SUBJECT
Global Acceptable Use Policy

DATE ISSUED/REVISION DATE
June 1, 2025

Purpose of the Policy

The purpose of the Global Acceptable Use Policy ("Policy") is to set forth Users' responsibility for the appropriate use of Information Systems and for the security and protection of Aramark's Information Assets and Aramark Data. This Policy applies, regardless of location, unless otherwise set forth in a country-specific Appendix to this Policy. Such Appendices contain, where applicable, the specific rules by country or jurisdiction. In the event of a conflict between a country-specific Appendix to this Policy and this Policy, the country-specific Appendix shall control.

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 applies to 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 Information Systems; interact with Aramark Information Assets; or access, use, store, retrieve, transmit, or otherwise Process Aramark Data.

Roles and Responsibilities

All Users

- Use Information Systems in accordance with this Policy.

  Promptly escalate Information Security concerns or incidents to the Aramark Security Operations Center (security@aramark.com), IT Service Desk, Aramark Employee Hotline, or the User's Manager.
    - 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 www.aramarkhotline.com.
    - 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.

Chief Information Security Officer

The Chief Information Security Officer (CISO) is accountable, through the Chief Information Officer, to the Chief Executive Officer for:

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

Policy Statements

1.1 General Use and Ownership

- Users will comply with all applicable laws and regulations.
- Users will use Information Systems — e.g., any systems used to generate, receive and store voice, email and video — in a manner that is consistent with Aramark's Business Conduct Policy (BCP).

- Information stored on or passed through Aramark's computer communications hardware is not considered private and Users acknowledge they have no expectation of privacy in any Aramark Data flowing through such systems, unless otherwise required by applicable laws, include data privacy laws.
- Unless otherwise required by applicable law, Aramark Data is the sole property of Aramark.
- Aramark Data shall not be stored on any non-Aramark Information System unless expressly permitted by Aramark's corporate IT Department.
- All Information Systems used for Aramark business-related purposes, that Process Aramark Data, or that connect to Aramark's network must be authorized and financially approved by the corporate IT Department, including third-party software, cloud applications, and all applications that utilize AI are subject to Artificial Intelligence policy.
    - The use of all software including freeware, shareware and open source must be consistent with the permitted uses under licensing terms.
- Users must promptly report the theft, loss, or unauthorized disclosure of or access to Aramark Data, Aramark's Information Systems or Aramark's Information Assets (e.g., laptops and mobile devices).
- Users shall ensure that digitized forms of Aramark Data are stored in a location or on a system that is appropriately backed up by the corporate IT Department.
- Users will take reasonable care to avoid introducing viruses or other malware onto devices provided by Aramark (e.g., virus checking any software or data files prior to loading).
- Users will take reasonable care to ensure that permitted personal devices connected to Aramark's infrastructure are kept free of viruses and other malware, and Users shall not circumvent measures designed to protect devices from loading unauthorized software.
- User will complete required annual Security Awareness training in a timely manner

1.2 IDs and passwords

- Users will not share their user ID and password, even with the IT Service / Help Desk.
- Users will create passwords that are easy to remember but hard to break, and in compliance with Aramark's password policies.
- Users will not log on to any Aramark systems or applications using another User's credentials.
- User passwords should be unique to Aramark's Information Systems and should not be the same or similar to passwords for non-business purposes.
- Users will not store passwords in written format or via an electronic end-user documents such as Word, Excel, Notepad, etc.
- Users will comply with Aramark's Access Management and MFA policies.

1.3 Managing and Protecting Information

- Users will comply with Aramark's Global Records Management Policy.
- Users will not disclose Aramark Data to unauthorized third parties and will use reasonable efforts to protect themselves from phishing and other attempts to obtain Aramark Data or other personal information in a fraudulent manner.
- Users must not email unencrypted sensitive information, such as credit card numbers, social security numbers, or patient health information unless using Aramark corporate IT-approved encryption technology.
- Users shall take due care in protecting Aramark's confidential and proprietary information, such as customer, financial, business partner, vendor information or other trade or business secrets, including by not leaving confidential information in public areas, such as copy centers.

1.4 Personal Use

- Personal use of Aramark Information Systems is permitted as long as it is incidental and does not involve any prohibited activity, interfere with productivity or unreasonably deplete system resources or storage capacity.
- The ability to store personal data on Aramark Information Systems is a privilege, not a right, and Aramark can require such data to be removed.

1.5 Unacceptable Use

- Users will not use Aramark's Information Assets for personal gain.
- Users will not let unauthorized people have access to Aramark's Information Assets.
- Users will not knowingly download, copy, distribute or accept copyrighted or confidential materials (including software) without the authority of the owner.
- Users will not use any type of applications or devices, or modify device configuration, to circumvent management or security controls.
- Users will not download any illegal software onto an Aramark Information Asset. Aramark may remove such illegal software without notice.
- Users will not use personal devices which are approved for connection to Aramark networks to access websites which Users know or reasonably should know are likely to contain inappropriate material, or which are likely to expose such devices to viruses or malware.
- Users will not use personal email or commercial email services to conduct business. Only corporate issued email accounts are approved for use in corporate business.
- Users will not retransmit electronic material featuring offensive content.
- Users will not engage in mass transmission of unsolicited emails (SPAM).
- Users will not retransmit chain messages.
- Users will not spoof the identity of another user.
- Users will not open email attachments or click on embedded links if they have doubts regarding the authenticity of e-mails received, in which case Users shall forward such suspicious e-mails to the channels communicated by Aramark corporate for further analysis.
- Users will not use Aramark Information Assets to intentionally visit sites or news groups that are obscene, indecent or advocate illegal activity.
- Users will not participate in online gambling.
- Users will not put Aramark Data onto online forums, blogs or social networking sites.
- Users will not store music, video or other media-related files for non-business purposes on network drives.
- Users will not use hacking, network testing tools (sniffers) and eavesdropping software of any kind on Aramark networks unless such activities are within the ordinary scope of their job duties and are done with appropriate corporate approvals.
- Users will not engage in port scanning or security scanning without appropriate corporate approvals.

1.6 User-generated Content and Social Media

- Users will comply with Aramark's Social Networking Policy and Business Conduct Policy.

1.7 Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorized access or loss of Aramark Data, Aramark enforces a clear desk and clear screen policy.

- Users will protect Aramark Data using security features provided by Aramark's corporate IT Department (e.g., secure print on printers).
- Users will ensure computers are logged off, locked, or protected with a screen locking mechanism controlled by a password when unattended.
- Users will take care not to leave confidential material on printers or photocopiers.
- Users will dispose of all business-related printed matter using confidential waste bins or shredders.

1.8 Separation from Aramark and Return of Aramark Property and Equipment

- Users must return all Aramark Information Assets and other Aramark property to Aramark in good condition upon separation from Aramark. This includes items such as office keys; garage passes; building security passes; company-issued credit cards; Aramark manuals and documents; computers, printers, smart phones or tablets, fax machines, including charging and other ancillary equipment; and any and all electronic and print versions of Aramark Data, documents, and confidential or proprietary information. Users are responsible for any lost or damaged items, subject to applicable laws.
- Aramark shall terminate Users' email accounts upon separation from Aramark, and Aramark shall continue to be entitled to access such email accounts for business continuity reasons as well as to protect and defend Aramark's rights.
- Upon separation from Aramark, all files and data stored in any Aramark Information System or Aramark Information Asset assigned to a User shall be the sole property of Aramark. Users are responsible for removing any personal information from any such Aramark Information Systems and Information Assets prior to their separation from Aramark.

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 increases the risk of harm to Aramark, and may adversely impact our business, clients, 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. Failure to comply with this policy may result in suspension of access rights to Aramark systems.

References

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

- Aramark Business Conduct Policy
- Global Information Security Policy
- Global Information Security Incident Management Policy
- Social Networking Policy
- Global Access Management Policy
- Global MFA Policy
- Glossary for Information Technology

Revision History

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

Version	Author	Description	Date
1.0	Daniel Gorecki	Initial Version	6 Jan 2020
1.1	John Bell	Annual Review	2 Dec 2020
1.2	John Bell	Annual Review	29 Nov 2021
1.3	John Bell	Modification for clarity	4 Aug 2022
1.4	John Bell	Annual Review	1 Jun 2023
1.5	John Bell	Annual Review & Format update	1 Jun 2024
1.6	John Bell	Clarify Software license language	1 Jun 2025

Approval History

Version	Approval	Title	Signature	Date
1.1	Vince Miller	CISO		3 Dec 2020
1.2	Vince Miller	CISO		29 Nov 2021
1.3	Vince Miller	CISO		1 Jun 2022
1.4	Shawn O'Shea	CISO		1 Jun 2023
1.5	Shawn O'Shea	CISO		1 Jun 2024
1.6	Doug Traher	CISO	Signed by: ED167DC3FFEE464...	5/28/2025

Appendix:

United States Specific Exception.

Nothing in this Policy is intended to restrict U.S.-based employees, as defined by the National Labor Relations Act, from sharing their own or their co-workers employment-related information to a third party.

Appendix:
Germany Specific Exception on use of Internet and e-mail in the workplace. (Erklärung über die Internet- und E-Mailnutzung am Arbeitsplatz)

The following declaration of “use of Internet and e-mail in the workplace” overrides sections 1.4 Personal use of this Policy

§ 1 Ausschließlich dienstliche Nutzung des betrieblichen Internetzuganges

Der Mitarbeiter darf den Internetzugang am Arbeitsplatz **ausschließlich für dienstliche Zwecke** nutzen.

Jede private Nutzung ist untersagt, sowohl während, als auch außerhalb der Arbeitszeit.

§ 2 Ausschließlich dienstliche Nutzung des betrieblichen E-Mail-Zuganges

Der Mitarbeiter darf die vom Arbeitgeber zur Verfügung gestellte personalisierte oder allgemeine E-Mail-Adresse **ausschließlich für dienstliche Zwecke** benutzen.

Er darf diese Adressen insbesondere nur für dienstliche Zwecke bekannt geben.

Dem Mitarbeiter ist jede private E-Mail-Nutzung während und außerhalb der Arbeitszeiten untersagt.

§ 3 Vertraulichkeit, Sicherheit

Der Mitarbeiter hat die ihm zugeteilten Zugangsdaten, insbesondere seine Passworte, geheim zu halten und darf diese nicht an Dritte weitergeben.

Jede Internet- und E-Mail-Nutzung, die auf die Benutzung der Zugangsdaten des Mitarbeiters zurückzuführen ist, wird dem Mitarbeiter zugerechnet.

Der Mitarbeiter hat bei der dienstlichen Nutzung von Internet und E-Mail die allgemeinen Sicherheitsstandards zu berücksichtigen, insbesondere nur auf sicheren, vertrauenswürdigen Seiten surfen. E-Mails und Dateien unbekannter Herkunft dürfen nicht geöffnet werden.

Der Mitarbeiter ist verpflichtet, im Zweifel die IT-Abteilung des Arbeitgebers zu kontaktieren sowie dieser alle Sicherheitsprobleme oder Fehler-/Warnmeldungen des Systems unverzüglich mitzuteilen.

§ 4 Konsequenzen bei Verstößen

Der Mitarbeiter hat bei Verstößen gegen das Verbot der Privatnutzung mit arbeitsrechtlichen Konsequenzen, insbesondere Abmahnung bzw. Kündigung zu rechnen.

Der Arbeitgeber behält sich zudem die Geltendmachung weiterer Ansprüche vor, insbesondere auf Unterlassung sowie Schadenersatz.

Der Mitarbeiter wird in diesem Zusammenhang ausdrücklich darauf hingewiesen, dass im Falle ausdrücklich untersagter Privatnutzung und hieraus resultierender Schäden (bspw. durch Viren, etc.) erhebliche finanzielle sowie immaterielle Schäden für den Arbeitgeber entstehen können.

§ 5 Schlussbestimmungen

Mündliche Nebenabreden bestehen nicht. Änderungen oder Ergänzungen dieser Erklärung einschließlich dieser Bestimmung bedürfen zu ihrer Wirksamkeit der

Schriftform.

Die beigefügte „**Benutzerrichtlinie für ARAMARK IT-Systeme**“ ist wesentlicher Bestandteil dieser Erklärung

Sollte eine Bestimmung dieser Erklärung ganz oder teilweise unwirksam sein oder werden, so wird hiervon die Wirksamkeit der übrigen Bestimmungen dieser Erklärung nicht berührt. An die Stelle der unwirksamen Bestimmung tritt die gesetzlich zulässige Bestimmung, die dem mit der unwirksamen Bestimmung Gewollten wirtschaftlich am nächsten kommt. Dasselbe gilt für den Fall einer vertraglichen Lücke.

Der Mitarbeiter stimmt den Inhalten dieser Erklärung sowie den Inhalten der Benutzerrichtlinie IT ausdrücklich zu.