VIRTUAL CLUB MEETING
PRIVACY AND SECURITY CONSIDERATIONS

Since Virtual Club Meetings are relatively new to Lions Clubs, we must carefully incorporate this type of meeting into our Club operations, and do so in a safe and responsible way. This includes mitigating the risk of nonmembers gaining access to our Club's and our Club Member's private information. As a result, we're asking every member to be careful with how they manage and protect information, as well as understanding the responsibilities of outside Service Providers, our meeting Host(s), our individual Lions, and our meeting Participants.

All Clubs and Lions should adopt policies and practices that safeguard the privacy of their Virtual Meetings; whether the meetings are for Club, Board, Committee, or "other" purposes.

Following are several recommendations:

1. Ask Participants to **KEEP Login Credentials CONFIDENTIAL.**

2. Ask Participants to **NEVER share** login credentials with Nonmembers**.**

3. Ask Participants to **NEVER republish** login credentials on social media (e.g. Facebook or Twitter).

4. Ask Hosts to **Minimize lead time exposure when publishing login credentials**. Publish them no more than 1 or 2 days prior to the scheduled meeting's start date and time.

5. Ask Hosts to **use a secure means of communication** with members such as Email, SMS or Text messaging; and to use a mix of alpha (lower & upper case), and numeric characters for virtual meeting names and credentials, and vary the credentials for subsequent virtual meetings.

6. Ask Club Secretaries to keep **Club Address Book Information** up-to-date.

When a new member joins your Club, they should notify individuals such as Email Administrators, FreeConferenceCall Hosts and Webmasters as soon as possible so that the new member begins receiving private Club communications and Meeting login credentials; and so that the new member can access the Member Pages of their Club's website.

When a member leaves your Club, they should notify individuals such as Email Administrators, FreeConferenceCall Hosts and Webmasters as soon as possible so that the departed ex-member, will be removed from Club address books and will NOT continue to receive private Club communications and Meeting Login credentials. This will also prevent them from accessing the private information on the Members pages of their Club's website.

7. Clubs should **Monitor ALL participants during Virtual Meetings in Real-time**. The Host, the Lion Tamer or a designated "security monitor" should verify the identity of every attendee at the beginning of the meeting and immediately identify anyone who joins the meeting thereafter. If a participant can not be identified as being authorized to attend, they should be booted from the meeting as soon as that conclusion has been reached.