

Document Name	Acceptable Use Policy
Document Creation Date	02/11/2022
Document Created By	CISO-CSE
Version Control History	1.0
Document Reviewed Date	05/12/2024
Document Reviewed By	CISO & CRO
Document Approved By	Standing Committee on Technology

CSE Acceptable Use Policy

Overview:

An acceptable use policy (AUP) is a document stipulating constraints and practices that a user must agree to for access to a corporate network, the internet or other resources.

Objective:

From an information technology (IT) perspective, an AUP states what a user can and cannot do when using computers and computing resources. This applies whether the organization provides the device or it is a personal device that the user provides.

One of the benefits of an AUP is that it spells out acceptable and unacceptable employee behaviour and actions. AUPs also provide a company with a legal mechanism to compel compliance, and they describe penalties/penal actions for noncompliance.

Scope:

A disclaimer is often included in an AUP absolving the organization from responsibility for a data breach, malware or other issue. Statements about when a person is in violation of this policy and when law enforcement might be called in could also be included. The scope of this policy covers CSE as well as its subsidiary CCMPL.

Process:

A. This Acceptable Use Policy ("AUP") governs the usage of IT assets of The Calcutta Stock Exchange Ltd. (CSE) as well as its subsidiary company CCMPL for DP services.

B. This AUP shall be incorporated by default for all the employees of the Exchange and its subsidiary CCMPL

C. This AUP helps and protects the CSE, CCMPL and its Employees and Clients as a whole.

D. All hosting services provided by CSE shall be used by the Clients and Employees for lawful purposes only, and as per the applicable laws (including but not limited to privacy laws). Transmission, usage, storage, or presentation of any information, data or material in violation of applicable laws including the 'banned contents' is strictly prohibited. The 'banned contents' include, but are not limited to:-

1. **Illegal Material** - Includes illegally exploited copyrighted works, commercial audio, video, or music files, and any material that violates any applicable law or regulation of any country, and any material that is perceived to be misleading in any manner.
2. **Warez** - Includes, but is not limited to, pirated software, ROMS, emulators, phreaking, hacking, password cracking, IP spoofing and the like,

and encrypting of any of the above. It also includes any sites which provide "links to" or "how to" information about such material.

3. **HYIP** - HYIP sites, or sites that link to or have content related to HYIP sites.

4. **Proxy** - Any proxy set-ups or connections or any sort of activity through remote proxy connections on our hosting and/or in relation to our Colocation services.

5. **IRC Hosts** – (Hosting an IRC server that is part of or connected to another IRC network or server) Servers, found to be (1) connecting to or (2) part of these networks;

6. **Defamatory content** - any website content that makes a false claim, expressively stated or implied to be factual, or that may give an individual, business, product, services, group, government or nation a negative image.

7. **Bit Torrent** - Use of software and scripts for "bit torrents" including sending or receiving files using these mechanisms.

E. Adult Content:

CSE does not allow pornographic/child pornography or sexually-explicit images or any pictures/ video which are obtained illegally to be hosted on its servers.

F. Undertaking of the Employees and Clients

The Employees & Clients agrees and undertakes that;

1. Any attempt to undermine or cause harm to any of the servers of CSE is strictly prohibited.
2. In case of abuse of the resources provided by CSE, in any way, CSE reserves the unqualified right to immediately deactivate the Employees account
3. Denial of Service (DOS) attacks directed at CSE, or any attempt to launch a DOS attack from CSE servers are strictly prohibited. All infractions and or suspected infractions will be vigorously investigated and may result in immediate termination service.
4. CSE will use reasonable efforts to protect server for its clients / employees, The Employees and Clients are solely responsible for making back-up files in connection with its use of the Services.
5. Employees and Clients shall be responsible for any misuse of its Server/account, and it must take steps to ensure that others do not gain unauthorized access to its Server/account. It shall not use its account to breach the security of another account or server or attempt to gain unauthorized access to another network or server.
6. CSE will use commercially reasonable efforts to resolve all Incidents as soon as reasonably possible, but does not make any representations or warranties as to the timeliness of the resolution of any Incident.
7. Its password provides access to its account, and it is responsible to keep its password secure.
8. Sharing its password and user account access with unauthorized users is strictly prohibited. It will take care and prevent others from using its account. It will be responsible for all consequences of others using its account.
9. Attempting to obtain another user's account password is strictly prohibited, and will result in termination of Services.

10. It shall adopt adequate security measures to prevent unauthorized use of its account.
11. It shall not attempt to circumvent user authentication or security of any host, network or account which includes but is not limited to accessing data not intended for it, logging into or making use of a server or account. It is not expressly authorized to access, or probe the security of other networks. Use or distribution of tools designed for compromising security is prohibited. Such tools shall include but are not limited to password guessing programs, cracking tools or network probing tools.
12. It shall not attempt to interfere with services provided to any user, host or network or carry out DOS attacks which includes but is not limited to "flooding" of networks, deliberate attempts to overload a service, and attempts to "crash" a host.
13. Users who violate systems or network security may incur criminal or civil liability. CSE will cooperate fully with investigations of violations of systems or network security at other sites, including cooperating with law enforcement authorities in the investigation of suspected criminal violations.
14. It shall complete its own tests for computer viruses in accordance with best computing practice prior to each and every operational use of the Services.

G. Materials and Products

1. Connection speed represents the speed of connection to CSE and does not represent guarantees of available end to end bandwidth.
2. CSE is under no obligation to edit, review or modify the contents of the Clients' website. CSE shall not pro-actively monitor messages that are posted on the sites managed by CSE, but it reserves the right to remove such messages at its sole discretion, without notice to the Customer.
3. The first offence committed by the Clients' in respect of Proxy as set out in Clause D (4), above, will result in immediate suspension of their account. A second violation by the Client in this regard will result in immediate termination of its account and service.
4. Servers found to be (1) connecting to, or (2) part of, another IRC network or server will be immediately removed from CSE network, without notice. Such servers will not be reconnected to the network until such time that all traces of the IRC server are completely removed, and the Client allows access to its server to confirm that the content has been completely removed.

I. Network Misuse

1. All clients are allowed access to the public network and IP; however, misuse of the network and IP in any way, including interference, will result in a violation of this AUP. All violations of this AUP shall be subject to review by CSE, and an appropriate course of action shall be taken as determined by CSE in its sole discretion. Proper use of public network and IP must comply with all local, state, and Indian IT laws. Clients assume full liability for all content which they place on the server. Content displaying or transferring acts of copulation or exposed genitalia is prohibited, regardless of context. Forging any TCP/IP packet header or any part of the header information in any e-mail or newsgroup posting is deemed a violation of this AUP.

2. CSE assigns Clients an Internet Protocol address for Client's use, and to make server/service/Device accessible from public and local network, which hosted in CSE datacenter, IPs provided by CSE to the Client, for the same duration of service given by CSE to Client, Any activity performed by client or client's client or people/company of client, The Client will solely responsible.
3. CSE is providing IP for serving services to Employees/clients/companies, and for any unauthorised activities CSE is not responsible via allocated IPs.

J. Monitoring Policy

CSE Datacenter does not actively monitor the content on its servers. Dedicated server content will only be reviewed upon complaint. Content that does not violate local, state and Indian IT law or this AUP or the Terms of Service is deemed in compliance and shall remain intact. If content is deemed to be in violation of this AUP or the Terms of Service, it shall be reviewed by CSE, and a course of action shall be taken to correct the problem, which may result in termination of the account or service. To ensure lawful and valid use of CSE IP Addresses, CSE will continuously make efforts to monitor and keep tracks of network connection logs of all their TCP/IP Connections and IP addresses allotted to clients and employees

K. Usage Policy

1. **Spamming** via third-party proxy, aggregation of proxy lists, or installation of proxy mailing software. Configuration of a mail server to accept and process third-party messages for sending without user identification and authentication. Hosting web pages advertised within "spam e-mail" sent from another network ("spamvertising"). Hosting web pages or providing services that support spam. Any other unsolicited bulk messages, postings, or transmissions through media such as weblog posts, IRC/chat room messages, guestbook entries, HTTP referrer log entries, Usenet posts, pop-up messages, instant messages, or SMS messages. Instructing others in any activity prohibited by this AUP.
2. Operating CSE Service on behalf of, or in connection with, or reselling any service to persons or firms listed in the Spamhaus Register of Known Spam Operations database at www.spamhaus.org shall constitute a violation of this AUP.
3. **Block Removal** – If, as a result of a Customer's actions, CSE's mail servers or IP address ranges are placed on black hole lists or other mail filtering software systems, CSE may impose penalty or take strict action against the entity.
4. **IP Allocation:** CSE owns each IP address that it assigns to a Client/Employee. A Client shall not use IP addresses that were not assigned to it by CSE. CSE reserves the right to suspend the network access of any server utilizing IP addresses outside the assigned range.
5. **IRC Policy:** Customers may not operate and maintain IRC servers which connect to global IRC networks such as Undernet, EFnet and DALnet. Use of IRC plugins, scripts, add-ons, clones or other software designed to disrupt or deny service to other users is prohibited. Harassing or abusive IRC activity is expressly prohibited under the AUP, including (i) disruption or denial of service or (ii) the use or joining of "botnets" or the use of IRC BNC's or other proxy and redirection software. If a Customer's IRC servers are frequently compromised or

- attract denial of service or distributed denial of service attacks that disrupt or denies service to other Customers or users, CSE may null-route, filter, suspend, or terminate that Customer's service.
6. **Usenet Policy:** Usenet posts and content must conform to standards established by the Internet community and the applicable newsgroup charter. CSE reserves the right to determine whether such posts violate the AUP.
 7. **No VPN Policy:** We don't allow VPN service providers to host their services on CSE's infrastructure
 8. Send unsolicited commercial messages or communications in any form ("SPAM")
Receive complaints from cybercrime, About violations and/or fraud, Any activity which is prohibited as per the Indian IT act, Engage in any activities or actions that infringe or misappropriate the intellectual property rights of others, including, but not limited to, using or distributing third party information protected as a trade secret information in violation of a duty of confidentiality, using third party copyrighted materials without appropriate permission, using third party trademarks without appropriate permission or attribution;
 9. Engage in any activities or actions that would violate the personal privacy rights of others, including, but not limited to, collecting and distributing information about Internet users without their permission, except as permitted by applicable law;
 10. Send, post or host harassing, abusive, pornographic, libelous or obscene materials, or assist in any similar activities related thereto; Intentionally omit, delete, forge or misrepresent transmission information, including headers, return mailing and Internet protocol addresses;
 11. Engage in any activities or actions intended to withhold or cloak Customer's or its Users; identity or contact information;
 12. Using the CSE connectivity services for any illegal purposes, in violation of any applicable laws or regulations or in violation of the rules of any other service providers, websites, chat rooms or the like assist or permit any persons in engaging in any of the activities described above.

L. Violations of AUP

CSE may enforce this AUP, with or without notice to a User, by any action it deems reasonable, in its sole discretion. In addition to the remedial provisions provided elsewhere in this AUP, CSE may:

- Disable access to a User's content that violates this AUP.
- Suspend or Terminate a User's access to CSE Services, CSE Datacenter
- Network or its physical infrastructure.
- Remove DNS records from Servers.
- Block mail or any other network service.
- Effect IP address null routing.
- Take legal action against a User to enforce compliance with this AUP.

M. Reporting Violations

If there is a violation of this AUP, direct the information to the Administration of CSE at cseadm@se-India.com or via postal mail to: The Calcutta Stock Exchange Ltd. 7, Lyons Range, Kolkata 700001, India

Version Control History

Version Change Date:

Version Number:

Changes: