# FSP HOSTING ACCEPTABLE USE POLICY

## Scope

The Full Sail Partners, Ltd ("FSP") Acceptable Use Policy ("AUP") applies to all FSP hosted accountsand hosting services under an FSP Hosting Services Agreement. Definitions shall have the meanings set forth in the FSP Hosting Services Agreement or the FSP Hosting Master Services Agreement (the "MSA"), unless otherwise stated herein.

## Rationale

FSP's AUP is designed to help protect our Customers and the Internet community from irresponsibleor illegal activities.  FSP's network connects to many other networks, commercial and governmental, some with restrictions on usage. FSP's users must comply with all acceptable use policies for all networks that they traverse, and at all times comply with local, state, and federal laws as well as applicable international laws. Protection of our Customers and our resources, the ability to provide quality services to our Customers, conformance with existing laws, and the protection of our reputation as a hosting service provider are contributing factors to AUP violation decisions.

FSP does not actively monitor, nor does FSP exercise editorial control over, the content of anyapplication electronic mail transmission, mailing list, news group or other material created or accessible over FSP's Hosting Environment.

If an FSP hosting account is used to violate the AUP, FSP reserves the right to suspend or terminateCustomer's service with notice. FSP's preferred course of action would be to advise the account owner of the inappropriate behavior and offer any corrective action necessary. However, flagrant or repeat violations of the AUP will result in immediate termination of hosting services.

Terms for acceptable use within the Application Hosting Environment are as follows;

1. Sending unsolicited (spamming) commercial e-mail is prohibited from FSP's Hosted Environment. Using an FSP mail address to collect responses from unsolicited commercial e-mail is prohibited. Sending large volumes of unsolicited e-mail (mail bombing) from the Application being hosted is prohibited. FSP will notify the Customer of any spamming and/orbombing complaints and will suspend or terminate the Customer's hosting account as follows:
2. 1st written complaint/occurrence – FSP will issue to the Customer a forward of thewritten complaint with written notification of the complaint(s) and a reminder to theCustomer of FSP's AUP.
3. 2nd written complaint separate from 1$^{st}$ occurrence – FSP will issue to the Customer aforward of the written complaint with written notification of the complaint(s) and will penalize Customer an amount equal to one month's Hosting Monthly recurring Fee which will become due immediately.
4. 3rd written complaint occurrence – FSP will issue to the Customer a written notification of the complaints(s) and will terminate the Hosting Services Agreement and demand payment for all amounts remaining for the Term of the Hosting Services Agreement thenin effect as provided for in the Master Service Agreement.
5. Harassment: Sending threatening or harassing e-mail, after being requested to stop, isprohibited. Extremely threatening or harassing e-mail is always prohibited.
6. Attempting to impersonate any person, using forged headers or other identifying informationfrom your application is prohibited. The use of anonymous re-mailers and nicknames does not constitute impersonation.
7. Activities that adversely affect the ability of other people or systems to use FSP's hostingServices or the Internet bandwidth to FSP's Hosting Environment are prohibited.
8. Attempts, which will not be successful, to gain access to any computer system, or Customer's Data, without consent is prohibited.
9. Sharing FSP accounts with anyone or re-selling FSP Services without the express written consent from FSP (such as a Hosting Services Agreement) is prohibited.
10. Providing fraudulent or expired licensing on Application software that is covered under the Hosting Services Agreement or misrepresenting rights to upgrades or updates, discontinuance of maintenance contracts with the software manufacturer for which the rightsto upgrades or updates is based on is prohibited. If a Customer is found to be out of coverage with an active maintenance contract with the software manufacturer, Customer willhave ten (10) business days to remedy and become current with the maintenance contract with the software manufacturer. If Customer fails to bring

their maintenance contract currentwith the software manufacturer, FSP may, in its sole discretion, shut down access to the Customer’s Data, at which time Customer may terminate their Hosting Services Agreement and pay the service fee of $420, plus an amount equal to the fee for one quarter of service, at which time FSP will provide Customer with a backup of their SQL database.

11. Using programs to misrepresent the number of users, number of Active Employees being processed or series level size on the Application software is prohibited. If Customer is foundto be out of license on the Application software by a query of their data, FSP will notify Customer and request that Customer bring their software in alignment with licensing or FSP has the obligation to report licensing discrepancies to the software manufacturer.
12. FSP does not censor the content of any newsgroups. FSP does advise our users that toolsare available to screen an account's access to newsgroups that may be considered offensive. It is the account owner's responsibility to make use of such tools if desired.

## SYSTEM ADMINISTRATION, PRIVACY AND SECURITY

FSP does not monitor the activity of accounts except for measurements of system utilization, number of licensed users and Active Employees for software and billing records. It may be necessary for FSPemployees to examine accounting logs and other records to resolve problems. FSP reserves the right to access an account's electronic mailbox, software license or data directly to solve system problems or mail system errors.

FSP will cooperate with any and all appropriate legal authorities in investigating claims of illegal activity, including but not limited to, illegal transfer or use of copyrighted material, postings or e-mailcontaining threats of violence, or other illegal activity.

Customers are reminded that no computer system should be considered safe from intrusion. E-mailmay pass through many computer systems, and should not be considered a secure means of communication unless encrypted. Even then, email information is only as secure as the encryption method.