

Acceptable Use Policy

Revision: *Initial Release*

Effective: 2026-01-05



UNCONTROLLED COPY: ALWAYS VERIFY REVISION

<https://itservices.machspec.com/policies>

1 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and other electronic devices at Machine Specialties. These rules are in place to protect both the employee and Machine Specialties. Inappropriate use exposes Machine Specialties to cyber risks including but not limited to ransomware, compromise of network systems and services, data breach, and legal issues.

2 Scope

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

5.2

This policy applies to employees, contractors, consultants, temporary, and other workers at Machine Specialties, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Machine Specialties.

3 Definitions

Disruption

An unplanned event that causes an information system to be inoperable for a length of time

Honeypot

A decoy computer system or network set up to attract and trap hackers, malware, or other cyber threats. It mimics real systems but contains intentionally vulnerable software or weak security configurations to simulate easy targets. The purpose of a honeypot is to monitor, study, and analyze the activities of attackers without affecting the actual production networks.

Honeynet

A network of honeypots designed to lure, detect, and analyze cyber-attacks. It emulates a complete internet infrastructure with multiple systems, applications, and services to create a realistic environment that can attract attackers seeking to infiltrate networks for malicious purposes.

Proprietary Information

Any confidential and secretive business information that gives an organization a competitive advantage. This may include trade secrets, patents, formulas, patterns, compilations, programs, methods, techniques, processes, financial data, or any other proprietary business information developed or obtained by a company.

Ransomware

A type of malicious software that encrypts the victim's files and demands payment (ransom) from the user to decrypt them and restore access. This cyberattack often uses social engineering tactics to trick users into opening infected email attachments or clicking on malicious links.

Security breach

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially

accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose.

Spam

Unsolicited and unwanted electronic messages that are sent indiscriminately to many recipients. These messages can be sent via email, social media platforms, instant messaging systems, or other communication channels. Common types of spam include promotional content, phishing scams, and malware distribution attempts.

UNCONTROLLED COPY: ALWAYS VERIFY REVISION

<https://itservices.machspec.com/policies>

4 Policy

4.1 General Use and Ownership

4.1.1

Machine Specialties' proprietary information stored on electronic and computing devices whether owned or leased by Machine Specialties, the employee or a third party, remains the sole property of Machine Specialties. Employees must ensure through legal or technical means that proprietary information is protected in accordance with the Security Policy.

4.1.2

Employees have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Machine Specialties' proprietary information.

4.1.3

Employees may access, use or share Machine Specialties' proprietary information only to the extent it is authorized and necessary to fulfill their assigned job duties.

4.1.4

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, employees should be guided by organizational policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5

For security and network maintenance purposes, authorized individuals within Machine Specialties may monitor equipment, systems, and network traffic at any time, per the Cybersecurity Policy.

4.1.6

Machine Specialties reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1

All mobile and computing devices that connect to the internal network must comply with the Cybersecurity Policy.

4.2.2

All authentication methods must comply with the Cybersecurity Policy. Providing access to another individual, either deliberately or through failure to secure access, is prohibited.

4.2.3

Employees must use extreme caution when engaging with unknown senders. Any links or attachments they send could be malicious.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during 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 Machine Specialties authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Machine Specialties-owned resources.

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

4.3.1 System and Network Activities

1. Violations of 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, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Machine Specialties.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Machine Specialties or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting Machine Specialties business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.
5. Employees are not permitted to use their personal system as a communication channel between non-company and company affiliated electronic devices.
6. Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
7. Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
8. Using a Machine Specialties 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.
9. Making fraudulent offers of products, items, or services originating from any Machine Specialties account.

10. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
11. Effecting security breaches or disruptions of network communication.
12. Port scanning, security scanning, or penetration testing, is expressly prohibited unless authorized by the IT department.
13. 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.
14. Circumventing user authentication or security control of any host, network, or account.
15. Introducing honeypots, honeynets, or similar technology on the Machine Specialties network unless this activity is a part of the employee's normal job/duty.
16. Intentionally disrupting another user's authorized computer activities, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Machine Specialties employees to parties outside Machine Specialties.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, employees must realize they represent the company. Whenever employees state an affiliation with the company, they must also clearly indicate that the opinions expressed are strictly their own and not necessarily those of Machine Specialties. Questions may be addressed to the IT or HR Department.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Machine Specialties' networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Machine Specialties or connected via Machine Specialties' network.

4.3.3 Blogging and Social Media

1. Blogging or posting to social media platforms by employees, whether using Machine Specialties' 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 Machine Specialties' systems to engage in blogging or other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Machine Specialties' policy, is not detrimental to Machine Specialties' best interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from Machine Specialties' systems is also subject to monitoring.
2. Machine Specialties' Cybersecurity policy also applies to blogging. As such, Employees are prohibited from revealing any Machine Specialties confidential or proprietary information, trade secrets or any other material covered by Machine Specialties' Cybersecurity Policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Machine Specialties and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Machine Specialties Human Resources policies.
4. Employees may also not attribute personal statements, opinions or beliefs to Machine Specialties 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 Machine Specialties. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Machine Specialties' trademarks, logos and any other Machine Specialties intellectual property may also not be used in connection with any blogging or social media activity

5 Policy Compliance

5.1 Compliance Measurement

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

5.2 Exceptions

Any exception to the policy must be approved by the IT department in advance.

6 Enforcement

The acceptable use policy is enforced by the Director of IT or designated individual. Noncompliance and violations to this policy will be dealt with according to the sanctions policy.

7 History

Date of Change	Revision	Responsible	Summary of Change
2025-12-10	-	Owen Jacobs	Initial release