IT Acceptable User Policy

2016

IT Acceptable User Policy

The purpose of this policy is to outline the acceptable use of computer equipment at the Company. These rules are in place to protect the employee and the Company. Inappropriate use exposes the Company to risks including virus attacks, compromise of network systems and services, and legal issues.

This policy applies to employees, contractors, consultants, temporaries, and other workers at the Company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Company.

General use and ownership
While the Company 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 the Company network, management cannot guarantee the confidentiality of information stored on any network device belonging to the Company. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. For security and network maintenance purposes, authorised individuals within the Company may monitor equipment, systems and network traffic at any time. The Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and proprietary information
Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every 30 days.

All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete) when the host will be unattended.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. If unsure do not open and refer to Directors.

Unacceptable use
The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of 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 an employee of the Company authorised to engage in any activity that is illegal under local, national or international law while utilising the Company's owned resources. The lists below are by no means exhaustive, but attempts 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:

- 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 the Company's 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.

- 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.
- Providing information about, or lists of, the Company employees to parties outside the Company.

Photography/Videos

- Should you have taken part in any events or trials or photography sessions for the company where you were photographed or filmed. Ownership of the copyright and right to use those images, pictures, items, videos, social media or any other image containing your details, picture or photo will remain the property of your employer and may be used even after your contract has been terminated, for whatever reason. Any use by the company includes being shown on the company website.

Email and communications activities

- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorised use, or forging, of email header information.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Internet acceptable use policy

- The Company recognises the business need for some, if not all of its employees to have access to the internet while on the job, using company computers. As such, the Company has made the business decision to make the internet available to employees for Company business purposes.
- The Company intends for the internet to be accessed for business purposes and expects that employees will spend no more than 30 minutes per day accessing the Internet for non-business purposes.
- The Company specifically prohibits its employees from accessing the following types of sites using company computers:

    - Gambling sites
    - Online gaming sites
    - Auction sites
    - Hate sites
    - Pornographic sites
    - Any site engaging in or encouraging illegal activity

The Company reserves the right to use monitoring software to make sure that the company's IAUP is being adhered to by its employees. The Company may record and/or monitor one or more employees' computer and internet activity for any reason and without specific notice.

Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.
FTP	File Transfer Protocol the transferring of files from one electronic device or server to another.
Virus	A damaging computer program that can replicate itself from computer to computer.
Mail Bomb	The sending of a massive amount of e-mail to a specific person or system.
Trojan horse	A program that has the ability to collect or destruct data.
Worm	A program that has the ability to collect or destruct data and can move form computer to computer without any user intervention.
Ponzi	*A Ponzi scheme is a* fraudulent investment operation that involves paying returns to investors out of the money raised from subsequent investors
Pyramid	A pyramid scheme is a system of selling goods where commissions are paid to recruit new sellers.

Monitoring and review of this policy

E-Mail's sent to the business are the property of the Company. We have the right to retrieve and monitor all emails together with all computer and internet usage if or whenever it may be considered appropriate. In monitoring any use or any staff we confirm compliance with all laws that regulate the use of computers, data protection and confidentiality.

The Directors shall be responsible for reviewing this policy annually and more frequently when changes are made in legislation to ensure that it meets legal requirements and best practice.