International Plastic Modelers Society/USA

Information Security and Acceptable Use Policy

Created November 17, 2024

1. Overview

The International Plastic Modeler Society- USA Branch (IPMS/USA) is committed to protecting our volunteers, consultants, partners and the society from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP are the property of IPMS//USA. These systems are to be used for business purposes in serving the interests of the society, and of our members and partners during normal operations.

Effective security is a team effort involving the participation and support of every IPMS/USA volunteer and consultant (Team Member) who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and other electronic devices at IPMS/USA. These rules are in place to protect the Team Members and IPMS/USA. Inappropriate use exposes IPMS/USA to cyber risks including virus attacks, ransomware, compromise of network systems and services, data breach, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct IPMS/USA business or interact with internal networks and business systems, whether owned or leased by IPMS/USA, the Team Member, or a third party. All volunteers, contractors, consultants, temporary, and other workers at IPMS/USA are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in

accordance with IPMS/USA policies and standards and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to volunteers, contractors, consultants, temporaries, and other workers at IPMS/USA, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by IPMS/USA.

4. Policy

1.1 General Use and Ownership

IPMS/USA proprietary information stored on electronic and computing devices whether owned or leased by IPMS/USA the Team Member or a third party, remains the sole property of IPMS/USA. You must ensure through legal or technical means that proprietary information is protected from loss or misuse.

4.1.1 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of IPMS/USA proprietary information.

4.1.2 You may access, use or share IPMS/USA proprietary information only to the extent it is authorized and necessary to fulfill your assigned position duties.

Team Members are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, Team Members should consult the Executive Board (EBoard).

4.1.3 For security and network maintenance purposes, authorized individuals within IPMS/USA may monitor equipment, systems, and network traffic at any time.

4.1.4 IPMS/USA 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 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.2 All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.3 Postings by Team Members from an IPMS/USA email address to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of IPMS/USA, unless posting is during business duties.

4.2.4 Team Members must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Team Members 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 a Team Member of IPMS/USA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing IPMS/USA 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

The following activities are strictly prohibited, with no exceptions:

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 IPMS/USA.
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 IPMS/USA 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 IPMS/USA 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 export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
6. 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.

7. Using an IPMS/USA 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.
8. Making fraudulent offers of products, items, or services originating from any IPMS/USA account.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the Team Member is not an intended recipient or logging into a server or account that the Team Member is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to the EBoard is made.
11. Executing any form of network monitoring which will intercept data not intended for the Team Member's host, unless this activity is a part of the Team Member's normal job/duty.
12. Circumventing user authentication or security of any host, network, or account.
13. Introducing honeypots, honeynets, or similar technology on the IPMS/USA network.
14. Interfering with or denying service to any user other than the Team Member's host (for example, denial of service attack).
15. 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.
16. Providing information about, or lists of, IPMS/USA members or Team Members to parties outside IPMS/USA, except in the execution of assigned duties (e.g., the *Journal* mailing list provided to the printer).

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent IPMS/USA. Whenever Team Members state an affiliation to the society, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of IPMS/USA". Questions may be addressed to the EBoard.

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. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

1. Blogging or posting to social media platforms by Team Members, whether using IPMS/USA'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 IPMS/USA's 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 IPMS/USA's policy, is not detrimental to IPMS/USA's best interests, and does not interfere with a Team Member's regular work duties. Blogging or other online posting from IPMS/USA's systems is also subject to monitoring.
2. Team Members are prohibited from revealing any IPMS/USA confidential or proprietary information, trade secrets or any other confidential when engaged in blogging.
3. Team Members shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of IPMS/USA and/or any of its members. Team Members are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by IPMS/USA's Constitution and By-Laws.
4. Team Members may also not attribute personal statements, opinions, or beliefs to IPMS/USA when engaged in blogging. If a Team Member is expressing his or her beliefs and/or opinions in blogs, the Team Member may not, expressly, or implicitly, represent themselves as a representative of IPMS/USA. Team Members assume all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, IPMS/USA's trademarks, logos and any other IPMS/USA intellectual property also may not be used in connection with any blogging or social media activity.

2 Policy Compliance

2.1 Compliance Measurement

The EBoard 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 EBoard.

2.2 Exceptions

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

2.3 Non-Compliance

A Team Member found to have violated this policy may be subject to disciplinary action, up to and including termination of volunteer status or contract.

3 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam
- Ransomware

Revision History

Date of Change	Responsible	Summary of Change
November 17, 2024	EBoard	Initial policy approved.