SUBJECT

Global Data Classification Policy

DATE ISSUED/REVISION DATE

November 2020

Purpose and Intent of the Policy

The purpose of this Aramark Data Classification and Data Handling Policy ("Policy") is to protect Aramark Data and Information Assets to preserve their confidentiality, integrity, and availability in a manner that is commensurate with their value and that complies with applicable law. Aramark Data are an important company asset, which must be handled and protected appropriately. Failure to do so would represent a business risk and could adversely impact Aramark's reputation as well as the value of its lines of business.

This Policy applies to all employees, agents, contractors, business partners, and other workers at Aramark, including personnel affiliated with Contracted Suppliers (collectively, "Information Users") who access, use, store, share, transmit, or otherwise Process Aramark Data.

This Policy addresses two concepts: "Data Classification" and "Data Handling."

"Data Classification" is the process of categorizing and labeling data, based on sensitivity, confidentiality and applicable legal requirements.

"Data Handling" is the process of setting guidance—based on the classification types—for accessing, using, storing, sharing, transmitting, or otherwise Processing such data, including access rights. This Policy creates the criteria for "Data Classification" and sets forth guidance for "Data Handling."

Appendix A contains a glossary of pertinent terms and their definitions.

Roles and Responsibilities

1. **Information Owner** – Information Owners are accountable for ensuring that all Aramark Data for which they are the designated owners, are classified in accordance with this Policy and related guidance, to enable Aramark IT operations to enable appropriate protections on such Aramark Data in accordance with the classifications. Information Owners are also responsible for setting User guidance on classification and thereby promoting appropriate security standards.
2. **Chief Information Security Officer ("CISO") / Aramark IT Security** –The CISO is responsible for setting the technical security standards and requirements for Aramark Data, and ensuring that such standards and requirements are aligned and appropriate for each classification level, as further set forth in this Policy.
3. **Aramark IT Operations (including regional teams)**– Responsible for implementing, maintaining, and supporting the appropriate controls for securing Aramark Data in accordance with the classification established by the Information Owner and the security standards and requirements established by the Aramark / IT Security team. IT operations will provide the necessary technology tools to ensure appropriate levels of security for Aramark Data based on classification.
   For example:
   1. Making technology available to access, use, store, share and transmit Aramark Data securely, in accordance with this Policy.
   2. Providing approved mechanisms for sharing data security with external entities in support of business processes.
   3. Disallowing the storage of Confidential or Restricted Aramark Data on Removable Media.
4. **Information Users** – Responsible for complying with the requirements outlined within this Policy to ensure the proper handling and labeling of information based on the classification defined by the Information Owner.
5. **Legal** – responsible for communicating applicable legal requirements related to data classification and handling.
6. **Data Governance Committee** – This committee consists of a cross functional team with representation from Information Security, Legal, Corporate Compliance, IT Operations (including international) and co-chaired by the CISO and VP Legal, Privacy and Technology. The Committee is responsible for the content and enforcement of this Policy.

Levels of Data Classification

All Information Owners and Information Users shall classify all Aramark Data they own or handle into one of four (4) levels:

- Public
- Internal
- Confidential
- Restricted

Such classification levels are defined as follows:

Classification	Definitions
Public	Aramark Data that is public information and can be openly shared with all third parties. There are no legal, monetary, reputational or business impacts associated with this data. No controls are required to protect Public Aramark Data. Example: pamphlet describing Aramark services that Aramark sales team distributed at a sales conference
Internal	Aramark Data that can be shared only within Aramark. Disclosure of such Aramark Data outside of Aramark employees or contingent workers could create a limited adverse impact to the business (such as negative publicity and / or negative impact to client or consumer relationships), but such adverse impact is reasonably expected to be minimal. Limited controls are required to protect Internal Aramark Data. Examples: internal Aramark policies; company-wide memos or emails
Confidential	Aramark Data that is sensitive and can be shared only with approved individuals based upon a business need to know within Aramark. Disclosure of such Aramark Data outside the authorized Aramark team, and especially with unauthorized third parties, is reasonably expected to cause adverse impact to Aramark, Aramark Clients, Aramark employees, Aramark customers, business partners, and / or other individuals. Such adverse impact includes harm to current or future business interests, legal exposure, impact to brand, and harm to individual rights (including privacy rights). Heightened controls are required to protect Confidential Aramark Data and the controls must be compliant with applicable legal and contractual requirements. Examples: business contact information, pricing, contract terms, account-specific strategic decks
Restricted	Aramark Data that is highly sensitive and can be shared with a limited set of individuals based on a business need-to-know basis only, as authorized by Aramark's senior leadership. Disclosure of such Aramark Data outside of the need-to-know group is reasonably expected to cause substantial adverse impact to Aramark, Aramark Clients, Aramark employees, Aramark customers, business partners, and / or other individuals. Such material adverse impact includes harm to current or future business interests, legal exposure, impact to brand, and harm to individual rights (including privacy rights). Heightened controls are required to protect Restricted Aramark Data, which controls must be compliant with applicable legal and contractual requirements. Examples: Personal Information (other than business contact information), trade secrets, pre-release earnings information, company-wide strategic decks, non-public M&A, attorney-client privileged documentation

In classifying Aramark Data, beyond the examples above, Information Users should consult the Information Owner for guidance and consult with Aramark Legal and Aramark Information Security if additional guidance is required.

Information Owners must designate a classification for all information types which they are the owner of based on the 4 levels defined. Once the information is reviewed, the classification could be updated in the future if it is required.

It is the responsibility of the Aramark manager of a department, function or business unit to classify Aramark Data generated in the respective department, function or business unit if there is no designated Information Owner. For guidance on determining the appropriate classification, consult Information Security and/or Legal.

Any document generated, either in paper or digital form, should have a clear and explicit classification attached to it. The only exception to this requirement is a report or file automatically generated by an Information System. Example: Standard Oracle Financials E Accounts Payable (AP) or Accounts Receivable (AR) report. If any Aramark Data is missing a classification, then the Information User should notify the Information Owner to have such information classified in accordance with this policy.

For each new e-mail with a classification of “Confidential” or “Restricted,” Users must set Microsoft Outlook permissions to “Aramark Corporation – Confidential” or “Aramark Corporation – Restricted, view only, not for sharing,” respectively.

Data Handling

All Aramark Data other than public Aramark Data must have restricted access either in paper or digital media. All Information Systems containing Aramark Data classified as “Confidential” or “Restricted” should be evaluated in terms of its capabilities to segregate data and its security. Such data should be revaluated periodically in collaboration with Corporate Compliance, Legal and Information Security to ensure the classification and associated controls are appropriate and operating effectively.

Users should follow the below guidelines for all Aramark Data, other than Public data:

1. Internal, Confidential and Restricted Aramark Data should only be stored, transmitted, and Processed using Information Systems authorized by Aramark’s IT Operations.
2. Confidential and Restricted Aramark Data, including all copies and reproductions, should be clearly classified.
3. Confidential and Restricted Aramark Data may not be disclosed to anyone other than those individuals who possess a business need and are authorized to access such information.
4. When not in use, physical copies of documents containing Internal, Confidential and Restricted Aramark Data should be placed in a locked desk, cabinet, office, or other secure location for temporary storage.
5. For permanent storage, Internal, Confidential and Restricted Aramark Data should be stored within authorized repositories as stated within the Records Management Policy.
6. Internal, Confidential and Restricted Aramark Data should not exist on a publicly accessible repository, such as a network share or a cloud computing service that is accessible to individuals outside of those with a business reason to access such data.
7. Internal, Confidential and Restricted Aramark Data should be encrypted when stored at rest and in transit to prevent unauthorized access, modification, or disclosure.
8. Internal, Confidential and Restricted Aramark Data can be emailed using only an Aramark IT Operations-approved e-mail encryption solution.
9. Internal, Confidential and Restricted Aramark Data should be retained in accordance with the Records Management Policy.
10. Internal, Confidential and Restricted Aramark Data should be securely destroyed in accordance with the Data Destruction and Disposal Procedure.

All Information Users are responsible for handling data, based on the four classifications, and according with table set forth below as a guide. Digital data should have appropriate encryption based on industry standards.

	Distribution	**Storage /destruction**
Public	No restriction	No controls
Internal	Share only with Aramark employees and Contracted Suppliers that require such Aramark Data to provide products or services for Aramark.	Minimal security requirements, consistent with industry standards, and distribution / access limited to intended targets, preferably using Aramark approved Information Systems.
Confidential	Digital Documents: Share only with authorized Aramark employees and Contracted Suppliers via encrypted email, with "Aramark Corporation – Confidential" designation; or through Aramark IT Operations-approved platforms. (e.g., Microsoft Office 365 SharePoint, OneDrive or TEAMs sites) Paper Documents: store in a locked drawer and share only with authorized Aramark employees and Contracted Suppliers that have a current nondisclosure agreement (NDA) with Aramark.	Store in and share via Aramark IT Operations-approved platforms only and locked physical spaces. For clarity, such Aramark Data may not be stored in public servers.
Restricted	Requires permission from a manager to share. Digital Documents/Data: Share only with authorized Aramark employees and Contracted Suppliers via encrypted email, with "Aramark Corporation – Restricted" designation when sent to Aramark employee, or "Aramark Corporation – Restricted, view only, not for sharing" designation when sent to a third party. Paper Documents: store in a locked drawer and share only with authorized Aramark employees and Contracted Suppliers that have a current nondisclosure agreement (NDA) with Aramark.	Store in and share via Aramark IT Operations-approved platforms only and locked physical spaces. For clarity, such Aramark Data may not be stored in public servers, external storage or personal devices.

Compliance and Exceptions

The Data Governance Committee 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 communicate updated versions to all employees and relevant third parties.

Exceptions to this Policy are not permitted unless approved by the Data Governance Committee.

Any individual who has knowledge of a violation of this Policy should report that violation immediately to his or her supervisor, to the CISO, or Aramark Legal.

Appendix A: Glossary

Terms defined below importing the *singular* number include the *plural* and vice versa and terms importing gender include the masculine, feminine and neuter genders.

TERM	DEFINITION
"Aramark Data"	All data and information of Aramark, its clients, customers, suppliers or other third parties to the extent such data and information is created, collected, stored, processed or transmitted by Aramark or by third parties on behalf of Aramark, in electronic, verbal, or physical form. This data may or may not contain Personal Information.
"Breach"	An Information Security Incident that results in any (i) loss or theft of Aramark Data; (ii) unauthorized use, disclosure, destruction, loss alteration or acquisition of or access to, or other unauthorized Processing of Aramark Data; or (iii) unauthorized access to or use of, inability to access, or malicious infection of, Aramark Information Systems or information systems of an Aramark third party acting on behalf of Aramark that reasonably may compromise the privacy or confidentiality of Aramark Data.
"Contracted Suppliers"	A third-party vendor who has been contracted or otherwise retained to provided products or services for or on behalf of Aramark.
"Information Asset"	A tangible or intangible body of information that has value to an organization.
"Information Security Event"	An observable occurrence indicating a possible breach of information security or failure of controls. The occurrence of an Information Security Event does not necessarily mean that an attack has been successful or that there has been a security breach affecting the confidentiality, integrity and or availability of information.
"Information Security Incident"	Means one or multiple related and identified Information Security Events that could reasonably be expected to result in significant damage, risk, or harm to Aramark's Information Systems, Information Assets and Aramark Data, or could reasonably be expected to require reporting to a government authority or individuals.
"Information Security Incident Management Process'	The consistent and effective approach to the handling of Information Security Incidents, which governs all activities concerning incident response and incident handling.
"Information System"	A network or collection of communication channels and or multiple pieces of equipment used within an organization for the dissemination of information. Hardware, software, computer system connections and information, information system Information Users, and the system's housing are all part of an Information System.
"Personal Information"	Means any information that (a) relates to an identified or identifiable individual, (b) is protected under applicable privacy and security laws, or (c) that is linked or combined with information identified in (a) or (b) above, whether such data is in individual or aggregate form and regardless of the media in which it is contained. Without limiting the foregoing, an identifiable individual is one who can be identified, directly or indirectly. Personal Information includes, but is not limited to: name; home or other physical address; email address or other online contact information; telephone number; social security or similar government identification numbers; driver's license number; bank, loan, mortgage, or payment card account number; medical information; and date of birth.
"Process" or "Processes" or "Processing"	Means to perform any operation or set of operations upon Aramark Data, whether manually or by automatic means, including but not limited to collection, recording, sorting, structuring, accessing, storage, adaptation or alteration, retrieval, consultation, use, transfer, dissemination.
"Removable Media"	Portable device that can be connected to an information system (IS), computer, or network to provide data storage. These devices interface with the IS through processing chips and may load driver software, presenting a greater security risk to the IS than non-device media, such as optical discs or flash memory cards. Note: Examples include, but are not limited to: USB flash drives, external hard drives, and

TERM	DEFINITION
	external solid state disk (SSD) drives
“Security Incident Response Team” or “SIRT”	The dedicated information and cyber security skilled team that is trained in proactive and reactive defense practices.
“Security Operations Center” or “SOC”	Functional group responsible for monitoring, detecting and responding to Information Security Events.
“Security Vulnerability”	Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.
“User”	Means all employees, agents, contractors, consultants, business partners, and other workers at Aramark, including all personnel affiliated with Contracted Suppliers.

Version	Author	Description	Date
1.0	Naveen Palapura	Initial Major Version	25 Oct 2020

Version	Approval/Forum	Description	Date
1.0	Vince Miller + Irene Ayzenberg-Lyman	CISO + Aramark Privacy Counsel	24 Nov 2020