

Information and Financial Security Policies

1. SLP states the purpose of the Information Security Policy as - to protect the confidentiality, integrity, and availability of the firm's information assets, including client data, intellectual property, and sensitive business information. SLP also defines the scope of the policy and specifies the information assets and systems to which the policy applies - including computers, networks, cloud services, decks, presentations, and data provided by the partners or clients.
2. All information related to SLP's clients, partners, vendors, other team members, and projects must remain confidential and within the knowledge of only the team members with whom the information is entrusted.
3. SLP's document repository establishes and categorises information assets based on the projects and ownership.
4. Employees who use personal devices for work purposes must address confidentiality to SLP's client and SLP resources, data protection, and compliance with the policy.
5. Payments made by SLP to organisations must need a contract, an invoice, an electronic mail check by SLP with the corresponding organisation's contact persons listed on the organisation's website and who must not be the person with whom financial transaction is initiated; a telephonic check by SLP with the corresponding organisation's contact persons who must not be the person with whom financial transaction is initiated.
6. Payments made by SLP to individuals must need a contract, an invoice, an electronic mail check by SLP with the corresponding individual on the email address at which non-financial project work was initiated; a telephonic check by SLP with the corresponding individual on the phone number at which non-financial project work was initiated.