
Information Resources Policy for Non-Publix Associates

Publix Super Markets, Inc.

Publix[®]

Publication Date: March 1, 2021

Introduction

Purpose

Access to and use of Publix information resources imposes certain responsibilities and obligations and is granted subject to Publix's policies as well as local, state and federal laws. This policy sets Publix's expectations of acceptable conduct while accessing and using Publix information resources.

Scope

This policy applies to all Non-Publix associates and all information resources owned or operated by Publix or associated with Publix business.

Noncompliance

Noncompliance with this policy and any revisions may cause significant loss or damage to Publix's business operations, image or assets and therefore may be a serious offense. Non-Publix associates violating any portion of this policy will be held personally accountable and may be subject to

- termination of services
- appropriate legal action and/or
- legal liability for damages and any reasonable costs associated with the violation.

The obligation to protect Publix's information is ongoing even after termination of services with Publix.

Policy topics

The following topics are included in this policy.

- Definitions
 - Responsibilities and Rights
 - Prohibited Activities
-

Definitions

Purpose

This section defines terms used throughout this policy.

Non-Publix associates

Non-Publix associates are individuals accessing and using Publix information resources while performing services for Publix Super Markets, Inc. and its subsidiaries and affiliates (collectively "Publix"). Non-Publix associates are categorized as follows:

- Supplemental Workers – Individuals performing duties comparable to Publix associates on a temporary basis who are therefore not entitled to Publix employee benefits; this includes but is not limited to clerical or unskilled workers requested through the Publix Employment Office and independent contractors with specific skills, training, degree or occupational license requested through the HR Compensation department.
 - Business Associates – Individuals performing duties on behalf of their employer typically through a Publix agreement or contract with the Business Associate's employer; this includes but is not limited to consultants, vendors, suppliers, service providers, etc.
-

Information resources

Information resources include

- Publix information in any form (i.e., verbal, physical or electronic) and
- information technology associated with the creation, collection, processing, use, storage, transmission, analysis and disposal of Publix information.

Publix information and information technology are collectively known as *information resources*.

continued on next page

Definitions, Continued

Publix information

As used in this policy, Publix information can be classified as sensitive or private and includes, but is not limited to, the following:

- information about Publix and its operations not generally available to the public, such as information that reveals the process or know how by which Publix's existing and/or future products, services, applications and methods of operation are developed, manufactured, conducted or operated and the means and methods of marketing such products, services, applications and methods of operation
- information relating to Publix's performance, operations, suppliers, products, services, applications and methods of operation
- information about sales not otherwise made available to the public
- information that reveals the specific application of management and improvement methodologies at Publix
- intellectual property (i.e., type of property right that is not tangible, such as knowledge, ideas, discoveries, inventions, copyrightable works, patents, products, application source code, etc.) created for Publix or produced by Publix associates and/or Non-Publix associates (intellectual property is considered work for hire and therefore owned by Publix)
- protected health, personally identifiable or other private (non-public) information about customers and associates of Publix (except such information disclosed by the customer or associate without an expectation of privacy) and
- any other proprietary information.

continued on next page

Definitions, Continued

Publix information, continued

Sensitive information is information that could seriously damage Publix if disclosed to unauthorized parties within or outside of Publix. Examples include, but are not limited to, the following:

- Protected Health Information (PHI)
- Personally Identifiable Information (PII) such as a person's name with his/her SSN, driver's license number or bank account number
- full debit or credit card number
- strategic or operational decisions before they're announced, such as new market entries, and
- financial results or stock price before they're publicly released.

Private information is information that could harm but not seriously damage Publix if disclosed to unauthorized parties within or outside of Publix. Examples include, but are not limited to, the following:

- personal information such as a person's name with his/her home address, birth date or age, personal email address, or home or personal cell phone number
- personal information such as a person's SSN, driver's license number, personal email address, or home or personal cell phone number without his/her name
- new store locations and strategies
- future ad items and prices
- pricing zones and strategies
- trade secrets such as our product recipes
- associate pay rates and evaluation results
- associate benefits and retirement information
- Workers' Compensation claim information and
- technical information, such as system/network documentation, security vulnerabilities and application source code.

continued on next page

Definitions, Continued

Information technology

As used in this policy, information technology includes, but is not limited to, the following:

- computers such as desktops, mainframe, servers, etc.
- mobile computing devices such as laptops, tablets, smartphones, MP3 players, digital cameras and other technology
- online/cloud-based platforms, repositories and services (e.g., Azure, Google Cloud, GitHub, Dropbox, OneDrive, etc.)
- computer networks
- applications/software
- electronic messaging systems such as email, texting and paging systems
- telephone and voice mail systems
- internet sites
- storage devices such as DVDs, thumb drives, disks, external drives, etc. and
- copiers with hard drives that maintain document images.

In addition to the above, Publix specific information technology includes, but is not limited to, the following:

- online/cloud-based platforms, repositories and services that are developed, purchased or subscribed to by Publix
 - software and related resources that are owned, licensed, sponsored by, operated on behalf of or developed for the benefit of Publix
 - internet sites that are managed by or on behalf of Publix (Publix.com, social media sites, etc.)
 - intranet sites that are owned, managed or sponsored by, operated on behalf of or developed for the benefit of Publix (i.e., Publix Connection) and
 - technology by which Publix's existing and/or future products, processes, services, applications and methods of operation are developed, manufactured, marketed and sold.
-

Responsibilities and Rights

Purpose

This section describes Non-Publix associates' responsibilities and rights related to information resources.

Responsibilities

Non-Publix associates are responsible for

- abiding by this policy and any revisions
- notifying appropriate Publix management or the Computer Incident Response Team (CIRT) of known or suspected violations of this policy (Note: Contact the CIRT hotline by calling 1-866-994-CIRT (1-866-994-2478) or emailing <mailto:cirt@publix.com>.)
- carefully inspecting emails, only clicking on links and opening attachments that are from known senders or that have been verified with the sender, and forwarding any suspicious emails to spam.reporting@publix.com
- accessing, using, communicating, distributing, disclosing, storing, transporting and disposing of only those information resources authorized and assigned to them by appropriate Publix management or as required by law
- protecting their logon ID and password from unauthorized use
- appropriately protecting Publix information in electronic formats and using available security controls such as secured folders and email encryption (Note: Contact I/S Security and Compliance with questions regarding how to effectively secure Publix information in electronic formats by emailing <mailto:ISSecurityandCompliance@publix.com>.)
- appropriately securing Publix information in physical formats, such as within their workspace, file cabinets and designated storage areas
- appropriately protecting and securing Publix information technology (including, but not limited to, computer desktops, storage devices and mobile computing devices) while at home, while at work, between home and work, when traveling, etc. to prevent theft, damage and misuse
- connecting Publix issued mobile computing devices to the Publix network at designated intervals to receive critical security updates
- retaining and disposing of Publix information in accordance with applicable records management policies
- remotely accessing Publix information technology only as authorized by appropriate Publix management, using authorized methods and employing current anti-virus software
- procuring, obtaining, installing, copying, replicating or using software only as authorized by appropriate Publix management and permitted by applicable software licensing agreements and
- legally licensing and registering authorized software in Publix's name only as authorized by appropriate Publix management.

continued on next page

Responsibilities and Rights, Continued

Rights

Non-Publix associates should have no expectation of privacy with respect to their use of Publix information technology. Information stored or transmitted on and use of Publix information technology can and will be viewed and monitored by authorized Publix associates without permission or notice.

Publix is not responsible for the loss or deletion of claimed personal information (messages, data, files, etc.) stored or transmitted on Publix information technology.

Prohibited Activities

Purpose

This section describes prohibited activities by Non-Publix associates and prohibited activities using Publix information technology.

Prohibited activities by Non-Publix associates

Prohibited activities by Non-Publix associates include, but are not limited to, the following:

- using Publix information resources for personal gain or to conduct non-Publix business
- using another user's logon ID and password, except as authorized by appropriate Publix management
- sharing their own logon ID and password, except as authorized by appropriate Publix management
- exporting, transferring or copying security mechanisms utilized for authentication, verification or encryption (e.g., digital certificates, encryption keys, password hashes, etc.), except as authorized by appropriate Publix management
- loading, transferring or storing Publix information on non-Publix information technology, except as authorized by appropriate Publix management or required by law
- loading, transferring or storing Publix information on unauthorized Publix information technology, except as authorized by appropriate Publix management
- loading or storing non-Publix information on Publix information technology, except as authorized by appropriate Publix management or required by law
- connecting or installing Publix information technology (such as computers, applications, software, storage devices, mobile computing devices, etc.) to or on non-Publix information technology, except as authorized by appropriate Publix management or required by law
- connecting or installing Publix information technology (such as computers, applications, software, storage devices, mobile computing devices, etc.) to or on unauthorized Publix information technology, except as authorized by appropriate Publix management
- connecting or installing non-Publix information technology (such as computers, applications, software, storage devices, mobile computing devices, etc.) to or on Publix information technology, except as authorized by appropriate Publix management or required by law

continued on next page

Prohibited Activities, Continued

**Prohibited activities
by Non-Publix
associates, continued**

- browsing, intercepting or accessing another user's Publix information (physical or electronic), except as authorized by the user or appropriate Publix management
- discussing Publix information in a manner where the information could be overheard by others, such as on planes, in elevators and on mobile phones
- discussing or disclosing Publix information in a manner inconsistent with Publix policies, guidelines and practices, such as with the media or on social media sites
- disseminating, copying, releasing, divulging, using, communicating, disclosing or destroying Publix information, except as authorized by appropriate Publix management or required by law
- participating in surveys, except as authorized by appropriate Publix management
- using any tool or method to evaluate or compromise Publix information technology security (such as tools that discover passwords, identify security vulnerabilities or decrypt encrypted files), except as authorized by appropriate Publix management
- attempting to break into any Publix information technology, except as authorized by appropriate Publix management
- disabling monitoring and auditing features on Publix information technology, except as authorized by appropriate Publix management
- disabling or bypassing security tools or controls on Publix information technology, except as authorized by appropriate Publix management
- monopolizing systems, overloading networks with excessive data, degrading services or wasting computer time, disk space or other resources
- modifying the Publix standard computer desktop or laptop configuration (for example, using computer screen savers or wallpaper not provided by Publix)
- simultaneously connecting to external networks through technology such as DSL and wireless while being physically connected to the Publix network through Publix information technology such as computer desktops and laptops (this excludes logical connections through Citrix, AnyConnect, Azure Virtual Desktop, etc.)
- saving emails to a network drive, a hard drive, a cloud repository or portable media using a personal storage table (.pst) file and
- using unnecessary messages, graphics and pictures such as personal beliefs, affiliations, representations of Publix trucks in signature lines, etc.

continued on next page

Prohibited Activities, Continued

Prohibited activities using Publix information technology

Prohibited activities include, but are not limited to, using Publix information technology

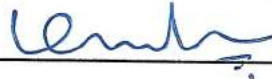
- to disclose, distribute or communicate unsolicited commercial announcements or advertising material, except as authorized by appropriate Publix management
 - in a manner that may constitute verbal abuse, slander, libel or defamation, or may be considered offensive, harassing, vulgar, obscene or threatening
 - in a manner that violates any local, state or Federal laws
 - to distribute or communicate with malicious intent any material that embarrasses or tarnishes the reputation of any individual or Publix
 - to attempt to break into any information technology, whether the information technology is owned by Publix, another person or another entity, except as authorized by appropriate Publix management
 - to conduct any illegal activities such as gambling, trafficking in weapons or drugs, or terrorist activities
 - to distribute chain letters, unauthorized mass mailings or malicious code
 - to browse pornographic web sites, hate-based sites, hacker or cracker sites or other sites that Publix has determined to be prohibited
 - to receive news feeds and automated data updates, except as authorized by appropriate Publix management and
 - to participate in external chat rooms, except as authorized by appropriate Publix management.
-

Information Resources Policy for Non-Publix Associates (Supplemental Workers)

Agreement

By signing this agreement, I acknowledge that I have read and understand the *Information Resources Policy for Non-Publix Associates* dated March 1st of the current year and agree to fully accept and adhere to this policy and any revisions. I understand that noncompliance with this policy and any revisions may cause significant loss or damage to Publix's business operations, image or assets and therefore may be a serious offense. I understand that if I violate any portion of this policy, I will be held personally accountable and may be subject to termination of services, appropriate legal action and/or legal liability for damages and any reasonable costs associated with the violation.

Printed Name: MOHANAVELU KUMARASAMY

Signature: 

Department: SUPPLY CHAIN

Date: 11/02/2021

Return instructions

Please detach this page and return it to the manager responsible for your work.
