Acceptable Use Policy (AUP)
For ALL Services – Revised 05/01/2022

This Acceptable Use Policy ("AUP") is part of the Cyber One Solutions, LLC. Master Services Agreement (the "Agreement"). All capitalized terms in this AUP have the meanings identified in the Agreement, unless they are otherwise defined below.

PROVIDER MAY SUSPEND OR TERMINATE THE SERVICES IN ACCORDANCE WITH THE AGREEMENT IF ANYONE IN YOUR ORGANIZATION VIOLATES THIS AUP. PROVIDER MAY REVISE THIS AUP AT ANY TIME AND FOR ANY REASON IN ITS SOLE DISCRETION. IN THE EVENT OF ANY SUCH REVISION, PROVIDER MAY, BUT IS NOT REQUIRED TO, PROVIDE YOU NOTICE OF THE CHANGE. YOU ARE SOLELY RESPONSIBLE FOR REMAINING AWARE OF ANY SUCH CHANGES DURING THE TERM OF THE AGREEMENT.

1. Client shall not use the Services to engage in or promote illegal or abusive behavior, including:
    a. Accessing, using, or monitoring any data, system, network, or internet-accessible account that does not belong to the individual, either in any way that breaches security or authentication measures or otherwise without express authorization from the Owner of the data, system, network and/or account.
    b. Interfering with the ability of any other Client of Provider to use or access the Services,
    c. Using any means, covert or overt, direct, or indirect, to collect, transmit or facilitate the collection or transmission of email addresses, screen names, personal identifiers or any other personal information without the consent of the person to whom that information pertains,
    d. Using any false or misleading metadata or personal identifiers in any electronic message transmitted using the Services,
    e. Distributing and software without confirming that the user affirmatively consents to its download and installation, or,
    f. Coordinating or participating in any activities that are reasonably likely to result in retaliation against the Services or against Provider, its officers, employees or agents.
2. Client shall not, directly or indirectly, publish, transmit or store on any system or network owned or operated by Provider any content – or any links to any content hosted elsewhere – that, in Provider's sole discretion:
    a. Relates in any manner to child pornography, bestiality, or non-consensual sex acts,
    b. Incites or threatens violence or contains harassing content or hate speech,
    c. Is unfair or deceptive under the consumer protection laws of any jurisdiction,
    d. Is defamatory or violates any person's privacy,
    e. Creates a risk to any person's safety or health or interferes with an investigation by law enforcement,
    f. Exposes trade secrets or other confidential information of another person or entity,
    g. Is intended to assist others in defeating copyright protections,
    h. Infringes another's copyright, trademark, patent, or other property right,
    i. Promotes any unlawful activity or is otherwise illegal or solicits conduct that is illegal under any applicable laws, or,
    j. Is otherwise malicious, fraudulent, likely or calculated to result in retaliation against Provider, or intended to harass or threaten any person or entity.
3. Client shall not use any hosted Exchange or other messaging Services delivered by Provider to send bulk email.
4. Client shall comply with all laws and regulations applicable to bulk or commercial email. Provider may – but is not required to – monitor your compliance with those laws and regulations, and Provider may block the

transmission of email that violates those laws and regulations. In addition, Client shall not use the Services to transmit or to facilitate the transmission of any communication to any person who has indicated that he or she does not wish to receive that communication.

5. Client shall not attempt to test the vulnerability of any system or network owned or operated by Provider with the exception of a Client specific cloud system. Client further shall not attempt to breach any security or authentication measures maintained by Provider on any of its systems or networks.
6. Client shall comply with the rules of any other network client is accessing using the Service.
7. Provider may prohibit Client from streaming any live events where, in Provider's sole discretion, there is a risk that the event may violate any part of this AUP.
8. Provider may prohibit Client from streaming any live events where, in Provider's sole and unfettered discretion, unreasonably interferes with the normal operation of that system, or that consumes a greater than expected share of the resources of that system. Provider may quarantine and/or delete any data stored on any shared system if that data is infected or corrupted and has potential to infect or corrupt any part of the shared system or any other data stored on, or within, that system.
9. Client must have valid and current information on file with Client's domain name registrar for any domain hosted on the Provider's network.
10. If Client registers a DNS record or zone on any systems owned or operated by Provider for a domain of which Client is not the registrant or administrative contact according to WHOIS records, then upon request from that registrant or administrative contact, Provider may modify, transfer, or delete that record or zone.

This area has been intentionally left blank.