SUBJECT

Global Information Security Policy

DATE ISSUED/REVISION DATE

December 2021

Purpose of the Policy

This Global Information Security Policy ("Policy") sets out the framework for the management of appropriate information security controls. Aramark has aligned the information security program with the NIST Cybersecurity framework. Aramark is committed to protecting its information assets from existing and emerging threats. Failure to do so would represent a business risk and could adversely impact the organization's reputation as well as the value of its lines of business.

Unless a term is specifically defined in this Policy, capitalized terms shall have the meaning set forth in the Glossary for Information Technology.

Scope

This Policy is the overarching policy which provides direction for and governs all Aramark Information Security policies, as well as associated standards and controls.

This Policy applies to:

1. All employees, agents, contractors, consultants, business partners, and other workers at Aramark, including all personnel affiliated with Contracted Suppliers (collectively, "Users") who have access to Aramark Information Systems, interact with Aramark Information Assets, or Process Aramark Data.
2. All Users who have access to Information Systems and Information Assets connected to Aramark network and any Information Systems and Information Assets supplied by or on behalf of Aramark.
3. All Users who have access to Information Assets owned or leased by Aramark or entrusted to Aramark by third parties.
4. All Users who have access to Information Systems managed by or on behalf of Aramark that Process, store or transmit Aramark Data.
5. All Aramark Data Processed by or on behalf of Aramark.
6. All aspects of the life cycle of Information Systems within the scope of this Policy, including the specification, design, development, installation, operation, connection, use and decommissioning of such Information Systems, services and equipment.

Roles and Responsibilities

1) All Users

Promptly escalate Information Security concerns or incidents to the Aramark Security Operations Center (securityassurance@aramark.com), IT Service Desk, or the Aramark Employee Hotline.

i) The Aramark Employee Hotline is managed by an independent service company, allowing users to make anonymous reports if preferred. In the United States and Canada, call 1-877-224-0411 or visit http://www.aramarkhotline.com

ii) To contact the Aramark Employee Hotline from outside the United States and Canada, visit www.aramarkinternationalhotline.com to obtain the local toll-free access number.

2) **Chief Information Security Officer**

The Chief Information Security Officer (CISO) is accountable for:

- Establishing and maintaining this Policy to reflect information security risk management best practices.
- Risk assessing, approving, and maintaining a list ofexceptions to this Policy.

3) **Procurement and Legal Functions**

- Implement processes that incorporate the requirement to adhere to this Policy into third-party contracts and follow internal approval processes for any exceptions.

Policy Statements

- Aramark's intent is to protect its Information Systems, Information Assets and Aramark Data.
- Aramark implements standards and processes that are applied proportionately, based on formal risk assessments, which are periodically reviewed and are based on the NIST Cybersecurity Framework series and other security best practices and applicable law.
- Aramark requires Contracted Suppliers that generate or Process Aramark Data to take a similar, risk-based approach to information security in accordance with the relevant Aramark Information Security policies and standards.
- Aramark will implement processes to incorporate requirements that adhere to this Policy in its third-party contracts and Aramark will follow internal approval processes for exceptions.
- Aramark systematically monitors and measures information security performance against its own and industry benchmarks.
- Aramark develops and improves information security policies and standards to provide sufficient protection for Aramark Data by addressing identified risks and consistency with applicable law, industry standards, frameworks, andguidance.

Risks and Implications

Failure to comply with this Policy could result in accidental or deliberate misuse of Information Systems, Information Assets and Aramark Data, leading to security breaches, virus attacks, and compromise of network systems and services. Improper use of Information Systems, Information Assets and Aramark Data as set forth in this Policy increases the risk of harm to Aramark's reputation, and may adversely impact Aramark's business, employees, suppliers and customers. Compliance with this Policy minimizes the risk of breaches of confidentiality, malicious or accidental corruption of data, theft of intellectual property, and failure to meet legal and contractual obligations.

Compliance

Aramark will regularly assess compliance with this Policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback. Any employee who has violated this Policy may be subject to disciplinary action up to and including termination. Aramark reserves the right to amend this Policy at any time and will publish updated versions to all employees and relevant third parties.

References

Aramark policies, standards, and documents associated with this Policy include the following:

- Aramark Business Conduct Policy
- Global Acceptable Use Policy

- Global Information Security Incident Management Policy
- Glossary for Information Technology

Revision History

The Policy supersedes all prior Information Security Policy or Program documents.

Version	Author	Description	Date
1.2	John Bell	Annual Review	8 Dec 2021
1.1	John Bell	Annual Review	2 Dec 2020
1.0	Daniel Gorecki	Initial Major Version	25 Oct 2019
E	Jeff Chumbley	Aramark Information Security Program	1 Dec 2017

Version	Approval/Forum	Description	Date
1.2	Vince Miller	CISO	29 Dec 2021
1.1	Vince Miller	CISO	3 Dec 2020
1.0	Daniel Gorecki	CISO	25 Oct 2019