JOE & THE JUICE

Acceptable Use of IT Equipment

Policy

Effective 2023

INTRODUCTION AND PURPOSE

This procedure and applicable supporting documents are designed to provide Joe & The Juice with a documented and formalized Acceptable Use of IT Equipment Policy

This policy and supporting procedures encompass all IT-system components owned, operated, maintained, and controlled by Joe & The Juice and all other internal and external system components that interact with these systems and all other relevant systems.

Responsibility

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a genuine commitment from all personnel, including management, internal employees, and users of system components, along with vendors, contractors, and other relevant third parties.

Additionally, by being aware of one's roles and responsibilities as it pertains to Joe & The Juice information systems, all relevant parties help to promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's world of growing cybersecurity challenges.

Responsibilities	Responsible
DEPARTMENT MANAGERS (where applicable)	**Awareness and training in procedures**
Joe & The Juice R&D Leadership	**Control and compliance with policy.**
Joe & The Juice Cybersecurity Group	**Yearly review & Policy Approval**
Joe & The Juice Employee	**Comply with policy**

Penalties

Failure to comply with this procedure by the Joe & The Juice staff may entail applying the corresponding measures established by current labor legislation. In the case of third-party personnel, the measures stipulated in the corresponding contract shall apply.

In addition, any user who detects a breach of any security control must communicate the fact through established channels. To this end, an Information Security incident management procedure must be followed and will be adequately communicated to all personnel.

Reviews

The document shall enter into force unless otherwise indicated, on the day of its approval and shall remain valid until it is modified or revoked in a subsequent document.

The document may be repealed in whole or in part by the competent area that approved them and in a subsequent document that expressly so states in a repealing provision.

The document will be reviewed at least once a year.

Exceptions

Exceptions to this policy are likely to occur. Requests for exception must be made in writing and must contain:

1) The reason for the request,
2) Risk to Joe & The Juice of not following the written policy,
3) Specific mitigations that will not be implemented,
4) Technical and other difficulties, and
5) Date of review.

Acceptable Use of IT Equipment Policy

Purpose

Defines acceptable use of equipment and computing services and the appropriate employee security measures to protect the organization's corporate resources and proprietary information.

Joe & The Juice Cyber Security Group's intentions for publishing an Acceptable Use Policy are not to impose restrictions contrary to Joe & The Juice's established culture of openness, trust, and integrity. Joe & The Juice is committed to protecting Joe & The Juice's employees, 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, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Joe & The Juice. These systems are to be used for business purposes to serve the company's interests and our clients and customers during normal operations.

Effective security is a team effort involving the participation and support of every Joe & The Juice employee and affiliate 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.

General Use and Ownership

Joe & The Juice proprietary information stored on electronic and computing devices whether owned or leased by Joe & The Juice, the employee or a third party, remains the sole property of Joe & The Juice. You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Joe & The Juice proprietary information.

You may access, use, or share Joe & The Juice proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. The corporate IT department are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. If there is any uncertainty, employees should consult their supervisor or manager.

For security and network maintenance purposes, authorized individuals within Joe & The Juice may monitor equipment, systems, and network traffic at any time, per Corporate IT *Audit & Log Management Policy*.

Joe & The Juice reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. System level and user level passwords must comply with the *Account & Credentials Management Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
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.
3. Postings by employees from a Joe & The Juice 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 Joe & The Juice unless posting is during business duties.
4. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

Unacceptable Use

1. 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).
2. Under no circumstances is an employee of Joe & The Juice authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Joe & The Juice owned resources.
3. 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 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 Joe & The Juice
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 Joe & The Juice 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 Joe & The Juice 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. 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 a Joe & The Juice 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 Joe & The Juice account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. 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 or logging into a server or account that the employee 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.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Cybersecurity Group is made.
12. 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.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the Joe & The Juice network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. 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.
17. Providing information about, or lists of, Joe & The Juice employees to parties outside Joe & The Juice

Email and Communication Activities

1. When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation with the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to Corporate IT & HR.
2. 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).
3. Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages.
4. Unauthorized use, or forging, of email header information.
5. 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.
6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
7. Use of unsolicited email originating from within Joe & The Juice networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Joe & The Juice or connected via Joe & The Juice's network.
8. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and social media

1. Blogging or posting to social media platforms by employees, whether using Joe & The Juice’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 Joe & The Juice’s systems to engage in blogging or other online posting is acceptable, if it is done in a professional and responsible manner, does not otherwise violate Joe & The Juice’s policy, is not detrimental to Joe & The Juice’s best interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from Joe & The Juice’s systems is also subject to monitoring.
2. Joe & The Juice’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Joe & The Juice confidential or proprietary information, trade secrets or any other material covered by Joe & The Juice’s Confidential Information 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 Joe & The Juice 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 Joe & The Juice’s *Code of Conduct Policy*.

4. Employees may also not attribute personal statements, opinions or beliefs to Joe & The Juice 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 Joe & The Juice. Employees assume all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Joe & The Juice's trademarks, logos and any other Joe & The Juice intellectual property may also not be used in connection with any blogging or social media activity – unless this is part of the employees' normal responsibilities.

Employee Equipment Issuance

1) Corporate IT is responsible for issuing hardware based on the specific requirements and role of the user. The equipment will be issued upon commencement of employment or role change that necessitates a change in equipment.
2) As part of our efforts to ensure efficiency, uniformity, and ease of IT support, Joe & The Juice has standardized on Windows machines for most roles. Windows machines offer the versatility, compatibility, and robustness needed for most of our operations.
3) Mac machines will be issued only to employees whose roles specifically require them. This includes developers working on iOS development and employees with specific graphic-intensive roles. Justification for the use of a Mac machine must be provided and approved by the Corporate IT department.
4) If an employee currently using a Mac machine requires a new machine and their role does not meet the above criteria, a Windows machine will be issued. This is to maintain our standardization policy and ensure efficient allocation and support of IT resources.

Return of IT Equipment

Upon termination or change of employment, all company-issued IT equipment must be returned to the IT department in a timely manner. Before returning, employees should ensure that all personal data has been removed and the device has been restored to its original state, where possible.

Please note, Joe & The Juice does not sell used IT equipment to employees or external parties. All hardware, regardless of age or condition, must be returned to the IT department. This policy is in place to maintain our IT assets and ensure proper disposal or repurposing of equipment in line with company and environmental guidelines.

Laptop Protection, Security, and employee liability

Policies must be in place to protect issued laptops from physical damage and theft. Polices should include:

1) General
    a) Power off your laptop whenever it is not in use.
    b) Keep your laptop close to you and in sight whenever possible. When it's not, store it securely.
    c) Never store passwords with your laptop or in its carrying case.
    d) Separate other forms of user authentication from your laptop at all times.
    e) Avoid travelling with your laptop if it's not necessary.
    f) Do not place drinks or food in close proximity to your laptop.

2) While at the Office
    a) When away from your desk, leave your laptop in a locked and secure location.
    b) If you need to step away from your laptop, ensure that it is locked or requires login upon return.
3) While Traveling In a Personal or Rental Car
    a) Extreme temperatures can damage a laptop. Do not leave a laptop in an unattended vehicle.
    b) If you must leave your laptop in an unattended vehicle for a short period of time, always lock it in the trunk. A visible laptop is a target.
    c) In the rare case when a vehicle does not have a trunk or lockable compartment, the laptop should still be locked in the vehicle and stored out of sight.
4) In Hotels
    a) Never leave your laptop unattended in hotel rooms.
    b) Secure your laptop in the room safe when you leave your room. If a room safe is too small or unavailable, lock your laptop in your travel luggage.
    c) Store the carry case and peripherals, such as a mouse and a charger, in your travel luggage.
5) While Traveling by Air
    a) Always carry your laptop with you; only place your laptop in checked baggage if required by the airline or airport security.
    b) If required to place your laptop in checked luggage, wrap it in soft foam or bubble wrap to cushion it. If possible, pack your laptop in luggage rather than your briefcase to make it less conspicuous to thieves.
    c) Beware of staged delays at security checkpoints, a tactic often used by thieves. Don't send your laptop through the screening devices until you are about to pass through the checkpoint. Always keep your laptop close to you. If an overhead compartment within an unobstructed view is not available, consider placing your laptop underneath the seat in front of you.
6) Proper Laptop Care and Liability
    a) Padded Case: Always transport your laptop in a padded case to prevent damage from shocks and falls. The case should be specifically designed for laptops and fit your machine properly.
    b) Avoid Water Damage: Do not keep any kind of liquids near your laptop inside the bag. Spilled drinks can cause serious damage to the laptop and loss of data. Always make sure your laptop and its case are in a dry environment.
7) Employee Liability: Employees are expected to take all reasonable measures to prevent damage to or theft of their company-issued laptops. This includes adherence to all guidelines outlined in this policy. If a laptop is damaged or stolen, and it is determined that the employee did not adhere to these guidelines, the employee may be held liable for the cost of repair or replacement.