

## Acceptable Use Policy

This acceptable use policy (the "Policy") defines acceptable practices relating to the use of Field Automated Communication Systems (FACS) services (the "Service") utilizing the FACS system (the "System") by customers and users ("Users") of FACS that have gained access to the Service through Client accounts.

This Agreement was last updated on January 1, 2020.

Users are required to adhere to all the policies specified in this AUP without exception.

The System may only be used for lawful purposes. Users may not violate any applicable laws or regulations of the United States. Should the User reside outside of United States, the laws of the United States and the country in which the User resides shall apply. Transmission, distribution or storage of any material on or through the System in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

The User acknowledges that FACS is unable to exercise control over the content of the information passing over the System and the Internet, including any websites, electronic mail transmissions, news groups or other material created or accessible over its System. Therefore, FACS is not responsible for the content of any messages or other information transmitted over its System. The System may be used to link into other networks worldwide and the User agrees to conform to the acceptable use policies of these networks. The User may obtain and download any materials marked as available for download off the Internet but is not permitted to use its Internet access to distribute any copyrighted materials unless permission for such distribution is granted to the User by the owner of the materials. The User is prohibited from obtaining and/or disseminating on-line any unlawful materials, including but not limited to stolen intellectual property, pornography, and/or any unlawful hate-speech materials.

All references to systems and networks under this section includes the Internet (and all those systems and/or networks to which user is granted access through the System) and includes but is not limited to the infrastructure of FACS itself. The User may not circumvent user authentication or security of any host, network, or account (referred to as "cracking" or "hacking"), nor interfere with service to any user, host, or network (referred to as "denial of service attacks"). Violations of System or network security by the User are prohibited, and may result in civil or criminal liability. FACS will investigate incidents involving such violations and will involve and will co-operate with law enforcement officials if a criminal violation is suspected.

It is explicitly prohibited to send unsolicited bulk mail messages ("junk mail" or "spam") of any kind (commercial advertising, political tracts, announcements, etc). This is strongly objected to by most Internet users and the repercussions against the offending party and FACS can often result in disruption of service to other users connected to the Service. Users may not forward or propagate chain letters nor malicious e-mail.

Equipment delivered to User by FACS is the responsibility of User until received by FACS and shall be maintained and returned in same condition as delivered. User shall keep all equipment leased or otherwise

delivered to User by FACS free and clear of any liens or encumbrances. Any and all damages to equipment while in Users possession, whether caused and/or inflicted by User or another party, is the responsibility of the User and Client and FACS reserves the right to charge for all reasonable hardware and time costs necessary to repair and/or replace the equipment.

A User may not attempt to gain unauthorized access to, or attempt to interfere with or compromise the normal functioning, operation or security of, any portion of the System. A User may not use the Service to engage in any activities that may interfere with the ability of others to access or use the Service or the Internet. A User may not use the Service to monitor any data, information or communications on any network or System without authorization. A User may not attempt to gain unauthorized access to the user accounts or passwords of other Users.

Users are entirely responsible for maintaining the confidentiality of password and account information, as well as the security of their hardware. Users agree immediately to notify FACS of any unauthorized use of their account or any other breach of security known to them. If users become aware of any violation of this Policy by any person, including Users that have accessed the Service through the user's account, the users are required to notify FACS.

Upon receipt of a complaint, or having become aware of an incident, FACS reserves the right to: a) inform the User's manager of the incident and require the manager or other supervisor to deal with the incident according to this AUP; b) suspend the User's account and withdraw the User's network access privileges completely; c) charge the User and Client for administrative costs as well as for machine and human time lost due to the incident; d) suspend access of the Client's entire network until abuse can be prevented by appropriate means; e) share information concerning the incident with other Internet access providers, or publish the information, and/or make available the Users' details to law enforcement agencies.

Any one or more of the steps listed above, insofar as they are deemed necessary by FACS in its absolute and sole discretion, may be taken by FACS. All cases of violation of the above Policy should be reported to [support@facsware.com](mailto:support@facsware.com).

FACS reserves the right to add, delete or modify any provision of this Policy at any time without notice, effective upon posting of the modified Policy at [www.FACSware.com/AUP](http://www.FACSware.com/AUP)