Position Name:	Local Information Security Officer
Department:	Information Technology
Grade:	Asst. Manager
Vacancy:	1
Qualification:	Post graduate in Computer Science or Computer Management, Certified Information Systems Auditor (CISA)/ (CISM) / CISSP
Experience:	3+ years
Location:	Aurangabad
Reporting to:	HOD - IT

Position Requirement:

1. Communication
2. Presentation
3. Risk Analysis
4. ISO27001 Knowledge
5. Documentation, Reporting and Analytical Ability

Purpose of Position:

1. To Act as Local Information Security Officer of SAIPL
2. Ensures IT security in company in respect to concern IT standards
3. To coordinate development and delivery of comprehensive information security program for SAIPL.
4. To cooperate in auditing SAIPL information technology infrastructure and security.
5. Validate the effectivity of security measures
6. Rollout/Maintains of ISMS in SAIPL

Tasks:

1. Coordinates Internal & external IT audit activities and planning of audit engagements.
2. Verifies that company employees are adhere to, and follow, IT safely and security guidelines as established by management.
3. Plans testing issues to ensure that proper controls are in place and Verifies that information contained within IT systems is accessible by authorized personnel only.
4. Executes and implements ongoing risk assessment program targeting information security and privacy matters; recommended methods for vulnerability detection, remediation and oversee vulnerability testing.
5. Performs the audits and writes reports of the misstatements, weakness and security risks to management.
6. Sets down methods to stay up-to-date for latest security and privacy advisories, alerts and vulnerabilities pertaining to SAIPL.
7. Performs as official campus contact point for information security, privacy and copyright infringement incidents, including relationship with laws enforcement agencies and Coordinates as cyber expert in the event of cyber incidence & assist SAIPL to deal with govt. authorities.
8. Manage the development and implementation of global security policy, guidelines and rules & procedures to ensure ongoing maintenance of security.
9. Maintain contacts with local, state & federal law enforcement and other related government agencies.
10. Participation in Information System Security committees (Region APAC)
11. Coordinates Service Level Agreements/Operational Level Agreements for SAIPL
12. Plans and promotes awareness and education of Information Security

13. Drafts and maintains documentation like PR, GRN preparation
14. Manages Data Center components