Social Media Policy

POLICY

This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner.

PROCEDURES

The following principles apply to professional use of social media on behalf of Apogee Security Services as well as personal use of social media when referencing Apogee Security Services.

- Employees need to know and adhere to the Apogee Security's Code of Conduct, Employee Handbook, and other company policies when using social media in reference to Apogee Security Service.
- Employees should be aware of the effect their actions may have on their images, as well as Apogee Security's image. The information that employees post or publish may be public information for a long time.
- Employees should be aware that Apogee Security may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to Apogee Security, its employees, or customers.
- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment.
- Employees are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the Human Resources Department and/or supervisor.
- Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorized Apogee Security spokespersons.
- If employees encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of a supervisor.
- Employees should get appropriate permission before you refer to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.

- Social media use shouldn't interfere with employee's responsibilities at Apogee Security. Apogee Security's computer systems are to be used for business purposes only. When using Apogee Security's computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, Apogee Security blogs and LinkedIn), but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.
- Subject to applicable law, after-hours online activity that violates the Apogee Security's Code of Conduct or any other company policy may subject an employee to disciplinary action or termination.
- If employees publish content after-hours that involves work or subjects associated with Apogee Security, a disclaimer should be used, such as this: "The postings on this site are my own and may not represent Apogee Security's positions, strategies or opinions."
- It is highly recommended that employees keep Apogee Security related social media accounts separate from personal accounts, if practical.

Employee Signature_____

Print Name_____

Date_____