ACCEPTABLE USE POLICY

This Acceptable Use Policy ("**AUP**") is a policy governing the use of the Services, as defined in the NOVOSERVE Terms of Service ("**TOS**"). This AUP is designed to provide a clear understanding of the rules, regulations, and restrictions in the use of NOVOSERVE's Services. In the event of a conflict between the terms of this AUP and the TOS, the terms and conditions of this AUP apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the TOS.

NOVOSERVE reserves the right to unilaterally amend the conditions stated in the AUP, you will be notified of any significant changes to the AUP.

1. **USE OF NOVOSERVE SERVICES**

1.1 CLIENT agrees to use NOVOSERVE's Services only for lawful purposes.
1.2 Specific activities that are prohibited include, but are not limited to:
   - Threatening harm to individuals or property or otherwise harassing behavior;
   - Terrorism;
   - Store or distribute material protected by intellectual property rights or any other copyrighted, trademarked, and other proprietary material without proper consent;
   - Store or distribute of material protected by industrial property rights without proper authorization (including the manufacture or use or distribution of counterfeit, pirated or illegal software or other product);
   - Fraudulently representing products or services;
   - (D)DoS attacks;
   - Store or distribute certain other types of material. Examples of prohibited material include, but are not limited to, software containing viruses and tools to compromise the security of or penetrate a computer system or IT infrastructure component (including, but not limited to, port scanning/knocking, hacking, and phishing);
   - Spamming;
   - Store or distribute zoophilia, child pornography, child erotica;
   - Facilitating, aiding, or encouraging any of the abovementioned activities;
   - Other content or activities that may cause harm to NOVOSERVE, other clients or third parties.
1.3 Additional activities are prohibited that appear in other sections of this AUP, including Article 3 (System Security).

2. **INVESTIGATION POLICY**

2.1 NOVOSERVE reserves the right to investigate suspected violations of this AUP following a report or at its own initiative.

2.2 Suspected violations of this AUP can be reported by sending an e-mail to abuse@novoserve.com following the requirements as set out in our Knowledgebase.(https://portal.novoserve.com/index.php?rp=/knowledgebase/17/How-do-I-report-Abuse.html).

2.3 When NOVOSERVE is notified by a third-party of a (suspected) violation by CLIENT and/or an End-user of the AUP and/or applicable law, NOVOSERVE shall notify CLIENT by way of an email.

2.4 When NOVOSERVE becomes aware of a possible violation, NOVOSERVE may initiate an inquiry that may include collecting information from CLIENT involved and the complaining party.

2.5 During an inquiry, NOVOSERVE may (temporarily) prevent access to CLIENT's equipment involved at the hardware and/or router and/or switch level.

2.6 CLIENT shall, within the response period defined in NOVOSERVE's notification, take corrective action to resolve the violation and, within that period, inform NOVOSERVE of the action taken by CLIENT.

2.7 If NOVOSERVE believes, in its sole discretion, that a violation of this AUP has occurred, it may take responsive action. Such action may include but is not limited to (partially) suspending Services or terminating Services, as referred to in Article 8 and Article 12 of the TOS. NOVOSERVE, in its sole discretion, will determine what action it will take in response to a (potential) violation on a case-by-case basis. In deciding its responsive action, NOVOSERVE will act diligently, objectively and proportionately and take the rights and legitimate interests of all parties involved into account.

2.8 If NOVOSERVE decides to take responsive action, NOVOSERVE shall inform CLIENT in a clear, comprehensive, and precise manner of its reasons for that action. The information shall include:

2.8.1 What responsive action has been taken, including its duration and territorial scope;

2.8.2 The facts and circumstances relied upon to take the decision;

2.8.3 Whether automated means have been used to detect the violation or to take the decision;

2.8.4 On what grounds (illegality or breach of TOS) the responsive action was taken and a reason as to why there was a breach;

2.8.5 Any possible option for redress, such as the option to file a counter-notice as described in section 2.9.

2.9 NOVOSERVE may provide CLIENT the option to file a counter-notice (through a ticket) to dispute the alleged violation. NOVOSERVE shall review the counter-notice and may, in its sole discretion, decide to reject CLIENT's counter-notice and require CLIENT to take immediate corrective action.

2.10 Violations of this AUP could also subject CLIENT to criminal liability. NOVOSERVE may report you to law enforcement authorities. If NOVOSERVE suspects that a criminal offence involving a threat to the life or safety of a person has taken place or may take place in the future, it is legally obligated to notify the relevant law enforcement authorities.

3. SYSTEM SECURITY

3.1 CLIENT receives a login and a password (the "**Login Credentials**") when (the account for) the Service is activated. CLIENT is fully responsible for non-disclosure of the Login Credentials and changing its passwords periodically.

3.2 When entering the Data Center, CLIENT must uphold NOVOSERVE's and the Data Center's facility rules & regulations. These are made available on-premises.

3.3 CLIENT is prohibited from using NOVOSERVE's Services to compromise the security or tamper with system resources on equipment in NOVOSERVE's network or at any other site. The use or distribution of software/tools designed for compromising security is prohibited. Examples of these tools include but are not limited to password cracking software/tools or network probing software/tools.

4. EMAIL USE

4.1 CLIENT may not send, propagate or reply to emails in any way that may be unlawful. CLIENT must avoid sending further emails to users after receiving a request to stop that activity.

4.2 Violations of NOVOSERVE's AUP outlined in this document can sometimes result in massive numbers of email responses. If a CLIENT receives so many emails that NOVOSERVE resources are affected, NOVOSERVE staff may block access to CLIENT's equipment at the hardware and/or router and/or switch level.

5. **ABUSE COMPLIANCE POLICY**

5.1 ABUSE HANDLING PROCEDURE

5.1.1   CLIENT shall adopt and apply an acceptable use policy for its End-users (as defined in the TOS), including employees and its contractors, compliant with NOVOSERVE's AUP and the law that applies to the Agreement.

5.1.2   CLIENT will log each abuse notification received from NOVOSERVE and CLIENT's follow-up and actions taken to such complaint.

5.1.3   CLIENT will ensure the availability of properly trained personnel to ensure that CLIENT and/or End-users comply with the AUP.

5.2 REPEAT INFRINGEMENT

5.2.1   CLIENT should make reasonable efforts to investigate suspected violations by End-users of its acceptable use policy following reports and take the necessary actions.

5.2.2   CLIENT shall immediately discontinue the Services's availability to the End-user if such End-user is discovered to be a repeated violator of the AUP.