Acceptable Use Policy

General. This Acceptable Use Policy ("AUP") addresses requirements applicable to Client's use of Mission Pathways' products, solutions and services ("Mission Pathways Solutions").

Appropriate Use. Client will not, and will not allow or authorize its users to use Mission Pathways Solutions to take any actions that (i) infringe on or dilute any Mission Pathways or third party copyright, patent, trademark, trade secret or other proprietary rights or rights of publicity or privacy; (ii) violate any applicable law, statute, ordinance or regulation (including those regarding export control); (iii) are defamatory, libelous, trade libelous, threatening, harassing, or obscene; (iv) interfere with or disrupt any Mission Pathways services or equipment or cause excessive or disproportionate load on Mission Pathways or its licensors or suppliers' infrastructure; (v) involve knowingly distributing viruses, Trojan horses, worms, or other similar harmful or deleterious programming routines; (vi) encourage conduct that violates any applicable local, state, national or international laws or regulations; or (vii) involve the unauthorized entry to any machine accessed via Mission Pathways Solutions. If Client violates any portion of this AUP, Client accepts sole responsibility for all remedial actions and costs related to such violation, including compliance efforts and costs associated with statutory obligations or government investigations.

Responsibility for Content. Mission Pathways provides cloud-based and related services and Client provides information and content. Client accepts sole responsibility for information and content collected, stored or transmitted by Mission Pathways Solutions on behalf of Client or its end users. Client controls and approves all aspects of its constituent communications and related content. If Client acquires content from third parties for republication, Client is solely responsible for ensuring it complies with any licensing requirements associated with such content. Client acknowledges that Mission Pathways exercises no control over the information passing through the Mission Pathways Solutions application, and that Mission Pathways assumes no responsibility for Client's content.

Privacy Policy; Data Protection. Client agrees to post and maintain its own privacy policy concerning its collection of personal information on websites or forms developed using Mission Pathways Solutions. Client is solely responsible for ensuring that its privacy policy complies with all applicable laws. Client shall be responsible for the accuracy, quality and legality, which includes notices, consents and "opt out" requirements, of (i) all Client data provided to Mission Pathways by Client or on Client's behalf; (ii) all Client data stored in Mission Pathways Solutions; and (3) the means by which it acquired all Client data.

Personal Information. Mission Pathways Solutions contain designated encryption functionality for the collection and storage of bank card and account numbers and individual identification numbers issued by government agencies and financial institutions. Client shall not use Mission Pathways Solutions to collect and store such information outside the encrypted fields within Mission Pathways Solutions.

Email Marketing. Please refer to **Acceptable Use Policy for Mission Pathways Email** below.

Enforcement of AUP. Mission Pathways reserves the right to suspend the provision of Mission Pathways Solutions or take other appropriate remedial action to address actual or suspected violations of the AUP. Mission Pathways will use reasonable efforts to notify Client and provide

an opportunity to cure before taking any such action, if practicable and if permitted by law. Client will cooperate with Mission Pathways in investigating complaints about potential violations and in taking any corrective action that Mission Pathways deems necessary to address such violations. Mission Pathways reserves the right to remove any Client content from Mission Pathways Solutions that Mission Pathways determines, at its reasonable discretion, may be illegal, tortious, or infringing on the rights of a third party. If Client becomes aware of any activity that violates this AUP, Client shall promptly notify Mission Pathways of any such violation and Client shall take all necessary action to cease such violation. Violations or suspected violations of this AUP shall be immediately reported to mailto:solutions@mission-pathways.com

DMCA. Client acknowledges that Mission Pathways is a "service provider" as defined in 17 USC § 512(k)(1), is subject to the Digital Millennium Copyright Act ("DMCA") and has the duties of a service provider under the DMCA. Client is solely responsible for ensuring that Client data and internet content and its provision of same to Mission Pathways complies at all times with all applicable laws and regulations.

AUP Updates. Mission Pathways reserves the right to modify this AUP from time to time, effective upon posting a revised copy to the Mission Pathways website at www.Mission Pathways.com. Replace with MP site address

Acceptable Use Policy – Email. Mission Pathways requires all email customers to adhere to the policy outlined below. For assistance with specific questions related to your email program, contact your Support representative.

Permission-based email – Before you use Mission Pathways' products for email, make sure you're allowed to send messages to recipients.

You must:

- Verify you have consent. Depending on how you obtain email addresses, consent might be explicit or implied.
- Explicit – If you don't already have relationships with recipients, you need explicit consent from them to send marketing or notification messages. They can provide consent online, by phone, or on paper forms. Wherever you collect email addresses, describe the nature of messages you send and the identities – such as domain names or brands – your organization uses when it sends email.
- Implied – If you're confirming online transactions, consent is implied. Consent might also be implied if recipients previously interacted with your organization.
- Ensure you have a valid legal basis for communications.
- Comply with data protection laws that apply to your organization.
- Explicit opt-in collection – When you use Mission Pathways products to collect email addresses as part of online form submissions, the screen must include a clear and conspicuous option to allow users to decide whether to opt in to receive email.

  Note: When a form's only purpose is to allow users to sign up for email, opt-in is implied.

- Email address lists acquired from third parties – If you purchase or use lists of email addresses from third parties, the list owners must use their own brands and email

systems to invite subscribers to opt in to receive email from your organization. Once you obtain consent for those recipients, you may then use Mission Pathways' products to send email to them.

Mission Pathways email append services – If you purchase or use Mission Pathways services to correct, update, or add email addresses for recipients who already exist in your database, you must still determine whether you have explicit or implied consent before you use Mission Pathways' products to send messages to them.

Unsubscribe requests – Messages must include a clear and visible link to allow recipients to unsubscribe from all marketing and non-transactional emails you send. To encourage recipients to reconsider, you may offer alternate options – such as which types of messages you send and how often you send them – from the screen where they confirm unsubscribe requests.

Unsubscribe propagation – If you use another email service provider in addition to Mission Pathways, ensure you update unsubscribe requests from each system to the other within five business days.

- **Sender identity and reply handling –** In each message you send, you must include:
- Your organization's identity
- A valid physical or postal address
- A valid "from" address
- Also, create and maintain email accounts for your top-level domain names, such as abuse@example.org and postmaster@example.org, to handle complaints and register them with abuse.net.

Undeliverable addresses – When messages to email addresses are undeliverable, Mission Pathways suppresses the addresses from future mailings. Mission Pathways uses internet email standards and requirements from major mailbox providers to determine which addresses to suppress. The criteria are set at the sole discretion of Mission Pathways and can change as necessary. You may not attempt to reset or reload these addresses or take other actions to circumvent the suppressions.

Unacceptable email practices – You may not:

- Use Mission Pathways products to send unsolicited commercial email messages.
- Obtain email addresses by harvesting them from websites or offline directories, or by auto-generating them.
- Send email communications that contain misleading or false information about the sender, subject, or content of a message.

Enforcement of email marketing best practices – Mission Pathways monitors spam practices via change link to direct to MP to determine whether organizations follow the email policy. If you fail to adhere to the terms, Mission Pathways will take corrective actions which may include, but are not limited to:

- Working with your organization to review your list building practices and identify how you obtained email addresses for people who didn't provide consent.

- Requiring you to remedy problems identified with your list building practices to ensure they are permission-based.
- Permanently removing one or more email addresses from your database.
- Sending your email from a server with a low sending reputation and therefore fewer delivery assurance benefits, such as a server that's not protected by Mission Pathways' whitelist status with major mailbox providers.

Important! Mission Pathways reserves the right to terminate bulk email service for organizations who fail to correct their list building and management practices.