Acceptable Use Policy

ChilledWeb Limited

Policy Name:	Acceptable Use Policy	Policy Ref:	CWAUAP
Date of Last Revision:	07 January 2023	Version No:	1.3

Contents

Overview

The intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to ChilledWeb's established culture of openness, trust and integrity. ChilledWeb is committed to protecting their 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, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of ChilledWeb. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every ChilledWeb 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.

Purpose

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

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct ChilledWeb business or interact with internal networks and business systems, whether owned or leased by ChilledWeb, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at ChilledWeb are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with ChilledWeb policies and standards, and local laws and regulation.
This policy applies to employees, contractors, consultants, temporaries, and other workers at ChilledWeb, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by ChilledWeb.

Policy

General Use and Ownership

1. ChilledWeb proprietary information stored on electronic and computing devices whether owned or leased by ChilledWeb, the employee or a third party, remains the sole property of ChilledWeb.
2. You have a responsibility to promptly report the theft, loss or unauthorised disclosure of ChilledWeb proprietary information.
3. You may access, use or share ChilledWeb proprietary information only to the extent it is authorised and necessary to fulfil your assigned job duties.
4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments 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.
5. For security and network maintenance purposes, authorised individuals within ChilledWeb may monitor equipment, systems and network traffic at any time.
6. ChilledWeb 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 Password Construction 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 unique username and password. You must lock the screen or log off when the device is unattended.
3. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
4. All requests for manual creation, deletion and changes of user accounts and privileges must be carried out by the Director. Logs will be kept of all account creation/deletion/changes.
5. Postings by employees from a ChilledWeb email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of ChilledWeb, unless posting is in the course of business duties.
6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Elevated Privileges

1. With the exception to NIX-based systems; users whose work requires system administration access will be given a separate specialist account for this purpose, in addition to their standard user account. Users request for their own System Administrator accounts are subject to approval by a Director.
2. Users of NIX-based systems do not have the ability to have a separate system admin account but it is managed by additional permissions that can only be applied by a Director.
3. Users with elevated privileges will restrict their use of accounts with elevated privileges to only official ChilledWeb business consistent with the System Administrator's role, job responsibilities, and the purpose for which the access was granted. The permissible use of ChilledWeb Systems for incidental personal purposes does not extend to a System Administrator's use of elevated privileges. System Administrators may not use their elevated privileges for any purposes outside of the scope for which such elevated privileges were granted.
4. System Administration accounts are created and managed by a Director.
5. System Administration accounts will use the ChilledWeb Password Construction Policy.
6. System Administration accounts will be requested, by email to the Director.
7. The Director will maintain and review monthly an Excel spreadsheet of all users that have been awarded elevated privileges.
8. In all other ways, these system administration accounts should be managed and the user is responsible for them similarly to standard accounts. When a user logs into a system admin account for the first time they are mandated to change their password before being able to continue.
9. ChilledWeb Company Directors are responsible for taking action to remove user's Administrator account when they move roles.
10. System Administration accounts will automatically be disabled when the users' standard account becomes expired.

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 ChilledWeb authorised to engage in any activity that is illegal under local or international law while utilising ChilledWeb-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 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 ChilledWeb.
2. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which ChilledWeb 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 ChilledWeb business, even if you have authorised 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 export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. 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.
7. Using a ChilledWeb computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the users local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any ChilledWeb 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 authorised 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.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Directors is made.
12. Executing any form of network monitoring which will intercept data not intended for the employees host, unless this activity is a part of the employees normal job/duty.

13. Circumventing user authentication or security of any host, network or account.
14. Interfering with or denying service to any user other than the employees host (for example, denial of service attack).
15. 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.
16. Providing information about, or lists of, ChilledWeb employees to parties outside ChilledWeb.

Email and Communication Activities

When using company resources to access and use the Internet, users must realise they represent the company. Whenever employees state an affiliation to 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 the Directors.

1. 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).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorised 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", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within ChilledWeb's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by ChilledWeb or connected via ChilledWeb’s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and Social Media

1. Blogging by employees, whether using ChilledWeb’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 ChilledWeb’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate ChilledWeb’s policy, is not detrimental to ChilledWeb’s best

interests, and does not interfere with an employee's regular work duties. Blogging from ChilledWeb's systems is also subject to monitoring.

2. ChilledWeb's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any ChilledWeb confidential or proprietary information, trade secrets or any other material covered by ChilledWeb'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 ChilledWeb and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.
4. Employees may also not attribute personal statements, opinions or beliefs to ChilledWeb 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 ChilledWeb. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, ChilledWeb's trademarks, logos and any other ChilledWeb intellectual property may also not be used in connection with any blogging activity

Exceptions

Any exception to the policy must be approved by the Directors in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.