Fillosophy Acceptable Use Policy

Overview

The IT/Web Design department is responsible for the upkeep and management of the company's website, which includes the building and support of the website itself and maintaining the website to keep up with state guidelines. This Acceptable Use Policy covers the security and utilization of all (Fillosophy's) data and IT hardware. It incorporates the utilization of email, web, voice and versatile IT hardware. This strategy applies to all (Fillosophy's) representatives, temporary workers and specialists (in the future alluded to as 'people'). All employees are aware and consent all statements and guidelines outlined in this document upon hire.

Purpose

The purpose of the IT department's is the enhancement of technology, creation and upkeep of the company website as well as other technological contributions and input. The IT department will consist of 3 well versed team members who will maintain the website and the overall company security to uphold guidelines. Web design and security are a crucial part of any business because it impacts how our customers look at our brand and taking steps to avoid unnecessary security risk. Our priority is the impression that we make on our customers to feel secured and have the best experience. The motivation behind this approach is to layout the satisfactory utilization of PC hardware at expectations. These principles are set up to secure the representative and unseemly use opens to hazards including infection assaults, bargain of organization frameworks and administrations, and lawful issues.

Scope

Digital marketing and cybersecurity are the keys to uphold any business virtually. In digital marketing, the scope of the media department contains promoting and branding through digital media. With cybersecurity training, we're able to inform and teach our employees to be responsible for upkeep of security, learning practices to identify issues for technical support to address, and to avoid possible threats of breaches. With educated employees, we're able to keep this company safe, secure, with the appropriate use of every individual satisfying government business ordinances and regulations. This strategy applies to the utilization of data, electronic and registering gadgets, and network assets to direct Fillosophy business or connect with interior organizations what's more, business frameworks, regardless of whether claimed or rented by Fillosophy, the representative, or a third party. All representatives, temporary workers, specialists, transitory, and different laborers at plans and its auxiliaries are answerable for practicing trustworthiness with

respect to suitable utilization of data, electronic gadgets, and organization assets in agreement with approaches and norms, and nearby laws and guidelines. This arrangement applies to workers, temporary workers, specialists, substitutes, and other laborers at Fillosophy, incorporating all staff subsidiaries with outsiders. This approach applies to all hardware that is possessed or rented by Fillosophy.

General Use and Ownership

1. Expectations exclusive data put away on electronic and processing gadgets regardless of whether possessed or rented by Fillosophy , the representative or an outsider, remains the sole property of Fillosophy. You should guarantee through lawful or specialized implies that restrictive data is ensured as per the Data Insurance Standard.
2. You have an obligation to expeditiously report the robbery, misfortune or unapproved exposure of Fillosophy exclusive data.
3. You may access, use or offer Fillosophy exclusive data just to the degree it is approved and important to satisfy your relegated work obligations.
4. Representatives are answerable for practicing decision making ability with respect to the sensibility of individual use. Singular offices are liable for making rules concerning individual utilization of Internet/Intranet/Extranet frameworks. Without such approaches, workers should be guided by departmental approaches on close to home use, and if there is any vulnerability, representatives ought to counsel their administrator or chief.
5. For security and organization upkeep purposes, approved people inside Fillosophy may screen gear, frameworks and organization traffic at any time, per Infosec's Audit Policy.
6. Aims claims all authority to review organizations and frameworks on an intermittent premise to guarantee consistent with this approach.

System and Network Activities

The Fillosophy systems and networks are all facilitated by the IT department. Our security systems and everything visible on the website should be up to date at all times and will be maintained to keep up status. Network activities for all employees should only contain that meant to its intended uses on company networks.
The accompanying exercises are carefully disallowed, without any exemptions:

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 InTents.

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 InTentsor the end user does not have an active license is strictly prohibited.

Accessing data, a server or an account for any purpose other than conducting Fillosophy business, even if you have authorized access, is prohibited.

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.

Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

Using an Fillosophy 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.

Making fraudulent offers of products, items, or services originating from any Fillosophy account.

Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

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, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.

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.

Circumventing user authentication or security of any host, network or account.

Introducing honeypots, honeynets, or similar technology on the network.

Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, by any means, locally or via the Internet/Intranet/Extranet.

Providing information about, or lists of InTents employees to parties outside of Fillosophy.

Account's Security: In Regard to Individual Responsibility

In order for individuals to login into their account, it is necessary to have a username and a password which are assigned upon hire. Individuals are responsible for any action from your own account. If there is a change in any username or password for a Fillosophy employee's account, contact IT to ensure there's a backup due to possible misplacement, or you fail to recall either username or password in the future in order to fix that issue as soon as possible.

DO NOT:

- Share username or password to ANYONE
- Unsupervised a computer with your account open
- Use another account that does NOT belong to you

- Leaving your password where anybody can see it
- Manipulating any information or system belonging to Fillosophy without permission
- Any attempts of accessing data without permission
- Accessing outside of the system or data that was not agreed
- Connect an unauthorized device to Fillosophy system or network
- Save Fillosophy data or software on an unauthorized equipment
- Sharing data or software without permission

TIPS & MAINTENANCE:

- If you lose your username/password, contact the IT department for further instructions and guidance
- If you decide to change your username/password, please contact IT to ensure your data is stored safely, and access is granted if updates/backups, etc. are needed in the future

It is the line manager's responsibility to ensure all employees are aware of the instructions on restrictions to the Fillosophy system and data.

Employee's Responsibilities: Internet and Email Usage

The internet and email of Fillosophy are for business purposes only. In other words, any outside usage that breaks the agreement or is harmful towards your business performance, employees acknowledge that they will be let go from Fillosophy, and subsequent charges may follow, resulting in the intensity and seriousness of the offence.

Individuals will be responsible for their action on the Internet and in their email.

DO NOT:

- Harass or abuse using an email or the Internet
- Abuse the Internet or email to gain advantages that do not benefit Fillosophy
- Any obscene language or behavior
- Possess or share offensive or inappropriate data
- Using a personal email account as your business account
- Gamble using the email account that belongs to the company (including the email account that was provided to you for working purposes only)
- Sending an email that can harm the reputation of Fillosophy

- Post an official information or opinion as a Fillosophy employee about Fillosophy without permission
- Undertake as the company without approval
- Send unencrypted data (leading to cybersecurity risks)

- Unauthorize downloads of copyrighted sources
- Break terms of rights or property agreement
- Unauthorized downloads
- Use of Fillosophy's equipment and Fillosophy's Internet without proper connections

Unauthorised Access Out of Sight

Valuable data being in the open will increase the risk of information being in the wrong hands. In order to protect your personal information and data from unauthorized access, please keep this in mind.

Prevent Unauthorized Access:

- Use the provided security feature to prevent sensitive information leaks
- Unsupervised devices must have a screen lock with a password or be logoff from your account
- Do not leave sensitive material on printers or photocopy machines
- Discard business papers through a shredder or confidential waste bin.
- Use a secure wifi at all times(do NOT use public wifi): if this becomes an issue, please contact the IT department for assistance and possible wireless hotspots and connections
- All laptops must have a privacy filter if work is taken off the premises, or employees are involved with confidential projects

Outside of Workplace

Employees will still be held liable for your devices off-site.
Be Responsible:

- Continue to follow the policy out of the workplace
- Files and devices must be supervised in a public space and not be unsupervised in the car
- Laptops must be in your carry-on baggage throughout your travel
- All information and data must be encrypted and saved
- Any and all company property must be properly handled and protected

- Devices such as laptops, phones, and tablets are required to have protection against unauthorized access

Saving On Storage Devices

In a situation without Internet access, and with the responsibility to transfer data securely, you can use a portable storage device such as a USB stick, memory card, or disks to save your work. However, you must use an authorized storage device approved by Fillosophy provided from the IT department so the encryption confidential information is supervised and regulated.

Software and Viruses

Only software approved and installed by Fillosophy's IT department is allowed on any of the company's devices, including PCs, laptops, phones, cars, etc. Following the software's license agreement is required. Employees must never leave anything personal in the computer. All antivirus software will be uploaded to Fillosophy PCs and laptops and must not be tampered with nor be removed. Any action of this will be inspected and privileges can be revoked.

Voice Equipment Conditions of Use

Equipment belonging to Fillosophy uses are for intended business operations. Delivering or obtaining confidential or personal information using Fillosophy's equipment is prohibited unless permitted under special extenuating circumstances or certain officers. Any non-dire messages should be transmitted in a different way of communication at the individual's expense. The use of Fillosophy technology for private business, threatening calls to any individual internal or external, international calls (unless a vendor or customer approved by Fillosophy officers) is strictly prohibited.

Termination of Contract

With the termination/layoff/firing of an Fillosophy employee, all company equipment and devices must be returned. All devices will be checked out or lent to individuals in order to keep all products in check and to confirm all devices have been returned. Individuals will have up to 2 weeks prior to termination date to return all company property and accounts.Failure to return company property will result in legal action. Individuals must not withhold nor use any developments or information from your employment that belongs to Fillosophy.

Privacy and Investigation

Everything in Filiosophy's computers belongs to the company of Fillosophy. Fillosophy's equipment lacks privacy for the user. Filosophy will do their best to not view your personal email, however this is not guaranteed. Such as a situation in an investigation if there are suspicious activities of broken agreement. To keep the system secured and running smoothly, Fillosophy has the authority to view all of your activities on devices that belong to Fillosophy.
Must be read along with:

- Computer Fraud and Abuse Act (CFAA)

All employees are required to consent to the policy above, and will be provided their own copy in order to allow individuals to be aware of the terms and conditions of acceptable use on all company devices and systems.

If any technical support is necessary throughout the individual's time employed by Fillosophy, connection will be available to combat any malfunctions in devices and connections. All employees are made aware of this acceptable use policy and must comply with all statements and regulations above. Any acts (security breaches, misuse of data and security, misconduct) that are not prohibited will be taken into investigation, and disciplinary and/or legal action may follow.