CME Group Guest Wireless Terms & Conditions

1.0 Terms & Conditions

1.1 User acknowledges that: (a) the Internet contains material that may be considered offensive; (b) CME Group ordinarily does not filter, censor, edit, or regulate the flow of data, software, graphic images, or other materials on the Internet to or from any of it's usage holders; (c) the Internet may from time to time contain hostile programs, viruses, worms, Trojan horses and other files that may affect or destroy the operation of or information on the users machine.

1.2 User agrees that CME Group neither endorses nor is responsible for (and under no circumstances shall be liable for) the content, accuracy or reliability of information and/or content accessed from the Internet or the user's guest wireless account. CME Group will in no way be responsible for the loss of files or materials due to deletion, error or malfunction. CME Group does not control, nor are we responsible for, data, content, services, or products (including software) that the user accesses, downloads, receives or buys via the guest wireless service.

1.3 The user agrees the service is not to be used for any unlawful purpose, or to transmit material that violates these terms and conditions, any applicable federal, state, and local laws, rules and regulations. This includes, but is not limited to materials which are subject to another entity's copyright, material which is threatening, material which is obscene or defamatory, and material which constitutes a trade secret of another person. The user further agrees that he/she is solely responsible for the compliance of information accessed from, uploaded to, or transmitted from the internet using the guest wireless account (including information obtained through any hyperlink) within any applicable law. All use of the guest wireless network is subject to monitoring and audit by the Technology Division and Information Security, and is subject to the policies and procedures of CME Group.

1.4 The user will comply with all CME Group policies, procedures and regulations, including but not limited to rules present in the Information Security Acceptable Use Policy. The user agrees to monitor periodically any changes to this policy. This policy is available on OpenExchange. *Prior to being granted access to the wireless network the user needs to read and sign a copy of the Acceptable Use Policy and the Guest Wireless Terms and Conditions Policy.* By accepting this, the user is also agreeing to abide by the CME Group Acceptable Use Policy.

1.5 Sharing Connections: A network connection supplied by CME Group is solely for the use of the individual subscriber assigned to that connection. User agrees to utilize the connection for his/her own personal use. Connections may not be shared among multiple users. CME Group Guest Wireless users cannot use any mechanisms (either hardware or software) to provide network connectivity to non-subscriber users. The user agrees to be fully responsible for any messages he/she transmits or authorizes another to transmit.

1.6 Servers & General Usage: The operation of any commercial or for-profit enterprise or advertising from the guest wireless network is prohibited, along with any re-sale of access or services. Illegal activities, including but not limited to, software piracy and copyright infringement are prohibited. In addition, IP spoofing, packet sniffing, virus distribution, or any activity that disrupts the network will subject the user to disciplinary action as discussed in CME Group's Information Security Acceptable Use Policy. The user may have their account terminated and referred to the proper authorities. CME Group retains sole discretion in determining which activities disrupt the network. Also, CME Group further reserves the right to terminate the connection of any program using an unusually high portion of bandwidth which unreasonably inhibits the use of the network by other CME Group users or administrators.

1.7 Termination: Upon any violation of this policy by the user of the guest wireless network, which at the CME Group's sole discretion is determined to be of a serious nature, the user's access may be terminated without notice and CME Group administrators may take other actions as outlined in this document and the Information Security Acceptable Use Policy. CME Group absolutely reserves the right to modify, monitor, or block access to any information on any web page or service provided through a web site that CME Group, in its sole discretion, believes is unacceptable, inappropriate or in violation of this policy. User agrees that CME Group's failure to respond to any violation shall not be deemed acceptance of such a violation, and that CME Group administrators may take corrective action at any time.

1.8 CME Group guest wireless network users shall take full responsibility for any messages that they transmit or authorize any other person to transmit through the network. The user shall obey the policies, laws and rules that apply to electronic communications. Users that violate these rules and laws or provide access to others who violate them may be subject to legal action.

2.0 Customer Support

The guest network is offered as a *best effort* system and CME Group does not guarantee that this network or service provided via this network (Internet) will be available at all times. CME Group approves only non-CME Group hardware for access to the network. CME Group cannot be responsible for individual hardware and software configurations. Please be advised that support for guest internet connectivity is limited.

3.0 Guest Network Hardware/Software Maintenance

3.1 Planned maintenance of the network hardware and software shall occur on a periodic basis. Such maintenance may make the network unavailable for periods of time. The CME Group Wireless staff will make reasonable efforts to schedule maintenance when network traffic is low. Advance notice of network downtime may be provided as circumstances permit.

4.0 Enforcement

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

External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5.0 Policy Exceptions

All requests for an exception to this policy must be submitted online at https://nsweb1/guest_internet/exception_req.html.

Issued by: Technology and Enterprise Computing Division, Information Security Department.