Acceptable Use Policy

This Acceptable Use Policy (AUP) governs the use of Emergency One Groups online services, including but not limited to its website, digital platforms, and any associated resources (collectively referred to as “Services”). By accessing or using the Services, you agree to comply with this AUP.

This policy was last reviewed on 08/05/2024.

Fair use

Users are granted access to the Services for lawful and legitimate purposes consistent with the intended functionality and scope of the Services. Users shall not access or use the Services in any manner that violates applicable laws, regulations, or this Acceptable Use Policy. Users shall not engage in any activities that could disrupt, damage, or impair the functionality of the Services, including but not limited to unauthorised attempts to access or manipulate the website's code, databases, or server infrastructure.

We are opposed to all forms of abuse, discrimination, rights infringement and/or any action that harms or disadvantages any group, individual or resource. We expect our customers and, where applicable, their users to likewise engage our Products with similar intent.

Customer accountability

Customers accessing Emergency One's online services ("Customers") are responsible for their conduct and activities while using the Services. Customers shall adhere to all applicable laws, regulations, and the provisions outlined in this Acceptable Use Policy ("AUP").

Customers shall use the Services for lawful and legitimate purposes consistent with the intended functionality and scope of the Services. Any use of the Services that violates applicable laws or infringes upon the rights of others is strictly prohibited.

Customers shall comply with all policies, guidelines, and terms of service established by Emergency One for the use of its online services. This includes but is not limited to the AUP, Privacy Policy, Terms of Use, and any additional agreements or terms governing the use of specific features or functionalities.

Customers agree to indemnify and hold harmless Emergency One, its affiliates, officers, directors, employees, and agents from any claims, damages, losses, liabilities, or expenses arising out of or related to the Customer's use of the Services, violation of this AUP, or infringement of any rights of third parties.

Emergency One reserves the right to amend or modify this AUP at any time without prior notice. By accessing or using Emergency One's online services, Customers acknowledge and agree to abide by the terms of this Customer Accountability section of the Acceptable Use Policy.

Prohibited activity

Users are strictly prohibited from engaging in any activities that violate applicable laws, regulations, or third-party rights. Prohibited activities include, but are not limited to:

1. **Unauthorised Access, Use, or Interference:** Users shall not attempt to gain unauthorized access to Emergency One's systems, networks, or data. This includes any actions aimed at bypassing security measures, exploiting vulnerabilities, or accessing restricted areas of the Services without proper authorization. Users shall not interfere with the normal operation of Emergency One's systems or networks, including but not limited to distributed denial-of-service (DDoS) attacks, network scanning, or other forms of malicious activity.

2. **Distribution of Malware:** Users shall not distribute, upload, or transmit malware, viruses, worms, ransomware, or any other malicious software or code that could harm or disrupt Emergency One's systems, networks, or data. This includes knowingly distributing infected files, links to malicious websites, or other forms of digital threats.
3. **Unauthorized Modification or Disruption:** Users shall not make unauthorized modifications to Emergency One's online services or disrupt the normal operation of the Services. This includes tampering with website code, altering configuration settings, or engaging in any activities that degrade the performance or availability of the Services for other users.
4. **Harassment and Defamation:** Users shall not engage in harassment, defamation, or any other form of abusive behavior towards others. This includes making threats, spreading false information, or engaging in cyberbullying, hate speech, or discriminatory conduct that violates the rights or dignity of others.
5. **Copyright, Trademarks and Intellectual Property**: Any material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorisation, and any material that is obscene, defamatory, constitutes an illegal threat or violates export control laws.
6. **Compromising Security or Integrity:** Users shall not engage in any activity that may compromise the security or integrity of Emergency One's systems or networks. This includes attempting to exploit vulnerabilities, conducting unauthorized port scans, or engaging in any other actions that could lead to unauthorized access, data breaches, or other security incidents.
7. **Spamming and Phishing:** Users shall not engage in spamming, phishing, or other forms of unsolicited communication through use of Emergency One's digital content. This includes sending bulk unsolicited emails, promoting fraudulent schemes, or impersonating Emergency One or its employees for malicious purposes.
8. **Unlawful or Offensive Content:** Users shall not post or transmit unlawful, obscene, or offensive content through use of Emergency One's digital content. This includes content that is defamatory, libelous, pornographic, discriminatory, or otherwise violates community standards or ethical norms.

SPAM and Unauthorised Message Activity

Our Services and Products must not be used for the purpose of sending unsolicited bulk or commercial messages in violation of the laws and regulations applicable to your jurisdiction (“spam”). This includes but isn’t limited to sending spam, soliciting customers from spam sent from other service providers, and collecting replies to spam sent from other service providers.

Our Services and Products must not be used for the purpose of running unconfirmed mailing lists or telephone number lists (“messaging lists”). This includes but isn’t limited to subscribing email addresses or telephone numbers to any messaging list without the permission of the email address or telephone number owner and storing any email addresses or telephone numbers subscribed in this way. All messaging lists run on or hosted by our Products must be “confirmed opt-in”. Verification of the address or telephone number owner’s express permission must be available for the lifespan of the messaging list.

We prohibit the use of email lists, telephone number lists or databases purchased from third parties intended for spam or unconfirmed messaging list purposes on our Products.

This spam and unauthorised message activity policy applies to messages sent using our Services, Products, or to messages sent from any network by the customer or any person on the customer’s behalf, that directly or indirectly refer the recipient to a site hosted via our Products.

Unethical, exploitative, and malicious activity
Our Services and Products must not be used for the purpose of advertising, transmitting or otherwise making available any software, program, product or service designed to violate this acceptable use policy, or the acceptable use policy of other service providers. This includes but isn't limited to facilitating the means to send spam and the initiation of network sniffing, pinging, packet spoofing, flooding, mail-bombing and denial-of-service attacks.

Our Services and Products must not be used to access any account or electronic resource where the group or individual attempting to gain access does not own or is not authorised to access the resource (e.g. "hacking", "cracking", "phreaking", etc.).

Our Services and Products must not be used for the purpose of intentionally or recklessly introducing viruses or malicious code into our Products and systems.

Our Services and Products must not be used for purposely engaging in activities designed to harass another group or individual. Our definition of harassment includes but is not limited to denial-of-service attacks, hate-speech, advocacy of racial or ethnic intolerance, and any activity intended to threaten, abuse, infringe upon the rights of or discriminate against any group or individual.
Other activities considered unethical, exploitative, and malicious include:

- Using our facilities to obtain (or attempt to obtain) services from another provider with the intent to avoid payment;
- The unauthorised access, alteration or destruction (or any attempt thereof) of any information about our customers or end-users, by any means or device;
- Using our facilities to interfere with the use of our facilities and network by other customers or authorised individuals;
- Publishing or transmitting any content of links that incite violence, depict a violent act, depict child pornography or threaten anyone's health and safety;
- Any act or omission in violation of consumer protection laws and regulations;
- Any violation of a person's privacy.

Our Products may not be used by any person or entity, which is involved with or suspected of involvement in activities or causes relating to illegal gambling; terrorism; narcotics trafficking; arms trafficking or the proliferation, development, design, manufacture, production, stockpiling, or use of nuclear, chemical or biological weapons, weapons of mass destruction, or missiles; in each case including any affiliation with others whatsoever who support the above such activities or causes.

Unauthorised use of Emergency One Property

We prohibit the impersonation of Emergency One Group, the representation of a significant business relationship with Emergency One Group, or ownership of any Emergency One Group property (including our Products and brand) for the purpose of fraudulently gaining service, custom, patronage or user trust.

About this policy

This policy outlines a non-exclusive list of activities and intent we deem unacceptable and incompatible with our brand. We reserve the right to modify this policy at any time by publishing the revised version on our website. The revised version will be effective from the date the customer uses our Services after we publish the revised version on our website; or 30 days after we publish the revised version on our website.