North American Lighting, Inc.

A Koito Group Company

IT Acceptable Use Policy

Policy Number: PER-057

Effective Date: October 1, 2018

Revision Date: October 1, 2018

PURPOSE: The purpose of this policy is to establish guidelines governing Team Member use of Information Technology services provided by NAL or our clients.

PROCEDURES:

Acceptable Use

NAL's intentions for publishing this Acceptable Use Policy are not to impose restrictions that are contrary to its established culture of openness, trust and integrity. NAL is committed to protecting its Team Members, partners and the company 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, network accounts providing electronic mail, World Wide Web (WWW) browsing, and File Transfer Protocol (FTP), are the property of NAL. These systems are to be used for business purposes in serving the interests of the company, and of our customers during normal operations. Effective security is a team effort involving the participation and support of every NAL Team Member and its affiliates who deal with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

GENERAL USE & OWNERSHIP -

1. While NAL's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the company. Because of the need to protect NAL's network, management cannot guarantee the privacy of information stored on any network device belonging to NAL.
2. Team Members are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, Team Members should consult their supervisor or manager.
3. NAL recommends that any information that users consider sensitive or vulnerable be encrypted when not stored on NAL network shares. Portable storage devices (thumb drives) should only be used if they can encrypt stored information.

SYSTEM & NETWORK ACTIVITIES -

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
2. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by locking the system when unattended.
3. Because information contained on portable computers is especially vulnerable, special care should be exercised to prevent theft or corruption of data.
4. Postings by Team Members from an NAL email address to newsgroups or forums should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of NAL, unless posting is in the course of business duties.
5. All systems used by the Team Member that are connected to the NAL Internet/Intranet/Extranet, whether owned by the Team Member or the company., shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
6. NAL network storage should be used for business purposes only. Any files found to be on the network that violate this policy will be removed immediately.

MOBILE DEVICES -

This section provides standards and rules of behavior for the use of NAL provided and personally-owned smart phones and/or tablets to access NAL resources and/or services. Access to and continued use is granted on condition that each user reads, signs, respects, and follows NAL's policies concerning the use of these resources and/or services. This section is intended to protect the security and integrity of NAL's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

1. To prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.
2. The device must lock itself with a password or PIN if it's idle for up to five minutes.
3. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
4. Smartphones and tablets belonging to Team Members that are for personal use only are not allowed to connect to the network.
5. Team Members' access to company data is limited based on user profiles defined by IT and automatically enforced.
    a. The Team Member's device may be remotely wiped if:
    b. The device is lost, stolen, or replaced.
    c. The Team Member is voluntarily or involuntarily separated from the company.
    d. IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.
6. While IT will take every precaution to prevent the Team Member's personal data from being lost, in the event it must remote wipe a device it is the Team Member's responsibility to take additional precautions, such as backing up email, contacts, etc.
7. The company reserves the right to suspend services in the event a security threat is detected.
8. Lost, stolen, or replaced devices must be reported to the company within 24 hours. Team Members are responsible for notifying their mobile carrier immediately upon loss of a device.

9. The Team Member is expected to use his or her devices in a legal, and ethical manner at all times and adhere to the company's acceptable use policy.

The Team Member assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

Unacceptable Use

The following activities are, in general, prohibited. Team Members may be exempted from these restrictions during their legitimate job responsibilities. Under no circumstances is an Team Member of NAL authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing NAL 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.

SYSTEM & 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 NAL.
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 NAL or the end user does not have an active license is strictly prohibited.
3. 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.
4. Introduction of malicious programs into the network, server or any NAL owned equipment (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Using a NAL 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.
6. Making fraudulent offers of products, items, or services originating from any NAL account.
7. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
8. Limiting productivity by creating security breaches or disruptions of network communication.
    a. 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. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
9. Port scanning or security scanning is expressly prohibited unless prior notification to NAL is made to the IT Security Manager in writing.
10. Executing any form of network traffic 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.
11. Circumventing user authentication or security of any host, network or account.

12. Interfering with or denying service to any user other than the Team Member's host (for example, denial of service attack).
13. 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.
14. Providing information about, or lists of, NAL Team Members to parties outside NAL
15. Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers
16. Passing off personal views as representing those of the organization

EMAIL & COMMUNICATIONS ACTIVITIES -

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
2. Any form of harassment via email, telephone 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", or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within NAL's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by NAL or connected via NAL's network.

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

MONITORING -

1. For security and network maintenance purposes, authorized individuals within NAL may monitor equipment, systems and network traffic at any time.
2. The company maintains the right to monitor the volume of Internet and network traffic, together with the Internet sites visited. Team Members shall have no expectation of privacy regarding websites visited, and the specific content of any transaction may be monitored without notification. NAL reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. Specific information can be found in the IT Rules of Engagement policy.

ENFORCEMENT -

Internal Investigations into possible violations of NAL policies or the law may be conducted by appropriate company personnel, such as the IT Security Department, the Human Resources Department, or other authorized group or we may hire an authorized third party to conduct investigations. All Team Members are required to fully cooperate with and assist any investigation when requested to do so.

All terms and conditions as stated in this document are applicable to all users of NAL's systems, network, and Internet connection. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by NAL.

As with other policies, violation of this policy can subject you to disciplinary action, up to and including termination. Misuse of NAL's platform can also be considered criminal activity under the Computer Fraud and Abuse Act (CFAA), which protects private businesses' confidential and proprietary electronic business information against misappropriation, unauthorized access, exceeding authorized access, and/or access that impairs the integrity or availability of data, a program, a system, or information.

If you learn of any misuse of NAL's platform or any other related violations of company policy, we ask that you immediately notify a member of management, the Corporate Compliance Officer, Corporate HR Department, the Information Security Officer, or call the NAL Link Line at (217) 465-6666.