Acceptable Use Policy

Version Control

Version	Date	Author	Change	Status
1.80	03/22/2021	Nick Coco	Initial Draft	Draft
1.81	06/17/2021	Nick Coco	Second Draft	Draft
1.82	07/12/2021	Nick Coco	Third Draft	Draft
1.83	08/06/2021	Gregg Robbins	Fourth Draft	Draft
1.84	12/20/2021	Gregg Robbins	Reformat, new template, new standards	Draft
1.85	04/11/2022	Gregg Robbins	Align with other ISO 27002 work	Draft
1.86	06/12/2023	Nick Coco	Quick edits for grammar	Draft
1.87	06/20/2023	Nick Coco	Introduction rewrite	Draft
1.88	06/30/2023	Nick Coco	Review edits of section 4	Draft
1.89	06/30/2023	Gregg Robbins	Review and edits	Draft
1.90	10/05/2023	Andrew Cordischi	Review and edits	Draft
2.00	10/09/0203	Andrew Cordischi	Published	Final

Confidentiality Notice

This document transmission (and/or the documents accompanying it) is for the sole use of the intended recipient(s) and may contain information protected by the attorney-client privilege, the attorney-work-product doctrine or other applicable privileges or confidentiality laws or regulations. If you are not an intended recipient, you may not review, use, copy, disclose or distribute this message or any of the information contained in this message to anyone. If you are not the intended recipient, contact the sender by reply e-mail and destroy all copies of this message and attachments.

Copyright Notice

Copyright 2023 by Watco Companies, LLC All rights reserved. This documentation or any portion thereof and related products may not be reproduced or used in any manner whatsoever without the express written permission of the publisher. This document is provided "as is" without any warranty of any kind, either express or implied, statutory, or otherwise; without limiting the foregoing, the warranties of satisfactory quality, fitness for a particular purpose or non-infringement are expressly excluded and under no circumstances will Watco Companies, LLC be liable for direct or indirect loss or damage of any kind, including loss of profit, revenue, goodwill, or anticipated savings. All such warranties are hereby excluded to the fullest extent permitted by law. Changes are periodically made to the information contained herein; these changes will be incorporated in new editions of the documentation. Watco Companies LLC may make improvements and/or changes to the documentation at any time.

Acceptable Use Policy

Table of Contents

Acceptable Use Policy

1. Introduction

The intention for publishing this Acceptable Use Policy is to define the rules and requirements to be followed regarding the use of Watco owned technology equipment and related systems. Related systems include but are not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet/Intranet browsing, network accounts providing file sharing and transfer, print/fax equipment, etc. Watco is committed to protecting the safety of all team members, customers, and partner organizations. Inappropriate use of computer equipment exposes Watco to risk including viruses, network compromise, and legal issues. For these reasons, technology systems provided by Watco are intended for business use purposes in serving the interests of the organization in the course of normal operations. Effective security is a team effort which benefits from the participation and support of every Watco team member and affiliate who deals with information and/or information systems. Every technology user is responsible for knowing these guidelines and conducting their activities accordingly.

2. Authority and Responsibility

- Watco Information Security Team:
  - Reviewing and updating information security related content.
- People Services:
  - Reviewing and updating the process periodically.
  - Approving of the process changes.
- All Team Members:
  - Understand and comply with the policy as written.

3. Glossary

3.1 **“Confidential Information (Sensitive Information)”**
Any Watco information that is not publicly known. This includes tangible and intangible information in all forms such as information that is observed or orally delivered, is in electronic form, is written, or is in other tangible form.

3.2 **“Electronic Messaging System”**
Any device or application that provides the capability of exchanging digital communication between two or more parties. Examples are email, instant messaging, and text messaging through applications such as Microsoft Teams or SMS messaging (cell phone messaging).

3.3 **“Information Asset”**
Any Watco data in any form and the equipment used to manage, process, or store Watco data that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

3.4 **“Partner”**
Any non-Team Member of Watco who is contractually bound to provide some form of service to Watco.

3.5 **“Password”**
An arbitrary string of characters chosen by a user that is used to authenticate the user when they attempt to log on, in order to prevent unauthorized access to their account. This includes alphanumeric passwords, pass phrases, and numeric PINs.

3.6 **“User”**
Any Watco team member or partner who has been authorized to access any Watco electronic information resource.

4. Policy Outline

4.1 User IDs and Passwords

- **Password Proximity to Access Devices** – Passwords used to access a technology device or location should not be written down and stored in close proximity to the device or location where they can be easily found and used by an unauthorized person.
  - For example, a computer logon password written on a post-it note should not be stuck to the computer monitor or under the keyboard.
  - An index card kept in your purse or wallet however is not considered in close proximity and is acceptable.
- **Individual Account Password Sharing** – Team members should not disclose the password associated with their individual User ID to another team member or third party. If access to another team member's account is needed for an immediate and justifiable business case, the IT Help Desk or Information Security Team should be contacted for assistance.
- **Password Reuse** – Passwords used for personal account access, such as personal email, should not be used for work account access. Additionally, passwords for Watco accounts should not be used for any service or systems that is not a Watco system. Team members should create strong, unique, passwords for work related accounts.
- **Password Vaults** – Watco Information Security Team provides a standardized password vault for company supplied computers that meets the various regulatory and security requirements for password vaults. A password vault allows team members to only have to remember one password to access the password vault and it can store all of your passwords securely in case you have difficulty remembering them. Contact the IT Help Desk and/or Information Security Team for more information or help in using these tools. Do not use browser password manger to store Watco system passwords as these systems do not meet Watco regulatory and security requirements. Do not install and use a third party password vault unless it is approved by the Information Security Team to meet our regulatory and security requirements.
- **Suspected Password Disclosure** – In the event a team member's password is suspected to have been exposed or compromised, the IT Help Desk and/or Information Security team should be contacted immediately. The team member's password should be reset for any affected accounts.

4.2 Electronic Messaging

- **Email Confidentiality** - For legal and security purposes, authorized individuals within Watco may retrieve any electronic mail messages sent by or to Watco team members. Such messages shall be treated as confidential by other individuals and accessed only by the intended recipient(s).
- **Reasonable Personal Use of Computer and Communications Systems** - Watco allows computer users to make reasonable personal use of its electronic mail and other computer and communications systems. All such personal use must be consistent with conventional standards of ethical and polite conduct.
  - For example, electronic mail must not be used to distribute or display messages or graphics which may be considered by some to be disruptive or offensive (such as sexual jokes or pornography).
- **Sending Unsolicited Electronic Mail** - Team Members must not send uninvited or unsolicited electronic mail (also known as spam) to any number of recipients. For sending large-volume or bulk email, Team Members must communicate with the Watco IT team to set up the appropriate solution.

4.3 Internet and Internal Network Usage

- **Unencrypted Personally Identifiable Information (PII) Sent Via Internet Prohibited** - Team Members must never transmit any personally identifiable information (such as social security numbers, passport numbers, driver's license numbers, personal addresses, etc.) unencrypted over the Internet. If a method to transmit such data is not immediately available, team members may contact the IT Help Desk and/or Information Security Team for assistance.
- **Supported Devices** - Only Watco supplied, or Watco approved, devices may connect to Watco internal data networks. This is to include both wireless (Wi-Fi) and wired network connections.
- **Watco Guest Network** – The Watco guest network is provided for the convenience of team members and visitors in order to connect personal devices for limited Internet access only. Watco supplied technology devices should not connect to the Guest network unless it is needed for momentarily testing of network connectivity or diagnostics.
- **Bandwidth Usage** – No team member may make personal use of a program that consumes large amounts of Internet bandwidth such that it affects other team members' ability to perform their job duties. Examples include streaming media services (video and/or audio), social media, gaming, etc.

4.4 Internal Systems Usage

- **Circumventing Security and Access Controls** – Team Members must refrain from installing any code or tool(s) that circumvents the authorized access control or security mechanisms found in operating systems or access control packages. All team members must also refrain from installing any VPN or network anonymizing software not provided by Watco unless otherwise approved by Watco Information Security Team.
- **Prohibition Against All Forms of Adult, Harmful, or Offensive Content** - All forms of offensive material or adult content are prohibited on Watco computers and networks. Prohibited activities or content include, but are not limited to:
  - **Adult Content:** Content depicting pornography or what could be considered pornography.
  - **Offensive Content:** Content that is considered defamatory, obscene, abusive, an invasion of privacy, or otherwise objectionable.
  - **Harmful Content:** Content that may damage, interfere with, intercept, or otherwise alter any technology system, software, or data.
- **Illegal Software Usage** – No team member may make use of, download, or install illegal software. This includes legal software obtained illegally. If there is a legitimate business need for an application that a team member does not already have access to, the IT Help Desk can be contacted for assistance in acquiring the needed software.

4.5 Equipment Security and Protection

- **Unattended Active Sessions** - If the computer system, workstation, or terminal to which a user is connected or using contains sensitive information, the user must not leave the computer system, workstation, or terminal unattended without logging out or invoking a password-protected screen saver.
- **Accepting Security Assistance from Outsiders** - Users must not accept any form of assistance to improve the security of their computers without first having the provider of this assistance approved by the Watco Information Security Team. This means that users must not accept offers of free consulting services, must not download free security software via the Internet, and must not employ free security posture evaluation web pages unless the specific provider of the assistance has been previously approved. If users are unsure whether a provider has been approved, the IT Help Desk and/or Information Security Team can be contacted for assistance.
- **Leaving Devices Unattended** – Watco provided devices must not be left unattended and unsecured in a public place.

In the event a technology device must be left in a personal vehicle, team members should make every effort to store the device out of sight. This can mean leaving technology devices in a locked trunk or compartment.

- **Data Privacy** - While Watco IT strives to provide a reasonable level of privacy; users of the company's technology systems should be aware that data created on corporate systems remains the property of Watco and should be handled appropriately.

5. Policy Enforcement

5.1 Violations of Policy

- Any violation of this policy may result in disciplinary action, up to and including termination of employment. Watco reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Watco does not consider conduct in violation of this policy to be within a Team Member's or partner's course and scope of employment, or the direct consequence of the discharge of the Team Member's or partner's duties. Accordingly, to the extent permitted by law, Watco reserves the right not to defend or pay any damages awarded against Team Members or partners that result from violation of this policy.
- Any Team Member or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager, or the People Services Department as soon as possible.

5.2 Exceptions to Policy

- All exceptions to this policy in part, or as a whole, must be approved by People Services and/or Watco Information Security. Any exceptions granted will be documented and shared among the appropriate parties.
- Exceptions to any single part of this policy does not constitute exception to the policy as a whole.