Information Security Sustenance Policy

1 Objective

This policy addresses aspects of compliance required to be adhered to and fulfilled with respect to APAR Information Security Policies. This policy also addresses the compliance requirements pertaining to relevant statutory legislations, contractual and regulatory obligations which the Organization is supposed to adhere to and fulfil so that it could help the Organization establish, maintain and sustain the desired information security posture.

2 Scope

This policy is applicable to all corporate offices and all the plant locations of APAR.

3 Policy

3.1. APAR has instituted a comprehensive set of Information Security Policies to protect the confidentiality, integrity and availability of its information assets. In order to ensure that policy deployment and implementation stays consistent, APAR shall establish an audit and review mechanism to ensure implementation and compliance to the policy is maintained.

3.2. APAR shall develop necessary systems and procedures to measure the effectiveness and to ensure continual improvement of the Information Security Policy.

3.3. The monitoring process for information security shall be done through the following mechanisms:

3.3.1. Periodic Review of implementation of Controls

(a) The Information Security Officer shall create an implementation roadmap (in terms of addressing Gaps, implementing controls from RA) for the respective business units based on the Information Security Policy, Procedures and Guidelines and the outcome of the Risk Treatment Plan and submit the same to CISO (Chief Information Security Officer) on yearly basis.

(b) The organization, Information Security Officer shall submit a status report of the implementation roadmap to the CISO at regular intervals bi-annually.

3.3.2. Internal Information Security Audits:

(a) The CISO shall ensure that the internal information security audits to check for compliance with Information Security Policy are conducted bi-annually. The internal information security audits shall also extend to

information security audits of Outsourced Service Providers to whom any of the activities of the Organization have been outsourced.

(b) CISO shall ensure that at least two information security audits in a year are conducted in the group.

(c) The Information Security Officer shall be responsible for approval and implementation of the corrective plan and closure of information security audit observations through submission to the CISO.

3.3.3. Audits by Third Parties:

(a) APAR shall appoint an independent third party to audit the Information Security Policy annually.

3.3.4. Periodic Reporting to ISAC:

(a) CISO based on the inputs provided by the Information Security Officer of location shall apprise the ISAC (Apex Committee) at regular intervals about information security posture once every 6 months at the minimum and Apex Committee shall review it. This shall include but is not limited to the following.

(b) Key issues from implementation plans and their progress.

(c) Major findings from internal information security audits.

(d) Major findings of independent audits by third parties.

3.3.5. Identification of Applicable Legislation:

(a) Through the Organization's Legal department, the ISAC/CISO shall be provided inputs on the applicable legislations, amendments, new rulings, notices in the gazette, promulgation of new laws, by laws, acts which shall have a bearing on the organization's Information Security. The CISO shall propagate the relevant aspects of applicable legislations to the rest of the Infosec Organization on a need to know and act basis.

3.3.6. Protection of Intellectual Property Rights:

(a) The Organization shall always ensure that Information assets; which it has procured, developed, modified; adhere to the legislative, contractual and regulatory requirements, does not contravene any of the applicable Intellectual Property Rights Laws.

(b)The Organization shall also protect its information assets of from the above mentioned when it gets into agreements with 3rd party through a clear mention of the applicable clauses in the contracts; which shall safeguard the Organizations interests in the light of any violation caused by the external party.

(c) No unauthorized software (including freeware, shareware) shall be used on any of the information systems of APAR.

(d) Unauthorized printing, photocopying, electronic transmission, and publishing in print media of copyright protected material of APAR or any such material which has been brought by APAR for business use is prohibited.

3.3.7. Protection of Organizational Records:

(a) All records as mandated by statutory/legal/regulatory authorities in India or of foreign origin, for which the Organization is responsible for compliance, shall be protected from damage through natural or manmade causes.

(b) APAR shall ensure that there is no misappropriation, falsification of records or their integrity confidentiality and availability is not compromised in any manner during their lifecycle from creation to destruction.

(c) The retention limit of statutory records shall be as mandated by the applicable legislation. However for business records/documents, the business group heads and or HODs shall determine the retention limit.

3.3.8. Data Protection and Privacy:

(a) The Organization shall always seek to protect the privacy of the personal information of its customers, employees and 3rd parties with whom the Organization has signed 3rd party agreement. Divulging of company facts shall only be done in keeping with statutory / contractual / regulatory / legal requirements. Such information shall always be protected from getting misused, leaked or falsified or traded with any interested party. A serious view as per the code of conduct policy shall be taken, shall a transgression of this nature is to occur or is detected. Should there be a change in the third party agreements the concerned department shall share the updated copy to the CISO and others concerned immediately.

3.3.9. Prevention of Misuse of Information Assets:

(a) All identified information assets of the Organization shall be productively used for official purposes only. Any unauthorized use of information assets shall be dealt with a disciplinary action. The stakeholders of the Organization shall be formerly communicated on a regular basis about this. This shall be done as per the Acceptable Usage of Office Equipment Policy and Procedure.

3.3.10. Regulation of Cryptographic Controls:

(a) Cryptographic controls when deployed shall adhere to the legal requirements as per applicable legislation in India and that of countries outside India, where the Organization maintains operations.

3.3.11. Security Policies and Procedures:

(a) The Organization shall ensure through a notice/circular and execute an undertaking from all the stake holders that they have read and understood the Information Security Policy of the Organization and that they shall abide by the same in spirit and matter and that any non-compliance against the same shall be tenable for an appropriate disciplinary action. The yearly goals of all employees shall include some percentage of their KRA to have a component of Information Security.

3.3.12. Technical Compliance Checking:

(a) The Organization shall conduct vulnerability and penetration testing of its critical Information Systems periodically with a periodicity of at least once every year.

3.3.13. Information Systems Audit Controls:

(a) Any audit which shall be done on the Information systems of the Organization shall not disrupt the business process. If any information systems audit tools are getting deployed, then they shall have restricted access to prevent any misuse. System logs/ administrator's logs/user logs shall not be deleted, as per the SOP (Standard Operating Procedure). Where ever logs are required to be maintained as per contractual/regulatory/statutory/legal requirement, then they shall be maintained for the specified duration. All audit records from internal/external audits shall be preserved as per the Organizations - Central Audit Policy and as mandated by the statutory and legal requirement. Data of effectiveness of controls shall be retained for the requisite number as required by business situation, statutory, contractual, regulatory requirements.

(b) Tools which are being currently used or those which shall be used for information system audits and the data generated through these tools shall be protected and kept separate from operational environment to prevent any possible misuse or compromise. There shall be separate machine on which the audit tools and the findings from this/these tools shall be stored in an encrypted format with role authorization for access clearly defined by the Compliance/Audit/Network Infrastructure Group.

3.3.14. Continual improvement:

(a) Whenever any non-conformity occurs, APAR shall review it for implementation of appropriate control/action and take corrective action to continually improve the suitability, adequacy and effectiveness of the information security management system.

4 Procedure

4.1. For protection of organizational Records, refer to Acceptable usage policy [ISMS-SM-06]

4.2. For Prevention of Misuse of Information Assets, refer to Acceptable Usage Policy [ISMS - SM -06].

4.3. Information security means the practices and procedures that help to protect information, generally held in electronic form from unauthorized access, modification or accidental change and help ensure availability of that information to authorized users on request. For safe business transactions, a secure legal environment is needed. Since the transaction and information on the internet are open to all, business could not be carried on through its medium unless businessmen are assured of the security.

4.4. The `Information Security Officer' of each location shall provide the CISO with a Positive Assurance Report covering aspects of legal compliance based on applicable legislations; refer to template of Positive Assurance Report.

4.5. The legal department shall provide the list of applicable legislations to all the `Information Security Officer' of respective location and CISO.

4.6. This activity shall be carried out once in 6 months or as required by the applicable legislation, for which the `Information Security Officer' of respective location shall be reminded in advance.

4.7. Technical compliance checking and Information System Audit Controls are provided as under.

4.8. As part of ensuring compliance the following activities shall be done every year and notified to the Information Security Apex Committee (ISAC) through the CISO of their satisfactory completion. They are mentioned as under:

a. Internal Audits by the organizations Audit cell or by the CISO or by employees trained in conducting Information Security Audit, minimum twice a year.
b. The methodology of performing the departmental information security audit shall be as per the audit plan. The checklists for the identified areas are also as per the audit plan. The audit checklists shall be prepared by the CISO and shall all the domains as mentioned in the Is027001:2013. The checklists shall be sent to the departments across APAR and the Is-DRs shall be responsible to complete the same within the assigned timeline and return the same to the `Information Security Officer'

c. With a specified date for the conducting of the audit after getting the necessary approvals and conformations from the HOD.
d. External Audit shall be carried out every year through an independent third party.
e. Submission of Positive Assurance statement on compliance aspects as listed in the Compliance Policy. Any objections or encumbrances of any nature shall be brought to the notice of the CISO. CISO shall provide directly or through the nominee a redressal of the problem which shall be final and binding upon the information security organization office bearer.
f. The ISO shall ask the CISO to submit every year, an organization wide audit calendar, activities planned and new initiative and a summary of the achievements of past year, lessons learnt, unfinished initiatives and corrective steps planned.
g. The Corrective Action pending from the audit cycle of last year shall be discussed with the Information Security Organization and shall be resolved accordingly. Pending issues shall be carried forward and a time frame to be defined as agreed upon by the auditee. These shall be concluded in the subsequent audit cycle.
h. A Health check Questionnaire and a spring cleaning Questionnaire shall be administered to all the branches and department, the data of which shall be collated and presented to the CIS0 who in turn shall inform the 'Information Security Officer'

4.9. The corrective action plan and preventive action plan shall be created in the format as mentioned below. This shall be prepared by the department ISMS implementer, reviewed by the HOD/ ls0 and approved by the HOD before being forwarded to the CISO.

4.10. If there is an Auditor/Auditee conflict then the same shall be resolved in the presence of the HOD and CISO as the case may be. If it does not get resolved then it shall be escalated to the APEX Committee whose decision in this regard shall be final and binding on the Auditee and the auditor.

4.11. If there is a conflict between the external auditor and the auditee, then the CISO shall make a representation on behalf of APAR to the Lead Auditor of the external auditing agency. Resolution of the conflict shall be based on the outcome of the appeal received and accepted by APAR.

4.12. At the time of conducting technical audit the following shall be adhered to:

a. A documented process and a plan shall be provided by the auditor to the Auditee clearly stating the duration/ nature and methodology which is going to be applied.
b. At no point in time shall any of the systems be compromised through exploitation of vulnerabilities.
c. During the time of VA/PT, there shall be person from Information Security Team/ Infrastructure Team under whose supervision the said activity shall be carried out.
d. The auditors shall ensure that they preserve the integrity of production data and shall not inadvertently delete or overwrite or modify this data and hence shall ask for `read only′ access.
e. Access to systems shall be provided through the prevailing access rights Mechanism with the necessary approvals.
f. All access by Auditors shall be logged and monitored as evidence.
g. Upon conclusion of the audit, all access rights shall be removed as per the documented procedure.

4.13. The template for reporting audit findings is given in Annexure 1.

4.14. The audit report shall be preserved for required number of years as required by business/ contractual and regulatory requirements.

4.15. The audit report shall be made available to the stakeholders on a need to know basis.

4.16. The systems audit shall be conducted by the `Information Security Officer′ under the CISO or any approved third party.

4.17. The audits shall be as per the annual audit plan which shall be communicated to the identified groups within the Organization by the CISO through the `Information Security Officer′ and the information security organization `Information Security Officer′.

4.18. The physical components of the information systems which shall be audited are:

a. Operating systems.
b. Applications.
c. Web Based Applications.
d. Servers.
e. Network Devices like routers and switches.

f. Interfaces.
g. Laptops and Desktops

4.19. The operational components of the information systems which shall be audited are:

a. Access Control Mechanism
b. Role Authorizations
c. Input data and Output Data Validation
d. Message Integrity
e. SLA Managements
f. Change Management process
g. System Patch and AV Updates
h. System Documentation
i. Software Development process
j. Backup process

4.20. Over and above the preceding two points, the information assets in hard format shall be audited for their entire lifecycle management comprising of creation, classification, storage modification, distribution and disposal.

4.21. The audit methodology shall be tool based or non-tool based; manual administration of an audit questionnaire shall be done in case of a non-tool based approach. However it shall be left to the auditor to combine the questionnaire along with the tool.

4.22. The tool's output shall be collected by the designated personnel from the Information Security Team. The output data shall be ported on the software available with the audit team.

4.23. Report shall be prepared based on the outputs obtained and compliances and non-compliances shall be flagged and communicated to the concerned technology group.

4.24. The output obtained through the running of the tool/scripts shall be stored on a dedicated server with restricted access provided to personnel as identified by the CISO.

4.26. A surprise audit shall be conducted by the audit team as per need.

4.27. Segregation of duties shall be maintained when audits are being conducted. The auditor shall not be allowed to audit his/her own department.

5 Enforcement

5.1. Any employee or third party found to have violated this policy and procedure shall be subjected to disciplinary action as per the Code of Conduct of APAR.

5.2. APAR Management interpretation of the clauses in this policy and procedure shall be final and binding on all the stakeholders. Management reserves the rights to alter or amend any clause in this procedure at any time as per its discretion.

6 Points of Audit

6.1. The audit check points for this procedure shall be as following:

a. Audit planning and execution process.

b. Creation and handling of audit records and evidences.

c. Storage and communication of audit findings and reports.

d. Resolution of auditor and auditee conflicts.

e. Points of audits as mentioned in each procedure of ISMS project shall form a part of this procedure.

7 Evidences

7.1. The evidences shall be maintained by the concerned departments / `Information Security Officer'.

7.2. The evidences to be maintained are as given under:

a. Audit Reports

b. Audit plan communication with receipt of acknowledgements from various business groups

c. Communication on auditor and auditee conflict along with resolution there off

d. Corrective and preventive Action plans as submitted by various groups

e. Audit checklists if they have been used

f. Evidences as listed under each procedure shall form a part of this procedure

g. The Annual audit plan as prepared by the CISO in conjunction with the `Information Security Officer'.

8 Metrics

8.1. The metrics shall be measured by the concerned departments/ Information security Team.

8.2. The periodicity of reporting shall be once in30days.

8.3. The metrics to be monitored are as given under:

a. Number of internal audits done per department internally.
b. Number of Non-conformances received during internal audit by various business groups.
c. Number of external audits done through an external agency.
d. Number of Non-conformances received in the audit done by the external agency.
e. Reduction in the number of non-conformances through the implementation of the corrective and preventive action plan.
f. Number of Non-conformances not closed from internal audit
g. Number of Non-conformances not closed from external audit.
h. Number of auditee and auditor conflicts in internal audit.
i. Number of repeat Non-conformances in external and internal audit.
j. Number of non-conformances for the points of audit and metrics as mentioned under each procedure.

9 Exceptions

9.1. Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the information owner. These may arise, for example, because of local circumstances, conditions or legal reason existing at any point of time.
9.2. Exceptions to the Information security policy and procedures may have to be allowed at the time of implementation of these policies and procedures or at the time of making any updates to this document or after implementation on an ad hoc basis based on business or a specific and a peculiar manifestation of circumstances which could be of temporary or permanent in nature.
9.3. All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through an Exception Form and sign-off on the same shall be maintained including ad-hoc requests.
9.4. The `Information Security Officer' shall review all exceptions, as the case may be, every year for validity and continuity.
9.5. APAR shall also list parameters to ensure that before acquiring new applications or other software and hardware, the set of applicable policies and guidelines shall be matched with the available security mechanisms of the product to ensure that the product has the necessary features. If not, then exceptions shall be approved before acquiring the desired product. Similarly, while developing new applications, the necessary security policies and guidelines have to be incorporated in the application or exceptions shall be obtained for the same from the 'Information Security Officer'.

10 Violations & Disciplinary Action:

10.1. Any employee or third party found to have violated this policy and procedure shall be subjected to disciplinary action as per the Code of Conduct of the APAR.

10.2. APAR Management interpretation of the clauses in this policy and procedure shall be final and binding on all the stakeholders. Management reserves the rights to alter or amend any clause in this procedure at any time as per its discretion.

11 Disclaimer

11.1. APAR reserves all rights and is the exclusive owner of all intellectual property rights over this information security policy and procedure document. This information security policy and procedure document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (such as floppy diskettes, hard disks, USB Drives, Pen Drives, Memory Cards, CDS, DVD's), and/or captured or transmitted through by any means (electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior written consent from the Information Security Team of APAR. The information security policy and procedure document is meant to be published on the intranet of APAR and/or any other forum as decided by the management of APAR. Anything not specifically stated in this information security policy and procedure document shall not be considered as implied in any manner.

11.2. For any clarifications related to this information security policy and procedure document with respect to its interpretation, applicability and implementation, please write to infosec@apar.com

12 Annexure 1

Information Security -Internal Audit -Report Format

Assessment report No :		Report Date:	
Location & Department		Audit Date:	
Lead Assessor		Assessors:	

Audit Scope: (Define the audit scope)

Audit Methodology: (Define the audit methodology)

Findings:

Internal Audit -Non Conformances			
Name Organization		Audit Date	
Location		Sector	
Department		DR	

Non Conformances from previous audits not closed

Sr No	NCs Major / Minor	Observation	ISO 27001:2013 Clause / Policy Ref.

Findings from current audit

Sr No	NCs Major / Minor	Observation	ISO 27001:2013 Clause / Policy Ref.
Auditor:			
Observation regarding verification of corrective action:			
Non-conformance closed: Yes / No			
Date:		Auditor:	

Conclusion:

Name:

Designation:

Qualifications:

Signature:

Date:

Place: