Perimeter SOLUTIONS
Quality Products. Exceptional Response.

Rev Aug 2020

Perimeter Solutions 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, image boards, comments sections, file sharing 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 Perimeter Solutions as well as personal use of social media when referencing Perimeter Solutions.

- Employees need to know and adhere to the Company's Code of Ethics, Employee Handbook, and other company policies when using social media in reference to Perimeter Solutions.
- Social media for personal use is permitted as long as it is in accordance with the Company's policies and as long as it does not interfere with productivity.
- Employees should be aware of the effect their actions may have on their images, as well as Perimeter Solutions' image. The information that employees post or publish may be public information for a long time.
- Employees should be aware that Perimeter Solutions may observe content and information made available by employees through social media, including on personal social media sites. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to Perimeter Solutions, 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. Posting prohibited social media material may lead to disciplinary action.
- 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, the Legal Department and/or their 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 the Legal Department.
- If employees find or encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and notify the Human Resource Department.
- 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 Perimeter Solutions. Perimeter Solutions computer systems are to be used for businesspurposes only. When using Perimeter Solutions computer systems, personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.
- Perimeter Solutions' social media accounts are managed by Resource Advantage. Please contact Resource Advantage for any questions, inquiries or posts related to Perimeter Solutions' social media accounts (ex: Facebook, Twitter, Instagram, Youtube, Perimeter Solutions blogs and LinkedIn).
- Resharing company sponsored public posts is allowed. (i.e.: retweeting a company tweet)
- Subject to applicable law, online activity that violates Perimeter Solutions' Code of Ethics, Perimeter Solutions' Employee Handbook, his policy 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 Perimeter Solutions, a disclaimer should be used, such as this: "The postings on this site are my own and may not represent Perimeter Solutions' positions, strategies or opinions."

Precautions from the IT Department:

- Practice safe behavior with email. Do not open any attachments or visit scrupulous links. Computers are equipped with security measures, but they are never failsafe.
- For internal social media and file sharing use check with IT for approval to make sure it is a secure platform. There are several pre-approved tools that exist (SharePoint, Teams, OneDrive, etc.)
- Protect company information, if sharing files externally use authorized platforms. Restrict content behind passwords, set time limits, etc.
- It is recommended to keep your network private and only admit people you know intothe network. This can help reduce the chance a criminal can use information for nefarious reasons.