Document Classification: Public		Issue Date: April 30, 2021

Supplier Cyber Security & Operations (CSE)

Expectations Manual

Mondelēz International

Version 2021 v.1

About

Where permitted by law and subject to local requirements, this document is referenced within contractual agreements between Mondelēz International (including affiliates) and those that provide Goods and/or Services (Suppliers). Suppliers are required to comply with applicable sections within this manual as indicated by MDLZ in such contracts. If no sections are omitted or noted as "not applicable" then all apply.

Issued by:	Approved by:
Information Risk Management Global Lead	Chief Information Security Officer (CISO)

Table of Contents

INTRODUCTION

The cyber security of our critical information systems and data is of high importance to us at Mondelēz International (MDLZ). We recognize that protecting our information systems is critical to continued operation and to comply with laws and regulations. We are committed to delivering high quality products to our consumers. One of the ways we achieve this is by ensuring the strength of our information systems security and third-party supply chain. We expect that our suppliers share this commitment and will protect our data as well so for that purpose we are making this document available to you here in hard copy and online at the Mondelēz International Supplier Portal web site at **https://www.mondelezinternational.com/procurement** or from your MDLZ Contracting Representative.

The English version of this document is considered the official version, but alternative languages may be available. The Supplier Cyber Security & Operations Expectations (CSE) outlined here are intended to help current and prospective new suppliers of information systems ensure that their own information systems meet MDLZ's and industry standards. These expectations have been developed by MDLZ and subject matter experts following a review of industry best practices, internationally recognized standards and effective frameworks. This review has led us to identify which policies and standards, if implemented properly, help to prevent a loss of confidentiality, integrity, availability of critical systems, data breaches and malware related incidents.

Each supplier processing electronic information for Mondelēz International must meet the applicable expectations in this manual.

This MDLZ CSE Manual, contains the elements we believe are essential for the effective management of Cyber Security. They are not intended to alter or eliminate any requirements that may be set in any contract, specifications, or government regulation. Any questions about these standards should be addressed by contacting the appropriate MDLZ Contracting Representative.

The terms used to designate requirements and recommendations stated in this document include:

• Shall, Will and Must - Mandatory with no exclusions.

• Should – Used to express a strong recommendation among other possible options.

• May – Used to indicate an action which is permissible, but not mandatory.

As a supplier you are responsible for ensuring that the requirements of the Cyber Security & Operations Expectations Manual are met AND are extended to any sub processor(s).

**** IMPORTANT ****

Not all security requirements within the CSE Manual may apply. Consult with your Mondelēz International Contracting Representative and agreements if not clear.

1. Access security and privacy

Supplier must:

- Allow access to MDLZ Data only to Supplier personnel who have a need to access it in order to perform obligations under this agreement.
- Use access control methods (including use of user id and strong passwords, auditing and logging, and information security change control procedures) for any system or device that could allow access to the MDLZ Data.
- At least annually, obtain and provide to MDLZ a current SSAE18 SOC 2 Type 2 report and an ISO 27001 certification (plus an ISO statement of applicability (SOA)) on its data security practices (or, if Supplier cannot obtain an SSAE18 SOC 2 Type 2 report or ISO 27001 certification, an alternative report that conforms to ISAE 3402 standards) from a recognized provider of such reports. Supplier may also be required to provide upon MDLZ's reasonable request a written summary of applicable practices described in this manual.
- Use appropriate technical and organizational measures in accordance with industry practices and the sensitivity of the information (including any Personal Information) to secure MDLZ Data and systems to which Supplier has access. Supplier shall comply with any specific data processing and handling requirements reasonably requested by MDLZ or determined by applicable laws and regulations.
- Encrypt all transmissions and storage of MDLZ Data and implement multifactor authentication for remote access when access relates to privileged access or any access to confidential data. Supplier will deploy virtual private network (VPN) or virtualized desktops (Citrix) to provide secure remote network connections.

1.1 Supplier acknowledges that in collecting, receiving, or accessing MDLZ Personal Information, including information about MDLZ's consumers, customers, suppliers, business partners, contractors or employees, Supplier shall comply with all applicable Privacy Laws, and MDLZ privacy policies. Supplier shall stay informed of possible changes to Privacy Laws and MDLZ privacy policies throughout the course of the agreement. Supplier shall not cause MDLZ to be in violation of any Privacy Laws or privacy policies.

1.2 Supplier shall execute any necessary agreements and acquire all necessary permits and authorizations pertaining to processing and handling of MDLZ Data from relevant regulatory authorities. Supplier shall only process or otherwise use MDLZ Personal Information to the extent necessary to provide the Services described in the agreement and as instructed by MDLZ, for the sole benefit of MDLZ (unless differently agreed in writing between Supplier and MDLZ) and in a manner consistent with this agreement. Without limiting the foregoing, Supplier shall not (i) sell any MDLZ Personal Information; (ii) collect, retain, use, disclose, or otherwise process MDLZ Personal Information: (a) for any purpose other than for the specific purpose of performing the Services and as set forth in this agreement and to the extent reasonably necessary; (b) outside of the direct business relationship between MDLZ and Supplier (unless differently agreed in writing between Supplier and MDLZ); and (c) if prohibited by applicable law, Supplier will not use such Personal Information for its own purposes or commercial interests (unless differently agreed in writing between Supplier and MDLZ) and represents, warrants and certifies that it understands and will comply with the restrictions set forth in this section and the entire agreement. The parties intend and agree that Supplier is a Service Provider, as defined under applicable Privacy Laws.

1.3 Supplier must provide MDLZ with reasonable advance notice in writing of any planned changes to the hosting location of MDLZ Data, or other security policies, standards, and practices related to MDLZ Data. If MDLZ determines that Supplier's changed policies, standards, or practices do not conform with MDLZ's then-current security policies, standards, and practices, Supplier shall take the actions MDLZ reasonably requests to ensure its policies, standards, and practices conform to MDLZ's policies or MDLZ may terminate the agreement on a no fault basis.

1.4 Supplier acknowledges that all MDLZ Data shall at all times remain the property of MDLZ and Supplier shall acquire no rights or interests in them.

1.5 Supplier must cooperate with MDLZ if a person makes a lawful request for: (i) access to his or her Personal Information; (ii) information about the categories of sources from which the Personal Information is collected; (iii) information about the categories or specific pieces of the individual's Personal Information, including by providing the requested information in a portable and, to the extent technically feasible, readily useable format that allows the individual to transmit the information to another entity without hindrance; or (iv) any other right the person has regarding his or her Personal Information under applicable Privacy Laws. Supplier shall promptly inform MDLZ in writing of any requests with respect to MDLZ Personal Information.

1.6 Upon MDLZ's request, Supplier must promptly delete a particular individual's Personal Information from Supplier's records. In the event Supplier is unable to delete the Personal Information of a particular individual for reasons permitted under applicable law, Supplier shall: (i) promptly inform MDLZ of the reason(s) for its refusal of the deletion request; (ii) ensure the privacy, confidentiality and security of such Personal Information; and (iii) delete the Personal Information promptly after the reason(s) for Supplier's refusal has expired.

1.7 Supplier must notify MDLZ in writing immediately, but in no event later than within twenty-four (24) hours of (i) actual or suspected Data Breaches (defined below); (ii) any unauthorized access to MDLZ Data or systems or any vulnerability that carries a risk of compromising MDLZ Data or systems or (iii) any possible violations of applicable data protection laws. Incidents shall be reported to the primary MDLZ contact in addition to the MDLZ Cyber Security Operations Center Cybersecurity@mdlz.com Supplier shall promptly at its own expense take actions (including any actions MDLZ reasonably requests) to comply with applicable laws and regulations governing Data Breaches and related matters. Supplier shall be responsible for any costs, fines, penalties, or other losses that MDLZ incurs as a result of any Data Breach arising from Supplier's negligence (act or omission) or breach of its obligations under this CSE and or its agreement with MDLZ.

1.8 Supplier shall retain MDLZ Data only for as long as required to perform its obligations under this agreement, except where (i) another retention period is strictly required by applicable law; or (ii) MDLZ asks Supplier in writing to retain certain MDLZ Data because of pending or anticipated litigation, investigation, audit or other purposes. At the termination of this agreement, Supplier shall, at MDLZ's option, return to MDLZ or securely destroy (such that no content is recoverable) all MDLZ Data. If MDLZ does not exercise this option within 30 days of the termination or expiry of this agreement, Supplier must provide 60 days' advance written notice to MDLZ and then proceed to permanently dispose of or destroy the MDLZ Data in a manner that prevents content recovery. If requested by MDLZ, Supplier shall provide a certificate to MDLZ attesting to its proper deletion or destruction of MDLZ Data.

2. Asset management

Supplier must:

- Maintain an updated inventory of systems and entities that process MDLZ Data including Personally Identifiable Information.
- In accordance with applicable legal requirements, protect MDLZ Data in both hardcopy and digital form by limiting access to authorized users and utilize methods of sanitizing or destroying media so that data recovery is technically infeasible.

3. Business continuity and IT disaster recovery

Supplier must:

- Implement a business continuity plan to ensure continued business operations in the event of a crisis.
- Maintain and periodically test a disaster recovery (DR) plan which provides for system backup, technology replacement, and alternate (recovery) site capabilities.
- Provide documentation of its DR solution annually or at other agreed frequency and share test results. If Supplier does not test DR plan, then Supplier needs to support MDLZ testing as mutually agreed.
- Implement mechanisms to control resource utilization of systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.

4. Network security

Supplier must:

- Maintain a firewall and network security settings to protect and segregate private and public networks from unauthorized use.
- Encrypt all transmissions and storage of MDLZ Data.
- Configure all mobile devices and portable media (including laptops, smartphones, tablets, storage devices, and wearable devices) to protect information against loss, theft, and unauthorized disclosure of MDLZ Data.
- Prevent user access to known malicious websites that pose a security risk.

5. Physical and environmental security

Supplier must:

- Maintain physical security and access controls for all of Supplier's data center(s) and facilities.
- Protect critical facilities against fire, flood, environmental and other natural hazards.

6. Secure software

Supplier must:

- Perform regular (at least annual) penetration testing using industry accepted methodologies. For example, OWASP Testing methodology or equivalent.
- Conduct quarterly vulnerability assessment using independent organization utilizing industry standard assessment methodologies, good practices including at a minimum NIST Cybersecurity framework, OWASP standard or equivalent good practice.
- Mitigate/remediate vulnerabilities identified during penetration testing and vulnerability assessment in accordance with Suppliers procedures to eliminate vulnerabilities and remove flaws that could otherwise facilitate security breaches. Mitigation may include deployment of security and maintenance patches (software and firmware) or other measures to reduce risk. Upon MDLZ request, Supplier shall provide evidence to demonstrate compliance. Supplier maybe subject to MDLZ provided vulnerability remediation standards.
- Follow secure software development methodologies as part of its software development lifecycle process.
- Ensure that the development community undergo regular software security/application security awareness training.

7. Supply chain risk management

Supplier shall provide MDLZ with reasonable advance notice in writing of any planned changes to the hosting location of MDLZ Data, or other security policies, standards, and practices that weaken or lessen security related to MDLZ Data. If MDLZ determines that Supplier's changed policies, standards, or practices do not conform with MDLZ's then-current security policies, standards, and practices, Supplier shall take the actions MDLZ reasonably requests to ensure its policies, standards, and practices conform to MDLZ's policies or MDLZ may terminate the agreement with Supplier on a no fault basis. Any such additional requests will be agreed upon by the parties in writing in accordance with contract change management procedures.

Supplier shall not subcontract any data processing operations under this agreement or otherwise provide a third party with access to MDLZ Data without MDLZ prior written consent. When MDLZ has provided such consent, Supplier shall take all reasonable steps to ensure the reliability of such third parties, and shall require their compliance with this agreement (and, if MDLZ requires, or if required by Privacy Laws, they will execute a separate confidentiality or other agreement with protections similar to those in this agreement). Supplier shall be responsible for any noncompliance of a third party, and this noncompliance will constitute a breach of this agreement as if committed directly by Supplier.

8. Cloud assurance

If Supplier wishes to sub-contract and/or assign any of Supplier's obligations associated with storing, processing or transmitting MDLZ Data to a third party or independent contractor (including but not limited to any cloud service provider), or contracts with any party for services that connect to the system that stores, processes or transmits data, each being a "Cloud Service Provider" the following applies:

1. Supplier warrants that any Cloud Service Providers engaged by Supplier to provide services are on written terms and conditions no less stringent than those set forth in the Agreement between Mondelēz and Supplier, and Supplier shall ensure that such Cloud Service Providers shall implement all security measures necessary to protect MDLZ Data Information processed by Supplier or such Cloud Service Providers under this Agreement.
2. Supplier will provide the capability to restrict the location of cloud processing / storage based on business requirements, as well as statutory, regulatory, and contractual obligations. Supplier must be able to identify the physical location of MDLZ Data processed or stored by the Cloud Service Provider.

9. Operational Technology

This section applies to technology supporting MDLZ manufacturing facilities. Supplier may be subject to the MDLZ Operational Technology standards (MINT). Consult with your primary MDLZ Manufacturing\Plant contact for any special requirements for Operational Technology.

At a minimum Supplier must:

- Use secure connection methods approved and provided by MDLZ to remotely connect to MDLZ Operational Technology.
- Protect Supplier's business and IT systems with measures in place to limit the effects of attacks such as denial of service.
- Implement network boundary protection and system and communication protection to protect the control systems and the communication links between system components from cyber intrusions.

Supplier shall provide additional scrutiny to the risks associated with embedded technology, based on the potential damages posed when used maliciously.

Supplier should specify the development, proactive management, and ongoing review of security embedded technologies, including hardening the hardware, firmware, software, transmission, and service protocols used for Operational Technology.

The supplier should develop, disseminate, and periodically review and update:

1. A formal, documented information security management system policy that addresses:

    a. The purpose of the information security management system as it relates to protecting the Suppliers personnel and assets.

    b. The scope of the information security management system policy as it applies to all Supplier staff and third-party contractors.

    c. The roles, responsibilities, management accountability structure, and coordination of the information security management system policy to ensure compliance with the Supplier security policy and other regulatory commitments.

2. Formal, documented procedures to facilitate the implementation of the information security management system policy and associated controls.

3. Formal change management process to ensure only approved access is permitted for any system or device that could allow access to the MDLZ Data.

Supplier shall deliver Services and Products related to control systems that describe:

1. required security capabilities (security needs and, as necessary, specific security controls),

2. design and development processes,

3. required test and evaluation procedures and required documentation.

The requirements must require updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented for duration as mutually agreed term between Supplier and MDLZ.

In addition, the Supplier shall support MDLZ by:

- providing MDLZ information describing the specification of the security controls employed within the control system.
- providing information describing the design and implementation details of the security controls employed within the control system (including functional interfaces among control components).
- limiting (where possible) the acquisition of commercial technology products with security capabilities to products that have been evaluated and validated through a relevant government-approved processes in the geographic area where Products and Services will be deployed.

Supplier must deploy security controls in accordance with applicable, policies, regulations, standards, guidance, and established service level agreements.

Outsourced Control System Services

Supplier must:

- implement governance oversight and user roles and responsibilities with regard to Supplier managed control system services
- monitor security control compliance of any contractors, sub processors or sub-service providers that Supplier is obligated
- ensure third-party providers are subject to the same control system security policies and procedures of the Supplier. All the contractor's equipment conforms to the same requirements as the Suppliers internal systems. Supplier must approve outsourcing of control system services to third-party providers (e.g., service bureaus, contractors, and other external service providers \ sub processors).

The outsourced control system services documentation includes service provider and end-user security roles, responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

Appendix A. Definitions

"Cloud Service Provider" means a cloud service provider is a third-party company offering a cloud-based platform, infrastructure, application, or storage services. Examples: Microsoft Azure, Google Cloud Platform, and Amazon Web Services
"Data Breach" means any breach of security leading to the accidental or unlawful disclosure, loss, alteration or other compromise of the confidentiality, integrity, or availability of MDLZ Data including Personal Information
"Goods" means products which Supplier is providing to MDLZ under contractual arrangements.
"Industry Standards" More information on standards and frameworks are available here : OWASP application security verification standard, NIST , SANS search "critical controls" , ISO 27001
"MDLZ Data" means MDLZ Data provided to, obtained by, or developed by Supplier in connection with this agreement, including Personal Information.
"MINT Standard" means standards developed for MDLZ manufacturing facilities.
"Operational Technology" is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.
"Personal Information" means any information that directly or indirectly identifies, relates to, describes or can be associated with or reasonably linked to an individual or household, and any other information defined as personal information, personal data, or other similar terms under all applicable Privacy Laws.
"Services" means services which Supplier is providing to MDLZ under contractual arrangements.
"Privacy Laws" means all state, federal, international, and provincial laws, rules and regulations applicable to Personal Information and any related information.

RELEASE NOTES

Initial version 1. April 30, 2021