# IT ACCEPTABLE USE POLICY

## OVERVIEW

The intention for publishing an acceptable use policy is not to impose restrictions that are contrary to Mister Car Wash's established culture of openness, trust, and integrity. The company is committed to protecting Mister Car Wash and its employees and partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/intranet/extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, and network accounts providing electronic mail, internet browsing, and file transfers are the property of Mister Car Wash. These systems are to be used for business purposes in serving the interests of the company and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Mister Car Wash employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and conduct their activities accordingly.

This policy is based on the standard template issued by the SANS Institute, a cooperative research and security education organization (https://www.sans.org).

## PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at Mister Car Wash. These rules are in place to protect the employee and Mister Car Wash. Inappropriate use exposes Mister Car Wash to risks, including virus attacks, compromise of network systems and services, and legal issues.

## SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Mister Car Wash business or interact with internal networks and business systems, whether owned or leased by Mister Car Wash, the employee, or a third party. All employees, contractors, consultants and other workers at Mister Car Wash and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Mister Car Wash policies and standards and local laws and regulations. Any exceptions to this policy are documented in the "Compliance" section.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Mister Car Wash, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Mister Car Wash.

## POLICY STATEMENT

### General Use and Ownership

Mister Car Wash proprietary information stored on electronic and computing devices, whether owned or leased by Mister Car Wash, the employee, or a third party, remains the sole property of Mister Car Wash. Employees must ensure through legal or technical means that proprietary information is protected.

Employees have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Mister Car Wash proprietary information.

Employees may access, use, or share Mister Car Wash proprietary information only to the extent that it is authorized and necessary to fulfill employees' assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of internet/intranet/extranet systems. In the absence of such policies, and if there is any uncertainty, employees should consult their supervisor or manager.

For security and network-maintenance purposes, authorized individuals within Mister Car Wash may monitor equipment, systems, and network traffic at any time.

### Security and Proprietary Information

System-level and user-level passwords must comply with the *IT Password Policy* (IT.4205-MCW-POL). Providing access to another individual, either deliberately or through failure to secure access, is prohibited.

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 or fewer minutes. Employees must lock the screen or log off when the device is unattended.

Postings by employees from a Mister Car Wash email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Mister Car Wash unless posting is in the course of business duties.

Employees must use extreme caution when opening attachments in emails received from unknown senders because such attachments may contain malware.

### Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Mister Car Wash authorized to engage in any activity that is illegal under local, state, federal, or international law while using Mister Car Wash-owned resources.

The lists below are by no means exhaustive. They are an attempt to provide a framework for activities which fall into the category of unacceptable use.

**System and Network Activities**

The following activities are strictly prohibited unless otherwise noted.

- Violating the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property or similar laws or regulations, including, but not limited to, installing or distributing "pirated" or other software products that are not appropriately licensed for use by Mister Car Wash.
- Copying copyrighted material without authorization. Such copying includes, but is not limited to, digitization and distribution of copyrighted music and photographs from magazines, books, or other copyrighted sources. Installing copyrighted software for which Mister Car Wash or the end user does not have an active license is strictly prohibited.
- Accessing data, a server, or an account for any purpose other than conducting Mister Car Wash business, even if employees have authorized access, is prohibited.
- Exporting software, technical information, and encryption software or technology in violation of international or regional export control laws is illegal. The appropriate management should be consulted prior to exporting any material that is in question.
- Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Revealing an employee's account password to others or allowing use of an employee's account by others. This includes family and other household members when work is being done at home.
- Using a Mister Car Wash computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Mister Car Wash account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient and logging into a server or account that the employee is not expressly authorized to access unless these actions are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless prior notification to Mister IT is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on the Mister Car Wash network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command or sending messages of any kind with the intent to interfere with or disable a user's terminal session via any means, locally or via the internet/intranet/extranet.
- Providing information about, or lists of, Mister Car Wash employees to parties outside Mister Car Wash without a valid business need and explicit permission.

**Email and Communication Activities**

When using company resources to access and use the internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

- Sending unsolicited email messages, including "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Using without authorization or forging email header information.
- Soliciting email addresses, other than that of the poster's account, with the intent to harass or collect replies.
- Creating or forwarding "chain letters" and "Ponzi" or other "pyramid" schemes of any type.
- Using unsolicited email originating from within Mister Car Wash's networks of other internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by Mister Car Wash or connected via Mister Car Wash's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

**Blogging and Social Media**

- Blogging by employees, whether using Mister Car Wash's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of Mister Car Wash's systems to engage in blogging is acceptable provided that it is done in a professional and responsible manner, does not otherwise violate Mister Car Wash's policy, is not detrimental to Mister Car Wash's best interests, and does not interfere with an employee's regular work duties. Blogging from Mister Car Wash's systems is also subject to monitoring. Mister Car Wash's restrictions on the use of proprietary information also applies to blogging. As such,

employees engaged in blogging are prohibited from revealing any Mister Car Wash confidential or proprietary information, trade secrets, or any other material covered by this policy.

- Employees shall not engage in any blogging that may harm or tarnish the image, reputation, and/or goodwill of Mister Car Wash and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments and engaging in any conduct prohibited by Mister Car Wash's *Equal Opportunity and Anti-Harassment Policy* when blogging.
- Employees may also not attribute personal statements, opinions, or beliefs to Mister Car Wash when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Mister Car Wash. Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to handling and disclosing copyrighted or export-controlled materials, Mister Car Wash's trademarks, logos, and any other Mister Car Wash intellectual property may also not be used in connection with any blogging activity.

### Compliance

Mister IT will verify compliance to this policy through various methods, including, but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Any exceptions to this policy must be approved by the IT Department in advance.

An employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

## DEFINITIONS

The following definitions of terms can be found in the SANS glossary (https://www.sans.org/security-resources/glossary-of-terms/):

- Blogging
- Honeypot
- Honeynet
- Spam

## RELATED POLICIES, PROCEDURES, AND FORMS

- *IT Password Policy* (IT.4200-MCW-POL)
- *Acceptable Use Acknowledgement* (IT.4000.1-MCW-FRM)

## REVIEW

This policy will be reviewed **annually** and updated as necessary.

| Name and Title | Date (YYYY-MM) |
|---|---|
| Lauren Babson, Vice President of Information Technology | 2021-02 |

## APPROVAL

Only a representative from the Policy Review Committee can approve a policy following the procedure set forth in GRC.1000.1-MCW-PRC.

| Name, Title, and Signature | Date (YYYY-MM) |
|---|---|
| *Lauren Babson*<br>Lauren Babson, Vice President of Information Technology | 2021-02 |

## HISTORY

| Version | Issue Date | Updated by | Revisions |
|---|---|---|---|
| Rev. 3 | 2021-02 | Lauren Babson | Removed reference to nonexistent “Audit Policy”. Updated “Related Standards” section. Altered references to Mister IT. |
| Rev. 2 | 2018-07 | Jeff Parry | Modification made to “Security and Proprietary Information” (10 minutes to 15 minutes). |
| Rev. 1 | 2017-03 | Jeff Parry | Document created. |