**Information Security Policy**

Information Security and adherence to security practices in compliance with industry standards adopted by software development industry and information security needs of the customer within the framework of Local and Federal Government is one of the top priorities of Nexelus. This is to ensure the protection of its intellectual property from all threats - internal or external, intentional, or accidental and natural disasters. In addition, achieving this goal Nexelus will ensure the following:

* Confidentiality of information assets is ensured, but not limited to third parties, Company Operational, personal, and electronic or electronic communications.
* A Business Continuity Management Framework will be made available and Business continuity plans will be developed to prevent disruption of business operations and to protect critical business processes from the consequences of major failures or disasters. Business continuity plans should be maintained and evaluated.
* All information security breaches, real or suspected, will be reported and investigated by the appropriate authorities not limited to the System Administration and Incident Response team.
* Appropriate access controls will be maintained, and data will be protected from unauthorized access. As such but not limited to:
  + Confidentiality, integrity, and availability to information are maintained throughout the process.
  + Access to information and information systems will be met as required by context and supporting business activities.
  + All managers are directly responsible for implementing the Security Policy within their respective departments.
  + Data security is managed through the NEXELUS Risk Management framework.
  + It is the responsibility of all staff to adhere to the Security Policy.
* A risk management framework will define risk and its management of all company assets (tangible / intangible and human). Individual risks are assessed and targeted at all risks, using appropriate risk mitigation controls and emergency plans are defined with unacceptable residual risk levels.
* All business assets (tangible / intangible with people) have a safe and secure environment.
* Employees are provided conducive work environment, free from accidental and occupational hazards.
* All employees are trained in information security functions, roles, and responsibilities.
* Physical, sensible, and remote access to all business assets (tangible / intangible), details and tangible locations are monitored and controlled.