IT GOVERNANCE

The purpose of this policy is to provide regulatory compliance, cost control, risk management and monitoring of proposed and existing business application and IT infrastructure

LEGAL COMPLIANCE

All necessary procedures shall be carried out so as to safeguard the organization from violating any legal obligations. The following guidelines are to make Company's information processing personnel's aware of and from violating any copyright laws or materials having any legal binding associated with it.

i. Adequate precaution would be taken on material for which there may be intellectual property rights (such as copyright, design rights or trademarks etc.).
ii. Important Company corporate records shall be safeguarded from loss, destruction and falsification (and within the legislative or regulatory environment which the organization operates).
iii. All relevant statutory, regulatory and contractual requirements shall be explicitly defined and documented for each information system.
iv. Any requirement for disclosure of internal correspondence to external agencies like courts would need to be complied with.
v. Legal advice shall be sought before cryptographic controls are implemented or exported.
vi. To ensure admissibility of evidence in case of an incident, consideration should be given to ensure that information systems comply with applicable published standards (or codes of practice) and rules for evidence laid down by the relevant law or court.
vii. There should be procedures and controls in place to ensure that the SRNL Construction IT facilities are used only for authorized business purposes.
viii. Information systems should be regularly checked for compliance with security implementation standards.
ix. Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes.
x. All users are expected to comply with the Information Technology related Rules, Regulations and notifications for the respective Country. Any breach of the same shall initiate disciplinary actions as mentioned elsewhere in this document and also civil and criminal actions as mentioned in the Statute.

xi. All charges for violation of the aforementioned statutes shall lie on the person individually and Company shall not undertake any liability merely because of the ownership of the assets in question.

INFORMATION SECURITY MANAGEMENT

This policy provides directions to develop and implement the Information Security Incident Management Process for networks and computers, improving user security awareness, early detection and mitigation of security weaknesses/incidents and suggesting the actions that could be taken to reduce the risk due to security weaknesses or incidents.

1. INCIDENT IDENTIFICATION

A security incident could be defined as an act of violating the IT policy. The following is an illustrative list of what actions can be classified as incidents:-

i. Attempts to gain unauthorised access to a system or its data, masquerading, spoofing as authorised users.

ii. Unwanted disruption or denial of service.

iii. Unauthorised use of a system for the processing, transmitting or storing data by authorised/ unauthorised users.

iv. Changes to system hardware, firmware or software characteristics and data without the knowledge of application owner and/ or Existence of unknown user accounts.

v. Whenever any employee notices or suspects any breach as mentioned above, respective IT Head would be informed immediately.

vi. Users shall not attempt to perform any investigations at his end which could unintentionally compromise investigation or contaminate evidence. The user shall not contact individual or Organization that are suspected of being the source of incident unless directed to do so by CEO.

2. ACCESS CONTROL POLICY

Appropriate logical and physical access control shall be put in place to ensure that information assets of SRNL Construction are provided comprehensive protection against unauthorised access.

2.1. LOGICAL ACCESS CONTROLS

To provide logical access to employees and third party staff on information assets (hardware, software, applications, etc.), it is important to give each individual a logical identity with which he/she shall be identified and authenticated by the IT systems.

2.1.1. User Access Management

i. User IDs shall be unique to each individual and a password known only to the owner of the User ID.

ii. Appropriate authorization shall be obtained from Department head through HR Department prior to creating the user IDs.

iii. An audit trail shall be kept of all requests to add, modify or delete user accounts/IDs and access rights.

iv. System privileges shall be assigned to roles rather than users.

v. A list of user IDs and the rights assigned to them shall be maintained and updated regularly. This list shall be reviewed periodically at least once in a quarter with HR data and business owners to maintain the desired level of authorization.

vi. Upon termination of their employment, contract or agreement, the access rights of all employees and third party staff to information assets shall be revoked. These user IDs shall be disabled for a specified duration (as directed by the employee's reporting manager or HR), and removed from the system.

vii. A review to identify the inactive or dormant user IDs shall be conducted at regular intervals (at least once every 6 months). Dormant or inactive user IDs that are no longer required shall be removed from the systems.

viii. Administrative rights for users who have access to critical information systems/ applications shall be reviewed at regular intervals at least once every quarter. The review / audit to be carried out by Relevant Department Heads.

2.1.2. Account Controls and Privilege Management

i. Account lockout threshold shall be configured in systems to ensure that user accounts are locked out after a predefined number of failed logon attempts.

ii. Account shall be locked out permanently after 5 (maximum) continuous bad attempts made by user.

iii. The privilege associated with each system (e.g. operating systems, databases, applications etc.) and their corresponding users shall be identified.

iv. Privileges shall be allocated to individuals on a 'need-to-have' basis in strict adherence to the authorization process for privilege access. Allocation of Privileged id shall be approved by the personnel authorized by IT Head / Department Head.

v. A record of all privilege accounts used on SRNL Construction information systems shall be maintained.

vi. Changes made to privilege accounts shall be logged.

vii. Authorizations for special privileged access rights are reviewed at once in 6 months.

viii. Whenever a user is transferred from one function/ geography to another function/ geography within SRNL Construction, the user access rights are to be revoked and re-allocated appropriately upon intimation from HR / Department Heads.

ix. All applications/databases wherever possible shall use inactivity timeout. Users shall be required to re-authenticate themselves after a specific period of inactivity (30 minutes) specifically on sensitive applications such as those involving financial information, organizational Intellectual Property, etc.

2.1.3. Password Controls

i. Users shall be forced to change the password on their first logon.

ii. All vendor-default user accounts in the information systems shall be disabled and passwords shall be modified to a different password.

iii. Passwords shall be distributed to users in a secure manner.

iv. Maximum password age shall be configured to 120 days, after which the account shall get locked if user fails to change his/her password within this period.

v. Users shall be notified to change their password 14 days prior to expiry. At least 5 reminders shall be sent to users warning them about the account lockout in case they fail to change their passwords.

vi. Password history shall be enforced, so as to restrict employees from using previous 3 passwords.

vii. Minimum password length shall be configured in systems to enforce the least number of characters that a password for a user account may contain. This value shall be 8.

viii. Password shall contain a number, combination of lower and upper case and/or special characters. Password shall be a mix of at least two types of non-alphabetic characters.

ix. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) shall be changed on at least a quarterly basis.

x. Passwords shall not be displayed in clear text when they are being keyed in, during transmission over public networks, or storage.

xi. Password Reset process shall be put in place to deal with the forgotten passwords and account lockouts. User password resets shall be performed by the respective administrator or authorized personnel only when requested by the individual to whom the user ID is assigned, after verification of his/her identity.

xii. A secure 'Password List' shall be maintained for all critical accounts. Only authorized individuals shall have access to this 'Password List'.

2.1.4. Guidelines for Password Construction

Passwords are used for various purposes at SRNL Construction. Some of the most common uses include: user level accounts, web accounts, email accounts and local router logins. Following are the guidelines for users to choose 'easy to remember but difficult to guess' password.

i. Contain both upper and lower case characters (e.g., a-z, A-Z).

ii. Have digits and punctuation characters as well as letters e.g., 0-9,!@#$ %^&*()_+|~-=\`{}[]:";'<>?,./).

iii. Server Administrator must use at least one ASCII characters in the password for the servers

iv. Standard user may or may not use ASCII characters in the password sequence.

v. Are at least eight alphanumeric characters in length

vi. Are not words in any language, slang, dialect, jargon

vii. Are not based on personal information, names of family etc.

User shall create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use any of the above examples as passwords!

2.2 PHYSICAL ACCESS CONTROLS

i. Access to offices, facilities and secure areas (such as Server Cabinet) shall be provided to authorised personnel only. Access to secure areas shall be controlled and monitored.

ii. All employees of SRNL Construction, third party staff, visitors such as clients, vendors, sub-contractors etc shall be required to display their ID cards at the office premises.

iii. All facilities shall remain secured before, during and after office hours or when unattended.

iv. Appropriate level of security controls including CCTV shall be implemented to prevent unauthorised access in office areas and facilities hosting critical equipment and data centres.

v. The movement of all incoming and outgoing information assets shall be checked and documented

vi. There shall be Implementation of appropriate fire protection measures, including installation of fire-suppression systems in areas such as Server deployed.

vii. Air-conditioning and humidity control systems to support information systems and equipment shall be placed accordingly in Server Area.

2.3 PORTABLE COMPUTING POLICY

Appropriate measures would be taken regarding the use of portable computing device. The purpose of this policy is to provide guideline for the use of mobile computing devices and their connection to the Company network.

i. Only Company approved portable computing devices should be used to access SRNL Construction Information Resources.

ii. Non Company computer systems that require network connectivity must be approved in writing by the Head of IT.

iii. Unattended portable computing devices must be physically secure. This means they must be locked in an office locked in a desk drawer or filing cabinet.

iv. Portable computing devices must be password protected.

v. Company data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols.

vi. Remote access to IT resources through SSL channel and should be rule based.

3.0 NETWORK SECURITY AND OPERATIONS MANAGEMENT

Adequate network controls shall be implemented by the IT function to ensure all devices connected in the network are securely configured, with appropriate controls for authentication, authorisation and accountability in place.

3.1 NETWORK CONTROLS

i. LAN and WAN shall be divided into sub-networks, protected by rule-based traffic filtering using firewalls, Virtual LANS and other appropriate technology.

ii. A De-militarized Zone (DMZ) shall be created with respect to devices whose security level does not warrant it to be placed on the internal network, such as Public Web Server that is accessible by anyone. Only non-critical mission Servers are allowed to host in this DMZ zone.

iii. The information systems, devices, applications, services, etc. which need to be placed in DMZ shall be identified and approved. Mission critical Servers may be hosted in another dedicated DMZ zone with very restrictive firewall policies if required

iv. Access to public web servers may be provided to our customers on case to case basis.

v. A list of unauthorized (non-essential or vulnerable) services and protocols shall be created and updated regularly. These unauthorized services shall be disabled or if possible, removed, from the IT systems connected to SRNL Construction network.

vi. Any default or non-essential network services and protocols shall be removed or disabled on the devices connected to the network.

vii. Clear text protocols (Telnet, FTP, etc.) shall not be used for device management or file transfers. The usage of secure protocols such as SSH, SFTP and SCP is highly recommended.

viii. Generic IDs and anonymous access to any administration or file transfer shall be disabled.

3.2 REMOTE ACCESS

i. Equipment that provides access to SRNL Construction network shall positively identify the user through a login sequence prior to providing access

ii. Remote Access will be allowed for users to any transaction based system. Such users with 10 minutes session inactivity shall be automatically disconnected. For System Administration, Maintenance or Development activities, inactivity activation period would be decided by the Head of IT and such access would be provided only personnel or agencies that might have to carry out such activities remotely.

4.0 E-MAIL SECURITY

As a productivity enhancement tool, SRNL Construction encourages the business use of electronic messaging systems for its employees. E-mail security is of prime importance and appropriate technological

and user level controls shall be implemented to maintain the confidentiality, integrity and availability of the E-mail system.

The objectives of the E-mail policy are to:

- Establish the rules for the business use of E-mail system of SRNL Construction and to adequately protect the information transmitted through E-mails
- Ensure that the E-mail system of SRNL Construction is not used for malicious activities.

4.1 AUTHORISED USE OF E-MAIL

i. All messages generated by the E-mail System are considered to be the property of SRNL Construction.

ii. The E-mail system should be used for business purposes only. However, Personal use of E-mail systems is allowed to a reasonable extent as long as that does not compromise company information and/ or reputation of SRNL Construction.

iii. If users receive any offensive or unsolicited material from external sources, they shall not forward/ redistribute it to either internal or third parties unless to the IT Team for further incident investigation.

iv. Users shall not share their E-mail passwords with other users.

v. Email Quota is categorized in size of 250 MB and 1 GB.

vi. All Departmental heads, project directors to be assigned e-mail quota of 2 GB. All others users would be assigned disk quota of 250 MB. Additional disk quota will be treated as an exception and will need Department Head and IT Head approval.

vii. Promotional mails would not be circulated unless approved by IT Head/Corporate Communications. Promotional mails would include "Road Shows by other Companies for sale of their products which might include cars, mobile phones, mobile schemes etc."

viii. Employees are strongly discouraged to send mails such as season greetings, chain being using SRNL Construction infrastructure resources.

4.2 PROHIBITED USE

The use of the E-mail System is strictly prohibited for the following activities:

i. Charitable fundraising campaigns, political advocacy efforts, private business activities or personal amusement and entertainment.

ii. Creating or distributing any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs or national origin.

iii. Forwarding or sending messages that have racial or sexual slur, political or religious solicitations or any other message that could damage the reputation of SRNL Construction.

iv. Transmitting any material that potentially contains viruses, Trojan horses, worms, time bombs or any other harmful or malicious program.

v. Sending / Storing audio, video files on mail servers, desktops, file servers.

vi. Defaming abusing, harassing, stalking, threatening or otherwise violating any legal and privacy laws.

vii. Using it in connection with surveys, contests, chain letters, junk E-mail, spamming, or any duplicative or unsolicited messages or

viii. Mail-bombing the other users.

4.3 USER ACCOUNTABILITY

i. The access of web mail services (e.g. Yahoo mail, outlook mail, Gmail etc.) will be provided only if the business requirement so justifies it, with prior approval of the Department HOD.

4.4 USER IDENTITY

i. Misrepresenting, obscuring, suppressing or replacing another user's identity on an electronic communications system is forbidden.

ii. The user name, electronic mail address, organisational affiliation and other information related to electronic messages or postings shall reflect the actual originator of the messages or postings

iii. At a minimum, users should provide their name and phone numbers in all electronic communications. Electronic mail "signatures" indicating job title, company affiliation, address and the other particulars are recommended for all E-mail messages.

4.5 CONTENTS OF ELECTRONIC MESSAGES

i. Users shall not use profanity, obscenities or derogatory remarks in electronic mail. The users caught in such action shall be subject to disciplinary actions.

4.6 INCIDENTAL DISCLOSURE

i. In case of business need it may be necessary to view the content of an individual user's communications. Approval for such access shall be taken from the Department heads/ CEO.

ii. However in case of technical support IT personnel may need access to individual's user id and password.

4.7 MONITORING AND ENFORCEMENT

i. The users shall have no expectation of privacy in anything they store, send or receive on the E-mail system. SRNL Construction reserves the right to monitor the messages without prior notice.

ii. Users of the E-mail system are required to comply with the E-mail Security Policy. Failure to comply may result in disciplinary action.

4.8 EMAIL ETIQUETTES

i. Users should make judicious use of "Reply All" and "Forward" buttons/options. In case the reply is not required to be sent to all, reply button should be used instead of reply all. While replying or forwarding, adequate care should be taken to remove attachments if they are not required. This is to avoid clogging of mail boxes and mail server thereby slowing down the entire mailing system of the Company.

5. SYSTEM SECURITY

5.1 CRITICAL DATA SECURITY

i. The critical systems, information, data that necessitates such grading based on its content and value to competition and outside world shall be identified.

ii. Access controls shall be put in place to maintain secrecy of information whether it resides on the client or the server side to maintain confidentiality, integrity and availability.

iii. All critical file transfers shall be done over a secure channel such as SCP, SFTP, etc.

5.2 SECURE CONFIGURATION OF DEVICES

i. All the systems shall be configured with up to date Anti-virus definitions and signatures.

ii. The changes on any of the critical systems shall be logged and audit trails maintained which contains user id and time of modification.

iii. Operating systems shall be configured to time-out/terminate on-line sessions after 10 minutes of inactivity.

5.3 USE OF REMOVABLE MEDIA

i. Removable Media ports/interfaces (USB Storage Devices, CD, DVD) usage within the Organization in general, shall be controlled by disabling the Removable Media Interfaces for all standard desktop / Laptop users except for USB mouse, blue tooth danglers.

ii. Wherever a business justification exists for the use of Removable Media, users shall seek approval from IT HOD and Head of the Department prior to use of such media. IT Function shall provide removable media access to the user only after reviewing business justification, availability of alternative mechanisms, and compensatory security controls with the IT. For power users who wish to take their own backups in media would have the USB port enabled. A list of power users would be prepared by Head of IT in consultation/approval with/from HOD/CEO.

iii. Specific time limits shall be allowed for enabling the removable media ports in Desktops & Servers. Access shall be reviewed based on the timeline.

iv. Removable media access shall be reviewed every 6 months

v. Employees shall store and keep their official removable devices securely to avoid any theft or unauthorized data access.

Control of Technical Vulnerabilities

i. The IT shall identify and document all technical vulnerabilities of information systems and evaluate the exposure to such vulnerabilities. Appropriate measures shall be taken to mitigate the associated risk.

ii. The IT Department shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability assessment and vulnerability closure.

INTERNET USAGE POLICY

i. Employees shall be provided with Internet access on documented business justification. IT shall take due care to filter objectionable sites and mail services.

ii. Any personal use shall not interfere with normal business activities, involve solicitation, be associated with any for-profit outside business activity and potentially embarrass the company.

iii. Users are prohibited from transmitting or downloading material that is obscene, pornographic, threatening and racially or sexually harassing.

iv. Approved sources for licensed software shall be made available to users. Users are prohibited from downloading any software from the Internet.

6. CHANGE MANAGEMENT

The goal of the Change Management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change related incidents upon service quality, and consequently to improve the day-to-day operations of SRNL Construction.

i. Assessment of the potential impact, including security impact of the proposed change(s) on critical systems shall be carried out.

ii. All approved change(s) on the critical systems shall be tested prior to implementing them on the production system.

iii. A Rollback plan for aborting and recovering from failed change(s) shall be documented before performing the change.

iv. All application changes would be done after following a proper approval system. The changes should be approved by the respective functional leads before being taken up by IT Department for carrying out the change.

v. Any changes in the configuration of any Network equipment or architecture should be recorded with proper reasons and approval obtained from Head of IT.

vi. Any Changes to the configuration of the Server in the form of Patch deployment, upgrade of Operating System should be recorded with proper reasons and approval obtained from Head of IT.

vii. As a standard deployment policy, all servers being deployed for production should have only the standard ports open and should be approved by Head of IT. This would be designated as base security configuration for Servers.

viii. All the approved change requests must be carried out only during the last week of the month

ix. In case of an Emergency Change request, the IT Head would take the decision, implement the change and document the same via exception handling

x. Development servers and Production servers should have the same deployment levels so that VA can be conducted on the same.

7. BACKUP POLICY

All critical data shall be appropriately backed up and secured. The purpose of this policy is to define guidelines for the secure backup and storage of Company's Electronic information assets.

Information Assets to be backed up:

i. Mail

ii. ERP and any other business application database

iii. Financial Database and Vault

iv. File Server

Frequency of Backup, type of backup and retention

i. First backup - full

ii. Daily backup incremental

iii. Weekly backup full

iv. Backups is to be retained and maintained for 2years

v. Automatic alerts should be sent from the backup software to administrator in case of any failures. The same should be recorded as an incident and rectified immediately either through a full backup or through the run-up incremental backup.

vi. The Backup storage would be labelled with sensitivity classification.

8. Online Storage

i. Online storage with snapshot and De-duplication would be retained for a period of 14 days in the Email Solution Providers Cloud System.

Periodic testing of Backup

i. Backup should be restored at least once a month for each of the information asset being backed up.
ii. The restoration should be tested for online storage.
iii.

9. INFORMATION DISCLOSURE POLICY

No Organizational information shall be publicized or given to third parties without prior authorization (limited to IT Security). This policy defines guidelines for making Company information public (both paper and electronic). Proper protection of this information is essential if the interests of not only SRNL Construction, but also customers and business partners, are to be preserved. These interests include maintenance of competitive advantage, trade secret protection, and preservation of personal privacy.

i. Unless it has specifically been designated as Public, all internal information must be protected from unauthorized disclosure to third parties.
ii. If any information needs to be made public and it falls within the limits of the approved limited of recipients then no Owner approval will required.
iii. The disclosure of sensitive information to consultants, contractors, and any third party must always be preceded by the receipt of a signed non-disclosure agreement (**NDA**). NDA format should be provided in the respective letter head of the Company incorporating the related changes.
iv. Unless an employee has been authorized by the information Owner to make disclosures, all requests for information must be referred to the Public Relations. Such requests include questionnaires, surveys, newspaper interviews, and the like.

    Specific information about company's internal events, including new products and services, staff promotions, reorganizations, and information system problems, must not be released to third parties, including members of the news media, without specific authorization from corporate communication

10. ASSET DISPOSAL POLICY

IT assets and Physical media (Viz. Hard Disk, Tapes, SD Cards, CD and DVD) should be disposed of in a secure manner. This policy defines guidelines for the secure disposal of Company's Media / Information (Electronic).

i. Secure methods will be used to dispose of electronic data and output. Head of IT or any nominated member of his team is responsible for overseeing the destruction of electronic copies containing confidential information. Employees may dispose of the electronic data themselves using the following methods:
    - Removing data by formatting disk drives before being sold or Replaced
    - "Degaussing" computer tapes to prevent recovery of data
    - Erasing CD/DVD to be re-used to prevent recovery of data

- Destroying discarded CDs/DVDs
- Microfilm must be cut into pieces or chemically destroyed
- Deleting on-line data using the appropriate utilities

ii. Personnel should not discard business related information in trash bins, and insecure disposal bags. Instead, information must be personally shredded or placed in secure recycling bag. This is applicable for both physical and electronic information.

iii. Documents that have reached their retention period must be securely destroyed following the guidelines as listed. If hardcopy cannot be shredded (like paper or microfilm), they should be incinerated.

11. EMPLOYEE SEPARATION POLICY

Upon resignation or termination of an employee, it should be ensured that no IT asset misused by the outgoing employee. The purpose of this policy is to provide IT Department the right to close all related accounts of the outgoing employee and take possession of the IT Assets in order to avoid misuse. In the event of an **IT administrator** separating out of the Company, adequate precautions would be taken to ensure the new Administrator is assigned all privileges and the outgoing administrator "admin accounts" are changed/sealed/closed well in advance to avoid any breach of security.

UNDERTAKING

I _____, _____ (designation) do hereby undertake that except with the prior consent of SRNL Construction Pte Limited in writing, I shall not disclose to any third party any other information that I may acquire in relation to any Contract whether in writing or orally including but not limited to documents, material, specifications, drawings, reports, trade secrets and data (known collectively as "Confidential Information").

Notwithstanding the foregoing, I the undersigned during the discharge of my duties and in good faith may disclose the "Confidential Information" to other employees and / or persons who are required to have knowledge thereof in relation to such "confidential Information" and who have been informed about the confidential nature of such Information or the information which is in the public domain or its disclosure is required under the Law. I have executed this undertaking voluntarily in order to keep such Information confidential and to use the Confidential Information only for the purpose for which it is meant for.

_____ (Signature)

_____ (Date)

_____ (Name)

_____ (Designation)