ACCEPTABLE USE POLICY
FOR NETWORK RESOURCES AND ELECTRONIC DEVICES

Overview

In order to protect Inspire Brands (otherwise "Inspire" or the "Company") and its employees, contractors, vendors, interns, volunteers, trainees, and other persons whose conduct is in the performance of work for the Company ("Team Members") from illegal or damaging actions by individuals, either unknowingly or knowingly, we have established the following Acceptable Use Policy ("AUP"). It is the Company's intent to balance our established culture of openness, trust, and integrity with establishing protections to safeguard our workplace.

The Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage, media, network accounts providing electronic mail, internet browsing, and File Transfer Protocol ("FTP") (collectively "Computing Resources") on equipment provided to the Company's Team Members are the property of Inspire. For personal mobile devices on which an employee is authorized to access the Company's email system, networks, or other electronic systems, the data and information contained on such devices that relates to and/or is obtained from the Company's email system, networks, or electronic systems ("Information Assets") are also considered part of the "Computing Resources." These Computing Resources are designated for Inspire's business purposes to serve the interests of the Company in the course of normal business operations.

Scope

Securing Inspire is a team effort involving the participation and support of every Team Member who deals with Inspire information and/or Computing Resources. Inspire Team Members must review and comply with this policy and conduct themselves accordingly. Please note that this policy is in place to protect both Team Members and the Company. Non-compliance with this policy exposes Inspire to risks including virus attacks, compromise of network systems/services, and potential legal issues. All Team Members are responsible for complying with this policy and any applicable laws and regulations.

This policy applies to everyone who accesses Inspire data or computing resources (including, but not limited to, all staff, visitors, vendors, contractors, volunteers, and business partners). This standard applies to all users of Inspire information globally.

Policy

A. General Use and Ownership

1. Inspire Computing Resources are to be primarily used for business purposes. Team Members are responsible for exercising good judgment regarding the reasonableness and appropriateness of personal use of the Inspire Computing Resources in accordance with Company policies, standards, and guidelines. Inspire Computing Resources must not be used for any unlawful or prohibited purpose.

2. Team Members have no expectation of privacy when using Inspire Computing Resources, even if the use is for personal use. Incidental personal use of email and the internet is permitted as long as (a) it does not distract from job responsibilities or create a situation that affects Inspire's reputation or business. and (b) follows relevant law and Inspire's ethics standards, policies, and procedures. Inspire trusts Team Members to be fair and sensible when judging what constitutes an acceptable level of personal use of the Company's information systems. If Team Members are uncertain, they should consult their managers.

3. Except as otherwise limited by law, Inspire has the right, but not the duty, to access, monitor, and review without notice all aspects of its Computing Resources and Information Assets, including, but not limited to, reviewing e-mail or other messages, and including personal communications that may need to be reviewed to determine whether they are related to Inspire's business. Some aspects of this standard affect areas governed by legislation in certain jurisdictions; in such cases, the need for local legal compliance has precedence over this guidance within the bounds of that jurisdiction. In these scenarios, local guidance must be developed to clarify how the standard is to be applied in that location.

4. Devices that interfere with other devices or users on the Inspire Computing Resources may be disconnected. Team Members are prohibited from actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources. Any data stored on the Computing Resources and any Information Assets may be disclosed to or used by Inspire for any authorized purpose.

5. Users are responsible for ensuring their security software and other software running on their corporate issued device(s)are kept current and in a supported state. Any concerns must be promptly reported to End User Support (eushelp@inspirebrands.com).

6. The use of devices listed on the FCC's Covered List that are deemed to pose an unacceptable risk to security, those devices identified by the Company to pose an unacceptable risk, and other such identified devices, especially those known to specifically pose security threats, are strictly prohibited from accessing Company Data Assets.[1]

[1] [1] List of Equipment and Services Covered by Section 2 of The Secure Networks Act. Sept. 2022. Published and maintained on the FCC's

B. User Identification and Passwords

1. Team Members are responsible for the security of data, accounts, and systems under their control and all activity that occurs on their account.

2. Keep passwords secure and do not share account or password information with anyone, including other personnel (including technology support teams), family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy. Compromised passwords must be reported to the Inspire Information Technology Department immediately by emailing Cybersecurity@inspirebrands.com.

3. Passwords must meet the minimum standards for Inspire and must be changed on a regular basis as outlined in the Access Control Policy. These standards must be met even if the system does not enforce the standard. If the system does not meet the standards, the user must use the features available to make as difficult as possible.

C. Unacceptable Use

The following activities are prohibited. The list below is by no means exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use.

1. Engaging in any activity that is illegal under applicable local, state, federal, or international law while utilizing Inspire Computing Resources.

2. Violating the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property laws, or similar laws or regulations, including, but not limited to, the installation, use, or distribution of "pirated" or other software products that are not appropriately licensed for use by Inspire.

3. Unauthorized copying of copyrighted material, including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, or copyrighted music (e.g., MP3s), and the installation of any copyrighted software for which Inspire does not have an active license.

4. Installing any unauthorized hardware or software, including shareware or freeware, on any of Inspire Computing Resources without first getting approval from the Inspire Information Technology Department.

website at https://www.fcc.gov/supplychain/coveredlist

5. Installing any software owned or licensed by Inspire on any computing resources or systems not owned by Inspire without first getting approval from the Inspire Information Technology Department.

6. Introducing malicious programs into the Inspire Computing Resources (e.g., computer viruses, worms, spyware, Trojan horses, rootkits, backdoors, etc.). Users must always guard against the risk of malicious programs being imported into Inspire's enterprise network by whatever means and must report any such actual or suspected infection immediately.

7. Using Inspire Computing Resources to actively engage in procuring or transmitting material that is in violation of any Inspire policy.

8. Making fraudulent offers of products, items, or services origination from any Inspire account.

9. Providing information about, or lists of, Inspire Team Members to unauthorized parties outside of Inspire.

10. Creating or forwarding email messages that can be defined or referred to as "junk mail," "SPAM," chain letter email, virus warnings, or other "pyramid" schemes or unauthorized advertising material. Specifically, chain email or virus warnings should be promptly reported to the Inspire Information Technology Department at Cybersecurity@inspirebrands.com and message(s) deleted.

11. Engaging in any form of harassment via email, texting, social media, telephone, or paging, whether through language, attachments, frequency, or message size or length.

12. Accessing or viewing any pornography, nudity, or similar illicit or inappropriate material.

13. Storing passwords or other identity information on any process, microcomputer, personal digital assistant, personal electronic device, or any magnetic or electronic media unless approved by the Inspire Information Technology Department.

14. Leaving any Inspire Computing Resource unattended while logged in, unless protected by a "password protected" screensaver.

15. Leaving any Inspire Computing Resource unattended and in plain sight, such as in the front seat of a car.

16. Circumventing user authentication or security of any of the Inspire Computing Resources.

17. Disabling or interfering with any Inspire-installed software including, but not limited to, anti-virus, VPN, Zscaler, logging, encryption, endpoint-management, or other security software.

18. Use of personal magnetic media, such as flash drives, disks, CDs, etc., on Inspire Computing Resources.

19. Tampering with Inspire Computing Resources for any reason.

20. Transferring information to or from an Inspire Computing Resource to a personal system without prior approval from the Inspire Information Technology Department.

21. Running or loading anything used to monitor network traffic, commonly used to spy on other network users and attempt to collect their passwords, i.e., "sniffers" or any other type of hacker- related software on Inspire Computing Resources without the prior approval of the Inspire Information Technology Department.

22. Downloading non-work-related MP3 music and video files, peer-to-peer software (i.e., Kazaa, Napster, etc.), or games onto Inspire Computing Resources.

23. Using personal or non-work-related streaming services on Inspire Computing Resources.

24. Use of Computing Resources to solicit for any purpose, personal or otherwise, without Inspire's consent.

25. Disabling or interfering with any Inspire-installed software including, but not limited to, anti-virus, VPN, Zscaler, logging, encryption, endpoint-management, or other security software.

26. Forwarding corporate emails to personal accounts.

D. Requesting Approval from the Inspire Information Technology Department

Inspire Information Technology Department approval involves submitting a formal request through the approved ticketing system to the Information Technology Helpdesk and receiving a reply indicating approval/acceptance or denial and following the standard change control process from within the Inspire Information Technology Department.

E. Termination of Employment

Upon termination of employment with Inspire for any reason, each individual shall immediately cease to use and return where applicable all Computing Resources, including but not limited to laptop computers, electronic files or documentation, access cards (e.g. building, phone, credit), mobile phones, and Company storage devices, and immediately cease accessing any Computing Resources, collaboration applications and online Company accounts.

F. Cooperation with Investigations

If requested by the Corporate Security, Legal, Compliance, Internal Audit, HR, Information Technology, or Cybersecurity departments, Team Members must provide their Computing Resources and/or personally owned technology containing Information Assets (e.g., USB drive, Camera, Smartphone, tablet, Personal computer) for inspection and possible copying, review, and use of its contents. Each Team Member will provide those requested devices without modifying or deleting any data on the devices. The Team Member will be required to provide any corresponding passwords that might be required to open the devices or applications therein. In such instances, the devices and their contents may be provided or disclosed to third-party service providers working on behalf of Inspire, such as attorneys or information technology professionals. The contents also may be disclosed to other third parties at the direction or upon request of a court, government agency, or law enforcement agency, or otherwise as authorized by law. Some aspects of this standard affect areas governed by legislation in certain jurisdictions; in such cases, the need for local legal compliance has precedence over this guidance within the bounds of that jurisdiction. In these scenarios, local guidance must be developed to clarify how the standard is to be applied in that location.

G. Enforcement

Failure to comply with this policy may result in disciplinary action up to and including termination.

_____ _____

Contractor Signature Date