztonsági iránymutatások időről időre frissíthetők. A Szállító köteles betartani a jelen Biztonsági irányelveket mindaddig, amíg üzleti kapcsolatot tart fenn a Nemakkal.
Kapcsolattartási információk	Ha kérdése vagy észrevétele van ezzel az iránymutatással kapcsolatban, a Nemak Információbiztonsághoz fordulhat a isec.suppliers@nemak.com címen.

Felülvizsgálatok

Verzió	Dátum	Kérelmező	A változások leírása
1.0	július/2022	Ricardo Serrano	Irányelv létrehozása
2.0	augusztus/2022	Edwin Macias	A dokumentum formátuma iránymutatássá változott
3.0	március/2023	Edwin Macias	*A Logikai hozzáférés-szabályozás* szakasz megváltozott: A Szállító vagy az alvállalkozó harmadik felek szolgáltatásainak megszűnésére vonatkozó szövegrész újrafogalmazásra került.
4.0	január/2024	Omar Duran	*A felhőszolgáltatások használata* szakasz hozzáadva

Ez a dokumentum a dokumentumkezelés általános folyamatát követi, amelyet a következő dokumentumban ismertetünk:

NPO-GBL-SEC-10 Dokumentumkezelési politika

Jóváhagyta

Verzió	Dátum	A jóváhagyó neve
1.0	július/2022	Edwin Macias
2.0	augusztus/2022	Alejandro Valdes Flores
3.0	március/2023	Alejandro Valdes Flores

4.0	január/2024	Edwin Macias

Ez a dokumentum egy fordítóprogrammal készült.

Требования к информационной безопасности для поставщиков

Январь 2024 года

Введение и цель	Настоящее руководство устанавливает требования к информационной безопасности (далее "Руководство по безопасности"), которые должны соблюдаться всеми поставщиками заказчика (далее "Nemak"). Целью настоящих Руководящих принципов безопасности является защита любой информации. Руководство по безопасности является неотъемлемой частью любого соглашения, заключенного между компанией Nemak и поставщиком, и поставщик должен соблюдать его для защиты конфиденциальности и целостности информации. Эти требования могут быть дополнены другими требованиями безопасности, любым соглашением об уровне обслуживания или любым другим документом, согласованным между Nemak и поставщиком.
Область применения	Этот документ относится ко всем поставщикам, которые имеют или могут иметь доступ к любому виду информации, принадлежащей компании Nemak и/или раскрываемой ею.
Исключения	В случае невозможности соблюдения требований безопасности следует сообщить об этом компании Nemak по следующему адресу электронной почты для соответствующей оценки: isec.suppliers@nemak.com.
Цель	Проинформировать Поставщика обо всех рекомендациях по безопасности, которые он должен соблюдать для защиты информации, раскрываемой компанией Nemak.
Определения	***Немак*** Nemak, S.A.B. de C.V. и ее дочерние компании. ***Соглашение*** Любое соглашение, заказ на поставку, письмо о назначении или другой документ, устанавливающий условия, на которых продукция и/или услуги должны быть поставлены и/или оказаны компании Nemak. ***CSIRT*** *(Группа реагирования на инциденты кибербезопасности)* Группа реагирования на инциденты кибербезопасности компании Nemak. ***Информация*** Вся конфиденциальная информация и информация, являющаяся собственностью компании Nemak, ее предприятий, клиентов, поставщиков или любых третьих лиц и имеющая к ней какое-либо отношение. ***Аудит*** Периодическая проверка работы Поставщика и соблюдения им всех условий Соглашения. ***Поставщик*** Любое физическое или юридическое лицо, предоставляющее продукты и/или услуги компании Nemak. ***Инфраструктурные платформы и услуги*** Системы, приложения и/или сетевые элементы и базы данных компании Nemak. ***Физические ресурсы*** Аппаратное или физическое оборудование, используемое исключительно в целях предоставления услуг или поставки продукции (например, компьютеры, принтеры, серверы, мониторы, мобильные устройства, съемные носители информации и т. д.).

	Логические ресурсы Программное обеспечение, системы или приложения, доступ к которым предоставляется исключительно в целях оказания услуг или поставки продукции. ***SLA*** Соглашение об уровне обслуживания
Роли и обязанности	***Немак:*** Сообщать третьим лицам о соответствующих правилах и мерах компании Nemak ***Поставщик:*** Обеспечение соответствия требованиям информационной безопасности
Общие требования	• Поставщик принимает все необходимые меры для защиты любой информации, к которой он имеет доступ, включая платформы и услуги инфраструктуры Nemak, независимо от того, получена ли она в результате предоставления услуг или поставки продукции или по любой другой причине, по которой Поставщику требуется доступ к информации, платформам и/или услугам инфраструктуры Nemak. • Поставщик должен соблюдать и заставлять любых субподрядчиков соблюдать Руководящие принципы безопасности, изложенные в настоящем документе, и должен сохранять доказательства, подтверждающие такое соблюдение. • Всегда соблюдайте эти Правила безопасности, даже если объем услуг был изменен компанией Nemak и поставщиком. • Подпишите Глобальный деловой кодекс компании Nemak для поставщиков, при этом подразумевается, что к поставщику будут применяться только те Руководства по безопасности, которые относятся к предоставляемым услугам.
Конфиденциальность	• Поставщик признает, что раскрытая компанией Nemak информация, к которой поставщик, его сотрудники или субподрядчики имеют и/или будут иметь доступ, является собственностью компании Nemak, ее клиентов, поставщиков и/или третьих лиц и защищена обязательствами о неразглашении. • Поставщик должен установить политику, процедуры и средства контроля для предотвращения любого несанкционированного раскрытия Информации сотрудниками или субподрядчиками, имеющими доступ к Информации. • Доступ к информации, инфраструктурной платформе и услугам предоставляется только сотрудникам и/или персоналу, привлеченному Поставщиком на субподрядной основе и исключительно в связи с оказанием услуг или поставкой продукции. • Поставщик заявляет и гарантирует, что персональные данные или конфиденциальная информация могут использоваться только в деловых целях и в строгом соответствии с любыми соглашениями между сторонами, а также политикой Nemak и действующим законодательством. • Поставщик должен обеспечить конфиденциальность информации, к которой он имеет доступ, путем заключения одного или нескольких соглашений о неразглашении. • Поставщик должен принимать активные меры для надлежащей защиты персональных данных или конфиденциальной информации, которые передаются ему в целях поставки продукции и/или услуг.
Физическая безопасность	• Поставщик должен обеспечить доступ к персональным данным и конфиденциальной информации только уполномоченному персоналу в соответствии с принципом "необходимо знать".

	• Поставщик должен принимать необходимые меры для защиты своих собственных объектов, ИТ-оборудования и инфраструктуры. • Персонал поставщика и/или субподрядчика должен всегда соблюдать политику и процедуры физической безопасности компании Nemak.
Персонал поставщика	• Персонал поставщика должен избегать любых конфликтов интересов, как указано в Глобальном деловом кодексе поставщиков компании Nemak. • Поставщик несет ответственность за то, что его персонал компетентен и/или сертифицирован для оказания услуг и что он поддерживает этот уровень в течение срока действия договора. Компетентность и/или сертификация персонала должна быть подтверждена к удовлетворению Nemak. • Поставщик должен в письменной форме проинформировать свой персонал о содержании данного документа. В случае необходимости Nemak может запросить у поставщика письменное подтверждение того, что он ознакомил свой персонал с содержанием данного документа, и поставщик должен обеспечить строгое соблюдение и выполнение этого документа своим персоналом или любым субподрядным персоналом.
Политика приемлемого использования ИТ-инфраструктуры	• Поставщик должен всегда эффективно использовать физические и логические ресурсы, предоставляемые компанией Nemak

Логическое управление доступом	• Сотрудники и/или персонал, привлеченный Поставщиком на субподрядной основе, должны принять требования информационной безопасности. Доказательства принятия таких условий должны быть доступны, если это требуется в ходе аудита или для любых других целей.
	• Поставщик обязуется разработать политику в отношении паролей в своих собственных инфраструктурных системах, руководствуясь следующими критериями:
	  ○ Минимальная длина 10 символов, по крайней мере, по одному символу из каждой из трех групп символов (строчные, прописные, цифры).
	  ○ Системы должны быть настроены таким образом, чтобы требовать смены пароля не реже одного раза в 12 месяцев или немедленно, если есть малейшие признаки того, что пароль был каким-либо образом скомпрометирован, или если есть сомнения, что он может быть известен третьему лицу.
	• После прекращения оказания услуг или расторжения контракта Поставщик должен отключить или ликвидировать учетные записи сотрудников или третьих лиц для использования ИТ-инфраструктуры Поставщика.
	• Если Nemak предоставляет учетные записи и пароли для подключения к системам Nemak, они не должны раскрываться и/или передаваться третьим лицам или сотрудникам Поставщика, которые не участвуют в предоставлении услуг или поставке продукции. Если Nemak предоставляет индивидуальные учетные записи, они не должны раскрываться и/или передаваться сотрудникам, даже если они участвуют в предоставлении услуг или поставке продукции.

- Поставщик несет ответственность за любую деятельность, осуществляемую с использованием учетных записей и паролей, предоставленных компанией Nemak персоналу поставщика.
- Nemak прекратит доступ Поставщика к Информации, если:
  - Цель была достигнута.
  - Нарушение Поставщиком настоящих Руководящих принципов безопасности.
  - Выявляются любые подозрительные действия.
  - Когда Немак сочтет это удобным.
- В случае, если Nemak предоставляет учетные записи пользователей (например, учетные записи Active Directory, VPN-доступ, электронную почту и т. д.) поставщику или третьим лицам, привлеченным поставщиком на субподрядной основе, поставщик должен немедленно уведомить Nemak, если применяется любое из следующих действий:
  - Сотрудник или субподрядчик уволен или больше не состоит в договорных отношениях с Поставщиком.
  - Сотрудник или привлеченная третья сторона больше не оказывают услуг компании Nemak.

  Уведомления должны быть направлены менеджеру по связям с поставщиками компании Nemak и в отдел информационной безопасности компании Nemak: isec.suppliers@nemak.com.

Управление ИТ-инфраструктурой

Доступ к сети

- Сеть поставщика должна быть защищена брандмауэрами, и доступ к ней может иметь только персонал поставщика.
- Для подключения к сети персонал поставщика должен использовать пользователя активного каталога.

Безопасное стирание

- После прекращения деловых отношений с Nemak или по запросу Nemak, в зависимости от того, что произойдет раньше, Поставщик должен применить безопасное удаление информации, чтобы обеспечить надлежащее удаление (или возврат, если применимо) Информации.

Защита от вредоносных программ

- Поставщик будет поддерживать продукты и оборудование, используемые для оказания услуг или поставки продуктов, с последними версиями антивирусных программ и обновлениями, предоставляемыми производителем. Брандмауэр в компьютерном оборудовании должен быть включен для блокирования любых попыток проникновения вредоносных программ.

Управление уязвимостями

- Поставщик обязуется проверять ИТ-инфраструктуру на наличие уязвимостей с целью обнаружения, уведомления и устранения уязвимостей, обнаруженных при оказании услуг или поставке продукции, а также на оборудовании Поставщика, используемом для оказания услуг или поставки продукции.

- Поставщик должен реализовать план по устранению уязвимостей в случае их обнаружения.

Исправление систем

- Поставщик должен обеспечить исправление серверов, пользовательских ПК и мобильных устройств в течение максимум 60 дней после выпуска патча.

Удалить доступ к VPN

- Поставщик соглашается использовать VPN для подключения к своим объектам только с аутентификацией Active Directory и без других вариантов подключения. Если возможно, поставщик должен использовать многофакторную аутентификацию с VPN.
- Доступ к VPN не может быть разделен между отдельными лицами.

Использование облачных сервисов

В случае с поставщиками облачных услуг поставщик соглашается включить следующие положения для защиты данных Nemak и доступности услуг:

- Обеспечение специализированной поддержки в случае инцидента информационной безопасности в среде облачных сервисов.
- Оказывать поддержку организации в сборе цифровых доказательств, принимая во внимание законы и правила, касающиеся цифровых доказательств в различных юрисдикциях.
- Обеспечение необходимого резервного копирования данных и конфигурационной информации, а также безопасное управление резервными копиями в соответствующих случаях.
- Предоставлять и возвращать информацию, такую как файлы конфигурации, исходный код, журналы и данные, принадлежащие организации, по запросу во время предоставления услуги или при ее прекращении.

Поставщик облачных услуг всегда должен уведомлять об этом:

- Изменения в технической инфраструктуре (например, перемещение, реконфигурация или изменения в аппаратном или программном обеспечении), которые влияют на предложение облачных услуг или изменяют его.
- Обработка или хранение информации в новой географической или юридической юрисдикции.
- Использование сторонних поставщиков облачных услуг или других субподрядчиков (включая изменение существующих или привлечение новых сторон).

Осведомленность в области информационной безопасности

- Поставщик должен внедрить программы повышения осведомленности и обучения (среди своих сотрудников) в отношении информационной безопасности, принятия превентивных мер и внедрения политик, процедур и средств контроля в отношении классификации и управления информацией.
- Поставщик должен не реже одного раза в год проводить для своих сотрудников базовое обучение по вопросам безопасности, обеспечивая их осведомленность:
  - Фишинговые риски
  - Сохранение пароля
  - Использование надежных паролей
  - Социальная инженерия
  - Социальные сети

Риски кибербезопасности и управление инцидентами	• Поставщик должен выявлять риски кибербезопасности и принимать соответствующие меры для предотвращения любых инцидентов, связанных с безопасностью. • Если поставщик вовлечен в инцидент безопасности, который затрагивает Nemak, то поставщик, в координации с CSIRT, должен работать вместе, чтобы вернуться к нормальной работе. • Поставщик должен немедленно уведомить компанию Nemak о любом фактическом или потенциальном инциденте, связанном с кибербезопасностью, и о нарушении конфиденциальности данных.
Непрерывность бизнеса	• Поставщик должен разработать планы обеспечения непрерывности бизнеса для критически важных систем. Эти планы должны включать, но не ограничиваться процедурами аварийного восстановления, которые проверяются не реже одного раза в год.
Аудит	• Немак имеет право: ○ Аудит работы Поставщика и соблюдения им настоящих Руководящих принципов безопасности. ○ Запрашивать доступ к отчетам/сертификатам третьих лиц, подтверждающим соблюдение мер контроля, связанных с предоставлением услуг или поставкой продукции.
Соответствие требованиям	• Поставщик должен надлежащим образом использовать все права интеллектуальной собственности и авторские права компании Nemak и третьих лиц. • Поставщик несет ответственность перед компанией Nemak за любое нарушение своих обязанностей, указанных в настоящем Руководстве по безопасности. • Несоблюдение Поставщиком или любым из его субподрядчиков данных Руководящих принципов безопасности может повлечь за собой штрафные санкции, предусмотренные Соглашением и действующим законодательством. • Поставщик соглашается возмещать ущерб, защищать и ограждать Nemak от любых претензий, возникающих в связи с нарушением данных Руководящих принципов безопасности. • Настоящее Руководство по безопасности может время от времени обновляться. Поставщик должен соблюдать эти Правила безопасности до тех пор, пока он поддерживает деловые отношения с компанией Nemak.
Контактная информация	Если у вас есть вопросы или комментарии по поводу данного руководства, вы можете обратиться в отдел информационной безопасности компании Nemak по адресу isec.suppliers@nemak.com.

Пересмотр

Версия	Дата	Запросчик	Описание изменений
1.0	Июль/2022	Рикардо Серрано	Создание руководства
2.0	Август/2022	Эдвин Макиас	Формат документа изменен на руководство
3.0	Март/2023	Эдвин Макиас	Изменен раздел *Управление логическим доступом:*

			Текст, связанный с прекращением услуг поставщика или субподрядчиков, был переформулирован.
4.0	Январь/2024	Омар Дюран	Добавлен раздел "*Использование облачных сервисов*

Этот документ соответствует общему процессу управления документами, описанному в:

NPO-GBL-SEC-10 Политика управления документами

Одобрено

Версия	Дата	Имя утверждающего лица
1.0	Июль/2022	Эдвин Макиас
2.0	Август/2022	Алехандро Вальдес Флорес
3.0	Март/2023	Алехандро Вальдес Флорес
4.0	Январь/2024	Эдвин Макиас

Этот документ был создан с помощью переводчика

对供应商的信息安全要求

2024 年 1 月

导言和目的	本指南规定了客户的所有供应商（以下简称 "Nemak"）必须遵守的信息安全要求（以下简称 "安全指南"）。 本《安全准则》旨在保护任何信息。安全指引构成 Nemak 与供应商之间签订的任何协议的组成部分，供应商应遵守这些指引以保护信息的保密性和完整性。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。
范围	本文件适用于所有接触或可能接触 Nemak 拥有和/或披露的任何类型信息的供应商。
例外情况	如果无法满足安全要求，应通过以下电子邮件通知 Nemak，以便进行相应评估： isec.suppliers@nemak.com
目标	告知供应商为保护 Nemak 披露的信息而必须遵守的所有安全准则。
定义	***尼马克*** Nemak, S.A.B. de C.V. 及其子公司。 ***协议*** 任何协议、采购订单、提名函或其他文件，其中规定了向 Nemak 供应和/或提供产品和/或服务的条款和条件。 ***CSIRT（网络安全事故响应小组）*** Nemak 网络安全事故响应小组。 ***信息*** Nemak 或其业务、客户、供应商或任何第三方持有的以及以任何方式与之相关的所有机密和专有信息。 ***审计*** 定期审查供应商的业绩和对协议的遵守情况。 ***供应商*** 向 Nemak 提供产品和/或服务的任何自然人或法人实体。 ***基础设施平台和服务*** Nemak 的系统、应用程序和/或网络元素及数据库。 ***物质资源*** 仅用于提供服务或供应产品的硬件或物理设备（如电脑、打印机、服务器、显示器、移动设备、可移动存储介质等）。

	逻辑资源 仅为提供服务或供应产品而允许访问的软件、系统或应用程序。 ***服务级协议*** 服务水平协议
角色与责任	***尼马克*** 向第三方传达 Nemak 的适当规定和措施 ***供应商：*** 确保符合信息安全要求
一般要求	• 供应商应采取一切必要措施，保护其可以访问的任何信息，包括Nemak基础设施的平台和服务，无论这些信息是来自提供服务或供应产品，还是由于任何其他原因，供应商需要访问Nemak的信息、平台和/或基础设施服务。 • 供应商应遵守并促使任何分包商遵守此处规定的安全准则，并应保留证明其遵守的证据。 • 即使 Nemak 和供应商修改了服务范围，也要始终遵守这些安全指南。 • 签署 Nemak 的《供应商全球商业准则》，不言而喻，只有那些与将要提供的服务相关的安全准则才适用于供应商。
保密性	• 供应商承认，Nemak 披露的、供应商、其员工或分包商人员已经和/或将要接触到的信息是 Nemak、其客户、供应商和/或第三方的财产，并受保密承诺的保护。 • 供应商应制定政策、程序和控制措施，以防止接触信息的员工或分包商未经授权披露信息。 • 仅允许供应商的员工和/或分包商人员在需要知情的基础上访问信息以及基础设施平台和服务，且仅限于与提供服务或供应产品有关的访问。 • 供应商声明并保证，个人数据或机密信息只能用于商业目的，并严格遵守双方之间的任何协议以及任何 Nemak 政策和适用法律。 • 供应商应签署一份或多份保密协议，以确保其有权访问的信息的保密性。 • 供应商应采取积极措施，正确保护为提供产品和/或服务而披露给其的个人数据或机密信息。
实体安全	• 供应商应确保个人数据和机密信息仅由授权人员在需要知情的基础上访问。 • 供应商应采取必要措施保护自身设施、IT 设备和基础设施。 • 供应商和/或分包商人员应始终遵守 Nemak 的实体安全政策和程序。

供应商人员	• 供应商人员应避免 Nemak 的《全球供应商商业准则》中规定的任何利益冲突。 • 供应商应负责其员工具备提供服务所需的能力和/或认证，并在协议期内保持这一水平。员工的能力和/或认证必须能够证明并令 Nemak 满意。 • 供应商应将本文件的内容书面通知其员工。如有需要，Nemak 可要求供应商书面确认已将本文件内容告知其员工，且供应商应确保其员工或任何分包商员工严格遵守和遵守本文件。
信息技术基础设施可接受使用政策	• 供应商应始终妥善使用 Nemak 提供的物理和逻辑资源

逻辑访问控制	• 供应商的员工和/或分包人员必须接受信息安全要求。如审计或出于其他目的需要，应提供接受上述条款和条件的证据。
	• 供应商同意根据以下标准制定其自有基础设施系统的密码政策：
	  ○ 最小长度为 10 个字符，3 个字符组（小写、大写、数字）中每个组至少有一个字符。
	  ○ 系统配置应要求至少每 12 个月更改一次密码，或者一旦有迹象表明密码以任何方式泄露，或者怀疑第三方可能知道密码，就立即更改密码。
	• 服务或合同终止时，供应商应禁用或取消员工或第三方使用供应商 IT 基础设施的账户。
	• 如果 Nemak 提供账户和密码以连接 Nemak 的系统，则不得向任何第三方或供应商的非服务提供或产品供应人员披露和/或共享这些账户和密码。对于Nemak授予的个人账户，不得在员工之间披露和/或共享，即使他们是提供服务或供应产品的一部分。
	• 供应商应对使用 Nemak 提供给供应商人员的账户和密码进行的任何活动负责。
	• Nemak 将在以下情况下终止供应商对信息的访问
	  ○ 目的已经达到。
	  ○ 供应商违反本《安全指南》。
	  ○ 发现任何可疑活动。
	  ○ 当 Nemak 认为方便时。
	• 如果 Nemak 向供应商或供应商分包的第三方提供用户账户（例如活动目录账户、VPN 访问、电子邮件等），供应商必须立即通知 Nemak 以下任何情况：
	  ○ 雇员或分包第三方被解雇或不再与供应商有合同关系。
	  ○ 雇员或分包第三方不再为 Nemak 提供服务。

通知必须发送给 Nemak 的供应商联络经理和 Nemak 的信息安全：isec.suppliers@nemak.com。

IT 基础设施管理

网络接入

- 供应商的网络应受防火墙保护，且只能由供应商的人员访问。
- 供应商的人员应使用活动目录用户连接网络。

安全擦除

- 在终止与 Nemak 的业务关系时，或在 Nemak 提出要求时（以先发生者为准），供应商应使用信息安全删除功能，以确保正确删除（或归还信息（如适用））。

反恶意软件保护

- 供应商应使用制造商提供的最新反恶意软件版本和更新维护用于提供服务或供应产品的产品和设备。 计算机设备中的防火墙必须启用，以阻止任何恶意软件尝试。

漏洞管理

- 供应商应扫描 IT 基础设施内的漏洞，以检测、通知和补救在提供服务或供应产品时发现的漏洞，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。
- 如果出现任何漏洞，供应商应实施补救计划。

系统修补

- 供应商应确保服务器、用户 PC 和移动设备在补丁发布后最多 60 天内打上补丁。

删除 VPN 访问

- 供应商同意使用 VPN 连接其设施，但只能使用 Active Directory 身份验证，不得使用其他连接选项。如有可能，供应商应在 VPN 中使用多因素身份验证。
- 个人之间不得共享 VPN 访问权限。

云服务的使用

对于云服务提供商，供应商同意包含以下条款，以保护 Nemak 的数据和服务的可用性：

- 在云服务环境中发生信息安全事故时提供专门支持。
- 支持组织收集数字证据，同时考虑到不同司法管辖区的数字证据法律法规。
- 提供所需的数据和配置信息备份，并视情况对备份进行安全管理。
- 在提供服务期间或服务终止时，应要求提供并返还组织所拥有的配置文件、源代码、日志和数据等信息。

	云服务提供商必须始终发出通知： • 影响或改变云服务产品的技术基础设施变更（如硬件或软件的搬迁、重新配置或变更）。 • 在新的地理或法律管辖区处理或存储信息。 • 使用同行云服务提供商或其他分包商（包括更换现有方或使用新方）。
信息安全意识	• 供应商应（在其员工中）实施有关信息安全的意识和学习计划，采取预防措施，并实施有关如何对信息进行分类和管理的政策、程序和控制措施。 • 供应商必须每年至少为其员工提供一次基本的安全培训，确保他们了解以下内容： ○ 网络钓鱼风险 ○ 妥善保管密码 ○ 使用高强度密码 ○ 社会工程学 ○ 社交媒体
网络安全风险和事件管理	• 供应商应识别网络安全风险，并采取适当行动防止任何安全事故。 • 如果供应商卷入影响 Nemak 的安全事件，供应商应与 CSIRT 协调，共同努力恢复正常运营。 • 供应商应立即通知 Nemak 任何实际或潜在的网络安全事件和数据泄露。
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 ○ 审核供应商的表现和遵守本《安全指南》的情况。 ○ 要求获得第三方的报告/证书，以验证与提供服务或供应产品相关的控制措施是否合规。
合规性	• 供应商应妥善使用 Nemak 和第三方的任何知识产权和版权。 • 供应商应就违反本《安全指南》中规定的任何责任向 Nemak 承担责任。 • 如果供应商或其任何分包人员未能遵守本安全指南，则可能会受到协议和适用法律规定的处罚。 • 如果因违反本安全指南而引起任何索赔，供应商同意对 Nemak 进行赔偿、为其辩护并使其免受损害。

- 本安全指南可随时更新。只要供应商与 Nemak 保持业务关系，就应遵守本《安全指南》。

联系信息 如果您对本准则有任何疑问或意见，可通过 isec.suppliers@nemak.com 与 Nemak 信息安全部门联系。

修订

版本	日期	请求者	变更说明
1.0	2022 年 7 月	里卡多-塞拉诺	制定准则
2.0	2022 年 8 月	埃德温-马西亚斯	文件格式改为准则
3.0	2023 年 3 月	埃德温-马西亚斯	更改了*逻辑访问控制*部分： 重新定义了与供应商或分包第三方服务终止有关的文本。
4.0	2024 年 1 月	奥马尔-杜兰	添加 "*使用云服务* "部分

本文件沿用了《文件管理流程》中描述的一般文件管理流程：

NPO-GBL-SEC-10 文件管理政策

批准人

版本	日期	批准人姓名
1.0	2022 年 7 月	埃德温-马西亚斯
2.0	2022 年 8 月	亚历杭德罗-巴尔德斯-弗洛雷斯
3.0	2023 年 3 月	亚历杭德罗-巴尔德斯-弗洛雷斯
4.0	2024 年 1 月	埃德温-马西亚斯

本文件使用翻译工具创建

Tedarikçiler için Bilgi Güvenliği Gereklilikleri

Ocak 2024

Giriş ve Amaç

Bu kılavuz, müşterinin tüm Tedarikçileri (bundan böyle "Nemak" olarak anılacaktır) tarafından uyulması gereken bilgi güvenliği gereksinimlerini (bundan böyle "Güvenlik Kılavuzları" olarak anılacaktır) ortaya koymaktadır.

Bu Güvenlik Yönergelerinin amacı, her türlü Bilgiyi korumaktır. Güvenlik Yönergeleri, Nemak ile Tedarikçi arasında yapılan herhangi bir anlaşmanın ayrılmaz bir parçasını oluşturur ve Tedarikçi, Bilgilerin gizliliğini ve bütünlüğünü korumak için bunlara uyacaktır. Bu gereklilikler, diğer güvenlik gereklilikleri, herhangi bir hizmet seviyesi anlaşması veya Nemak ile Tedarikçi arasında mutabık kalınan diğer herhangi bir belge vasıtasıyla tamamlanabilir.

Kapsam

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

İstisnalar

Bir güvenlik gerekliliğine uymanın mümkün olmaması durumunda, ilgili değerlendirme için Nemak'a aşağıdaki e-posta adresinden bildirilmelidir: isec.suppliers@nemak.com

Amaç

Nemak tarafından ifşa edilen Bilgilerin korunması için uyması gereken tüm Güvenlik Yönergeleri hakkında Tedarikçiyi bilgilendirmek.

Tanımlar

Nemak
Nemak, S.A.B. de C.V. ve bağlı ortaklıkları.

Anlaşma
Ürünlerin ve/veya hizmetlerin Nemak'a tedarik edileceği ve/veya sunulacağı hüküm ve koşulları belirleyen herhangi bir anlaşma, satın alma siparişi, adaylık mektubu veya diğer belge.

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

Bilgi
Nemak veya işletmeleri, müşterileri, tedarikçileri veya herhangi bir üçüncü şahıs tarafından tutulan ve bunlarla herhangi bir şekilde ilgili olan tüm gizli ve tescilli bilgiler.

Denetim
Tedarikçinin performansının ve herhangi bir Sözleşmeye 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 elemanları ve veritabanları.

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

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

SLA
Hizmet Seviyesi Anlaşması

Roller ve Sorumluluklar	***Nemak:*** Nemak'ın uygun düzenlemelerini ve önlemlerini üçüncü taraflara iletmek ***Tedarikçi:*** Bilgi güvenliği gereksinimlerinin uyumluluğunu sağlamak
Genel Gereklilikler	• Tedarikçi, Nemak Altyapısının Platformları ve Hizmetleri de dahil olmak üzere, ister hizmetlerin sağlanmasından veya ürünlerin tedarikinden kaynaklansın isterse de Tedarikçinin Nemak'ın Bilgilerine, Platformuna ve/veya Altyapı Hizmetlerine erişmesini gerektiren başka herhangi bir nedenden kaynaklansın, erişebildiği her türlü Bilgiyi korumak için gerekli tüm önlemleri alacaktır. • Tedarikçi, burada belirtilen Güvenlik Yönergelerine uyacak ve tüm alt yüklenicilerin uymasını sağlayacak ve bu uyumu gösteren kanıtları muhafaza edecektir. • Hizmetlerin kapsamı Nemak ve Tedarikçi tarafından değiştirilmiş olsa bile, her zaman bu Güvenlik Yönergelerine uyun. • Nemak'ın Tedarikçiler için Küresel İş Kurallarını imzalayın, sadece sunulacak hizmetlerle ilgili olan Güvenlik Kurallarının Tedarikçi için geçerli olacağı anlaşılmaktadır.
Gizlilik	• Tedarikçi, Nemak tarafından açıklanan ve Tedarikçinin, çalışanlarının veya taşeron personelinin eriştiği ve/veya erişeceği Bilgilerin Nemak'ın, müşterilerinin, tedarikçilerinin ve/veya üçüncü tarafların mülkiyetinde olduğunu ve gizlilik taahhütleri ile korunduğunu kabul eder. • Tedarikçi, Bilgiye erişimi olan çalışanlar veya alt sözleşmeli personel tarafından Bilginin yetkisiz ifşasını önlemek için politikalar, prosedürler ve kontroller oluşturacaktır. • Bilgiye ve Altyapı Platformuna ve Hizmetlerine erişim, yalnızca Tedarikçi tarafından taşeron olarak görevlendirilen çalışanlara ve/veya personele bilmesi gerekenler temelinde ve yalnızca hizmetlerin sağlanması veya ürünlerin tedariki ile ilgili olarak verilecektir. • Tedarikçi, kişisel verilerin veya gizli bilgilerin yalnızca iş amaçları için ve taraflar arasındaki herhangi bir Anlaşmanın yanı sıra Nemak politikaları ve yürürlükteki yasalarla sıkı bir uyum içinde kullanılabileceğini beyan ve garanti eder. • Tedarikçi, bir veya birden fazla gizlilik anlaşması imzalayarak erişebildiği Bilgilerin gizliliğini sağlayacaktır. • Tedarikçi, ürün ve/veya hizmet 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 yetkili personel tarafından bilmesi gerekenler temelinde erişilmesini sağlayacaktır. • Tedarikçi, kendi tesislerini ve BT ekipmanlarını ve altyapısını korumak için gerekli önlemleri alacaktır. • Tedarikçi ve/veya taşeron personeli Nemak'ın Fiziksel Güvenlik politika ve prosedürlerine her zaman uyacaktır.
Tedarikçi Personeli	• Tedarikçi personeli, Nemak'ın Tedarikçiler için Küresel İş Kurallarında belirtildiği gibi çıkar çatışmalarından kaçınacaktır. • Tedarikçi, personelinin hizmetlerin sağlanması için yetkin ve/veya sertifikalı olmasından ve Sözleşme süresi boyunca bu seviyeyi korumasından sorumlu olacaktır. Personelin yetkinliği ve/veya sertifikasyonu Nemak'ı tatmin edecek şekilde kanıtlanabilmelidir.

	• Tedarikçi, personelini bu belgenin içeriği hakkında yazılı olarak bilgilendirecektir. Nemak, ihtiyaç duyması halinde Tedarikçiden, personelini bu belgenin içeriği hakkında bilgilendirdiğini yazılı olarak teyit etmesini talep edebilir ve Tedarikçi, personelinin veya herhangi bir taşeron personelinin bu belgeye sıkı sıkıya bağlı kalmasını ve uymasını sağlayacaktır.
BT Altyapısı Kabul Edilebilir Kullanım Politikası	• Tedarikçi, Nemak tarafından sağlanan Fiziksel ve Mantıksal Kaynakları her zaman iyi bir şekilde kullanacaktır
Mantıksal Erişim Kontrolü	• Tedarikçi tarafından taşeron olarak görevlendirilen çalışanlar ve/veya personel Bilgi Güvenliği gerekliliklerini kabul etmelidir. Bu şart ve koşulların kabul edildiğine dair kanıtlar, herhangi bir denetim veya başka bir amaç için gerekli olması halinde mevcut olacaktır. • Tedarikçi, kendi altyapı sistemlerindeki şifreler için aşağıdaki kriterlere sahip bir politikaya sahip olmayı kabul eder: ○ Minimum 10 karakter uzunluğunda, 3 karakterli grupların (küçük harf, büyük harf, rakam) her birinden en az bir karakter olacak şekilde. ○ Sistemler en az 12 ayda bir veya şifrenin herhangi bir şekilde ele geçirildiğine dair en ufak bir belirti varsa ya da üçüncü bir tarafın şifreyi bildiğine dair şüphe varsa derhal şifre değişikliği gerektirecek şekilde yapılandırılmalıdır. • Hizmetlerin veya sözleşmenin feshedilmesi üzerine Tedarikçi, Tedarikçi'nin BT Altyapısını kullanmak için çalışan veya üçüncü taraf hesaplarını devre dışı bırakacak veya ortadan kaldıracaktır. • Nemak, Nemak'ın sistemlerine bağlanmak için hesaplar ve şifreler sağlarsa, bunlar herhangi bir üçüncü tarafla veya hizmetlerin sağlanmasının veya ürünlerin tedarikinin bir parçası olmayan Tedarikçi personeli ile ifşa edilmemeli ve/veya paylaşılmamalıdır. Nemak tarafından verilen bireyselleştirilmiş hesaplar için, hizmetlerin sağlanmasının veya ürünlerin tedarikinin bir parçası olsalar bile personel arasında ifşa edilmemeli ve/veya paylaşılmamalıdır. • Nemak tarafından Tedarikçi personeline sağlanan hesaplar ve şifreler ile gerçekleştirilen her türlü faaliyetten Tedarikçi sorumlu olacaktır. • Nemak, aşağıdaki durumlarda Tedarikçinin Bilgilere erişimini sonlandıracaktır: ○ Amaç yerine getirilmiştir. ○ Tedarikçi tarafından bu Güvenlik Yönergelerinin ihlal edilmesi. ○ Herhangi bir şüpheli faaliyet tespit edilir. ○ Nemak uygun gördüğünde. • Nemak'ın Tedarikçi'ye veya Tedarikçi'nin alt yüklenicisi olan üçüncü taraflara kullanıcı hesapları (örn. Active Directory hesapları, VPN erişimi, E-posta vb.) sağlaması durumunda, Tedarikçi aşağıdakilerden herhangi birinin geçerli olması halinde derhal Nemak'a bildirimde bulunmalıdır: ○ Çalışanın veya taşeron üçüncü tarafın iş akdinin feshedilmesi veya artık Tedarikçi ile sözleşmeye dayalı bir ilişkisinin kalmaması. ○ Çalışan veya taşeron üçüncü taraf artık Nemak'a hizmet vermemektedir. Bildirimler Nemak'ın Tedarikçi irtibat yöneticisine ve Nemak'ın Bilgi Güvenliğine gönderilmelidir: isec.suppliers@nemak.com

BT Altyapı Yönetimi	*Ağ Erişimi* • Tedarikçi ağı güvenlik duvarları ile korunacak ve sadece Tedarikçi personeli tarafından erişilebilecektir. • Tedarikçi personeli ağa bağlanmak için bir aktif dizin kullanıcısı kullanacaktır. *Güvenli Silme* • Nemak ile iş ilişkisinin sona ermesi üzerine veya Nemak tarafından talep edildiğinde, hangisi önce gerçekleşirse, Tedarikçi, Bilgilerin uygun şekilde silinmesini (veya varsa iade edilmesini) sağlamak için güvenli bilgi silme yöntemini uygulayacaktır. *Antimalware Koruması* • Tedarikçi, hizmetlerin sağlanması veya ürünlerin tedariki için kullanılan ürün ve ekipmanların bakımını, üretici tarafından sağlanan en son antimalware sürümleri ve güncellemeleri ile yapacaktır. Bilgisayar ekipmanındaki güvenlik duvarı, herhangi bir kötü amaçlı yazılım girişimini engellemek için etkinleştirilmelidir. *Güvenlik Açığı Yönetimi* • Tedarikçi, hizmetlerin sağlanmasında veya ürünlerin tedarikinde ve ayrıca Tedarikçinin hizmetlerin sağlanması veya ürünlerin tedariki için kullanılan ekipmanında bulunan güvenlik açıklarını tespit etmek, bildirmek ve gidermek için BT Altyapısı içindeki güvenlik açıklarını tarayacaktır. • Tedarikçi, herhangi bir güvenlik açığı durumunda bir iyileştirme planı uygulayacaktır. *Sistem Yaması* • Tedarikçi, sunucuların, kullanıcı bilgisayarlarının ve mobil cihazların yama yayınlandıktan sonra en fazla 60 gün içinde yamalanmasını sağlayacaktır. *VPN Erişimini Kaldır* • Tedarikçi, tesislerine bağlanmak için VPN'i yalnızca Active Directory kimlik doğrulaması ile kullanmayı ve başka hiçbir bağlantı seçeneği kullanmamayı kabul eder. Mümkünse Tedarikçi VPN ile Çok Faktörlü Kimlik Doğrulama kullanacaktır. • VPN erişimi kişiler arasında paylaşılmayacaktır.
Bulut Hizmetlerinin Kullanımı	Bulut hizmet sağlayıcıları durumunda Tedarikçi, Nemak'ın verilerinin korunması ve hizmetlerin kullanılabilirliği için aşağıdaki hükümleri içermeyi kabul eder: • Bulut hizmeti ortamında bir bilgi güvenliği olayı olması durumunda özel destek sağlayın. • Farklı yargı alanlarındaki dijital kanıtlara ilişkin yasa ve yönetmelikleri dikkate alarak dijital kanıt toplama konusunda kuruma destek olun. • Gerekli veri ve yapılandırma bilgilerinin yedeklenmesini sağlamak ve uygun şekilde yedekleri güvenli bir şekilde yönetmek. • Hizmet sunumu sırasında veya hizmetin sonlandırılması sırasında talep edildiğinde, kuruluşun sahip olduğu yapılandırma dosyaları, kaynak kodu, günlükler ve veriler gibi bilgileri sağlamak ve iade etmek. Bulut hizmeti sağlayıcısı her zaman bildirimde bulunmalıdır:

	• Bulut hizmeti teklifini etkileyen veya değiştiren teknik altyapı değişiklikleri (örn. yer değiştirme, yeniden yapılandırma veya donanım ya da yazılım değişiklikleri). • Bilgilerin yeni bir coğrafi veya yasal yetki alanında işlenmesi veya saklanması. • 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 nasıl sınıflandırılacağı ve yönetileceğine ilişkin politikaların, prosedürlerin ve kontrollerin uygulanması konusunda (çalışanları arasında) farkındalık ve öğrenme programları uygulayacaktır. • Tedarikçi, çalışanlarına yılda en az bir kez temel güvenlik eğitimi vermeli ve çalışanlarının aşağıdakilerin farkında olmalarını sağlamalıdır: ○ Kimlik avı riskleri ○ Şifrelerini güvende tutmak ○ Güçlü parolaların kullanımı ○ Sosyal mühendislik ○ Sosyal medya
Siber Güvenlik Riskleri ve Olay Yönetimi	• Tedarikçi, siber güvenlik risklerini belirleyecek ve herhangi bir güvenlik olayını önlemeye yönelik uygun önlemleri alacaktır. • Tedarikçinin Nemak'ı etkileyen bir Güvenlik Olayına karışması durumunda, Tedarikçi, CSIRT ile koordineli olarak normal operasyonlara dönmek için birlikte çalışacaktır. • Tedarikçi, herhangi bir fiili veya potansiyel siber güvenlik olayını ve veri ihlalini derhal Nemak'a bildirecektir.
İş Sürekliliği	• Tedarikçi, kritik sistemler için iş sürekliliği planları geliştirecektir. Bu planlar, yılda en az bir kez test edilen felaket kurtarma prosedürlerini içerecek ancak bunlarla sınırlı olmayacaktır.
Denetim	• Nemak şu haklara sahip olacaktır: ○ Tedarikçinin performansını ve bu Güvenlik Yönergelerine uygunluğunu denetlemek. ○ Hizmetlerin sağlanması veya ürünlerin tedariki ile bağlantılı kontrollere uygunluğu doğrulayan üçüncü tarafların raporlarına/sertifikalarına erişim talep etme.
Uyumluluk	• Tedarikçi, Nemak'ın ve üçüncü şahısların Fikri Mülkiyet Haklarını ve Telif Haklarını iyi bir şekilde kullanacaktır. • Tedarikçi, bu Güvenlik Kılavuzunda belirtilen sorumluluklarını ihlal etmesi durumunda Nemak'a karşı sorumlu olacaktır. • Tedarikçi veya alt sözleşmeli personelinin bu Güvenlik Yönergelerine uymaması, Sözleşmede ve yürürlükteki yasalarda belirtilen cezalara neden olabilir. • Tedarikçi, bu Güvenlik Yönergelerinin ihlalinden kaynaklanan herhangi bir talep durumunda Nemak'ı tazmin etmeyi, savunmayı ve zararsız tutmayı kabul eder. • Bu Güvenlik Yönergeleri zaman zaman güncellenebilir. Tedarikçi, Nemak ile iş ilişkisini sürdürdüğü sürece bu Güvenlik Yönergelerine uyacaktır.
İletişim Bilgileri	Bu kılavuzla ilgili sorularınız veya yorumlarınız varsa, sorunuzla birlikte isec.suppliers@nemak.com adresinden Nemak Bilgi Güvenliği ile iletişime geçebilirsiniz.

Revizyonlar

Versiyon	Tarih	Talep Sahibi	Değişikliklerin Açıklaması
1.0	Temmuz/2022	Ricardo Serrano	Kılavuzun oluşturulması
2.0	Ağustos/2022	Edwin Macias	Belge formatı kılavuz olarak değiştirildi
3.0	Mart/2023	Edwin Macias	*Mantıksal Erişim Kontrolü* bölümü değiştirildi: Tedarikçi veya Taşeron Üçüncü Tarafların hizmetlerinin sona ermesine ilişkin metin yeniden tanımlanmıştır.
4.0	Ocak/2024	Omar Duran	*Bulut Hizmetlerinin Kullanımı* bölümü eklendi

Bu belge, aşağıda açıklanan genel belge yönetimi sürecini takip eder:

NPO-GBL-SEC-10 Belge Yönetimi Politikası

Tarafından onaylandı

Versiyon	Tarih	Onaylayanın Adı
1.0	Temmuz/2022	Edwin Macias
2.0	Ağustos/2022	Alejandro Valdes Flores
3.0	Mart/2023	Alejandro Valdes Flores
4.0	Ocak/2024	Edwin Macias

Bu belge bir çevirmen aracı kullanılarak oluşturulmuştur