2601 Main Street, Suite 830
Irvine, CA 92614
Toll Free: (877) 560-3473
Fax: (949) 474-5967
http://www.MindFireInc.com

Email and SMS Acceptable Use Policy
Email Security and Encryption Policy

1. Overview

Electronic Mail (aka Email) and SMS (Short Message Service aka Text Messaging) are now used in all industry verticals as a major communication, awareness, and promotional methods. At the same time, misuse of email and SMS can pose many legal, privacy, and security risks, thus, it's important for users to understand the appropriate use of Email and SMS communications.

2. Purpose & Scope

The purpose of this policy is to ensure the proper use of MindFire, Inc's email and SMS systems by customers and business associates, and make users aware of what MindFire, Inc deems as acceptable and unacceptable use of such communication frameworks. In addition, this policy includes a discussion on MindFire, Inc's Email platform and transmission security.

3. Policy

3.1. All use of email and SMS must be consistent with MindFire, Inc policies and procedures of ethical conduct and safety and be in compliance with applicable laws and proper business practices.

3.2. MindFire, Inc email and SMS communication infrastructure should be used primarily for business-related purposes associated with MindFire, Inc or its customers. Any communication promoting any competitor of MindFire, Inc is prohibited.

3.3. The MindFire, Inc email and SMS systems shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Anyone who comes across any email or SMS generated out of MindFire, Inc's

systems with this type of content, must report the matter to MindFire, Inc's support organization. A complete list of prohibited content is detailed in the section 5 titled *Compliance* below.

3.4. MindFire, Inc may monitor messages without prior notice, and contact individuals for compliance related discussions. However, MindFire, Inc is not obliged to monitor every email or SMS message sent through its systems.

3.5. ALL EMAILS and SMS

3.5.1. Must comply with all applicable laws and regulations including but not limited to CAN-SPAM (Controlling the Assault of Non-Solicited Pornography And Marketing), CASL (Canadian Anti-Spam Law) and E-Privacy Directive from the European Union. For SMS, the messages must comply with rules and regulations established by Common Short Code Administration (CSCA). In addition, your messages must meet the following requirements:

3.5.2. May not contain any false, misleading or deceptive information in its content or header, and may not attempt to obscure or hide the source of the message.

3.5.3. Must not be characteristic of spam as determined by the sole discretion of MindFire, Inc.

3.6. BULK OR COMMERCIAL EMAIL and SMS

Bulk or Commercial email and SMS messages are defined as any message for which the primary purpose is the commercial advertisement or promotion of a commercial product, website, or service. MindFire, Inc requires that for all Bulk or Commercial Emails and SMS, the sender must adhere to the following:

3.6.1. Must not send email and SMS to lists that have been purchased from a third party.

3.6.2. Intended recipients must have given their consent to receive email or SMS specifically from the sender.

3.6.3. Procedures for seeking consent include reasonable means to ensure that the person giving consent is the owner of the email address or mobile phone number for which consent is given.

3.6.4. Evidence of each recipient's consent in retained in a form that can be promptly produced on request. Evidence should contain at a minimum the date, time and method of obtaining the consent.

3.6.5. Procedures are in place that allow a recipient to revoke their consent – such as an unsubscribe link in the body of the email, or sending a STOP message to a SMS sender. The sender must honor revocations of

consent and notify the recipient within 48 hours.

3.6.6. Sender must have a Privacy Policy posted for all to review.

3.6.7. Emails must not generate excessive blacklistings or any critical blacklisting as determined at the sole discretion of MindFire, Inc.

3.6.8. Email must not generate excessive SPAM complaints as determined at the sole discretion of MindFire, Inc.

3.6.9. Email list must contain valid email addresses and must not generate excessive failures or hard bounces as determined at the sole discretion of MindFire, Inc.

4. Security and Encryption

This section applied only to emails sent out of MindFire, Inc's system and not SMS.

4.1. Users may only send email originating from a domain address that is registered to the User, is under the User's control, or that the User has received permission to transmit from on behalf-of the owners of the domain.

4.2. In order to secure the domain associated with the "From Email Address" of the emails, the domain(s) must be identified by using a Sender Policy Framework (SPF) record in the Domain Name Service (DNS) of the particular domain. MindFire, Inc's support team will provide instructions for SPF record setup if necessary.

4.3. MindFire, Inc recommends digitally signing every email being sent from their system using Domain Key Identification (DKIM). This allows the emails to be securely delivered to their destination email addresses. MindFire, Inc's support team will provide instructions for DKIM record setup if necessary.

4.4. MindFire, Inc's premium email service sends all the emails using TLS encryption if the receiving mail server supports it. The premium email service is available as a standard on MindFire, Inc's Studio platform and as an upgrade on MindFire, Inc's LWC product.

5. Compliance

5.1. NO MISSION CRITICAL OR HIGH RISK USE

5.1.1. The service is not designed, intended, or authorized for use in any mission critical, emergency, life-saving or life sustaining systems, or for any other application in which the failure of the service could lead to personal injury or death, or to physical or environmental damage.

5.2. ABUSE

5.2.1. You may not use MindFire, Inc's email and SMS infrastructure to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including but not limited to:

5.2.2. Interference with service to any user or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system, and transmitting computer viruses and Trojan horses.

5.2.3. Collecting or using email addresses, mobile phone numbers, screen names, or other personal identifiers and related information without the consent of the person identified or the owner of the information.

5.2.4. Probing, scanning, penetrating, reverse-engineering or testing the vulnerabilities of a MindFire, Inc's network, service, system or device to breach, attempt to breach or collect information about security or authentication measures, or any similar or related activity, without MindFire, Inc's express written consent.

5.2.5. Any conduct that causes or is likely to result in retaliation against MindFire, Inc's network, website, employees, officers or other agents, including but not limited to engaging in behavior that results in any server being the target of a Distributed Denial of Service (DDoS) attack.

5.2.6. Any conduct that is deemed abusive or malicious as determined at the sole discretion of MindFire, Inc.

5.3. PROHIBITED CONTENT

MindFire, Inc's network or email distribution systems may not be used to publish, transmit or store any content or links associated with the following:

5.3.1. Constitutes, depicts, fosters, promotes or relates in any manner to adult oriented material or activity including but not limited to pornography.

5.3.2. Excessively violent, incites violence, threatens violence, or contains harassing content or hate speech.

5.3.3. Creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement.

5.3.4. Activities associated with terrorism.

5.3.5. Exposes trade secrets or other confidential or proprietary information of another person without explicit permission.

5.3.6. Infringes on another person's copyright, trade or service mark, patent, or other property right.

5.3.7. Promotes illegal drugs or illegal arms trafficking, violates export laws.

5.3.8. Is otherwise illegal or solicits conduct that is illegal under laws applicable to MindFire, Inc, its customers and business partners.

5.3.9. Is otherwise malicious or fraudulent, as determined by the sole discretion of MindFire, Inc.

5.3.10. In addition, MindFire, Inc, in conjunction with their services infrastructure partners, have determined that certain types of Emails generate higher than normal abuse and feedback loop complaints, and in order to protect the reputation of our network and to achieve the highest rates of deliverability for all of our customers, we are unable to allow Emails being sent with the following contents:

5.3.10.1. Payday loans (short term unsecured loans)

5.3.10.2. Debt collection

5.3.10.3. Debt consolidation and reduction

5.3.10.4. Credit repair

5.3.10.5. Tax relief programs

5.3.10.6. Online Gambling

5.3.10.7. Get rich quick, Ponzi, or pyramid schemes, investment opportunities

5.3.10.8. Work from home or make money online opportunities

5.3.10.9. Day trading or penny stocks