Information Security Requirements for Suppliers

August 2022

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.

ERT
Nemak Emergency 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 to Supplier and the access is no longer needed, Supplier must immediately notify Nemak's contact person in order to take appropriate action.

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.
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 Nemak's Emergency Response Team (ERT), 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.

Document History

Version	Date	Name	Short Description of Changes
1.0	July/2022	Ricardo Serrano	Creation of guideline
2.0	August/2022	Edwin Macias	Document format changed to guideline

This document follows the general document management process described in:

NPO-GBL-SEC-10 Document Management Policy

Document Approval

Version	Date	Name of Approver
1.0	July/2022	Edwin Macias
2.0	August/2022	Alejandro Valdes Flores