Social Media 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, micro blogs, 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. The following principles apply to professional use of social media on behalf of Secure Risk Management Limited as well as personal use of social media when referencing Secure Risk Management Limited:

- Employees need to know and adhere to the Company's Code of Conduct, Employee Handbook, and other company policies when using social media in reference to Secure Risk Management Limited.
- Employees should be aware of the effect their actions may have on their images, as well as Secure Risk Management Limited image / reputation. The information that employees post or publish maybe public information for a long time.
- Employees should be aware that Secure Risk Management Limited may observe content and information made available by employees through social media. Employees should use their best judgement in posting material to ensure that it is neither inappropriate nor harmful to Secure Risk Management Limited, 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, libellous, or that could potentially 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 always 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 Secure Risk Management Limited spokespersons.
- 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 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 Secure Risk Management Limited. Secure Risk Management Limited Computer systems are to be used for business purposes only. When using Secure Risk Management Limited computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, Secure Risk Management Limited blog sand LinkedIn), but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.
- It is highly recommended that employees keep Secure Risk Management Limited related social media accounts separate from personal accounts, if practical.

Signed: _____ **Position:** Managing Director **Date**: 1st December 2024