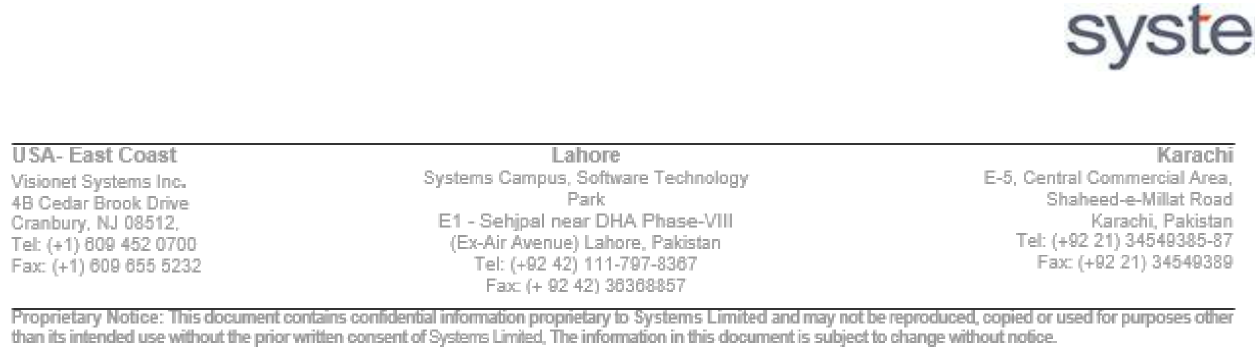
SYSTEMS LIMITED POLICIES DOCUMENT

SL-Pol-Doc

Version – 1.1



USA- East Coast
Visionet Systems Inc.
4B Cedar Brook Drive
Cranbury, NJ 08512,
Tel: (+1) 609 452 0700
Fax: (+1) 609 655 5232

Lahore
Systems Campus, Software Technology
Park
E1 - Sehjpal near DHA Phase-VIII
(Ex-Air Avenue) Lahore, Pakistan
Tel: (+92 42) 111-797-8367
Fax: (+ 92 42) 36368857

Karachi
E-5, Central Commercial Area,
Shaheed-e-Millat Road
Karachi, Pakistan
Tel: (+92 21) 34549385-87
Fax: (+92 21) 34549389

Proprietary Notice: This document contains confidential information proprietary to Systems Limited and may not be reproduced, copied or used for purposes other than its intended use without the prior written consent of Systems Limited, The information in this document is subject to change without notice.

Document Overview

Title	**Systems Limited Policy Document**	Version	**1.1**
Project	**ISMS , SMS , QMS Policies & Procedures**	Status	**Approved**
Client	**Systems Limited**	Type	**Internal**
Doc #	**Sys-Pol-Doc**	Doc Date	**22-May-2018**
Author	**Information Security**	Last Save	**28-July-2020**
Document Classification	**Public**		
Description			

Revision History

Ver #	**Rev Date**	**Author**	**Reviewed By**	**Brief Description**
1.0	May 22, 2018	Syed Anwer Gillani	AVP / CISO	Approved
1.1	28-July-2020	Syed Anwer Gillani	Tauqeer Ahmed	Annual Review

Distribution List

Public

Approved By

Name	**Role**	**Version**
Tauqeer Ahmed	AVP Infosec	1.0 – draft
Tauqeer Ahmed	AVP Infosec	1.1 – Approved
Tauqeer Ahmed	AVP Infosec	1.1 – Approved

1. VISION STATEMENT

Systems Limited as an Institution is committed to being the Leader of IT & ITES in the Region through our Thought Leadership, Sustained Service Delivery Excellence, Strong Customer Focused Employees, Strong relationship with our Customers, Partners, and Vendors. To that end we must continuously innovate, enhance our service offerings, achieve superior financial results and increase value to our clients and trusted shareholders. These unwavering expectations provide the foundation of our commitment to those whom we interact

2. MISSION STATEMENT

Systems Limited is dedicated to provide the Highest Quality Business Solutions, IT & IT Enabled Services and People to our clients and business partners that earns their respect and loyalty, we aim to be the number one service provider through our battle tested methodologies, processes, frameworks and customer focused resources in the niche Industry and Technology/Business Sector we operate.

Please note:

Policies should be read out in the session with actual Policy documents, in order to get the complete over view of management directions and context of Organization

3. ITSM POLICY STATEMENT:

It is the policy of Systems Limited to implement an IT Service Management framework within the scope of its geographically distributed BPO & IT departments providing information processing services to various sectors.

1. The provision of services shall be aligned to customer and user needs.
   a) Services shall be delivered to a defined quality, sufficient to satisfy requirements identified from business processes.
   b) A clear service portfolio shall be developed and maintained as a basis for all service delivery and service management activities.
   c) For all services, a corporate level SLA and / or specific SLAs, which have been agreed with relevant stakeholders, shall be in place.
2. To effectively manage services and underlying components, a process-based approach to service management shall be adopted.
   a) All required processes shall be defined, communicated and improved based on business needs and feedback from people and parties involved.
   b) All roles and responsibilities for managing services (including roles as part of service management processes) shall be clearly defined.

3. Service management processes shall be continually improved.
   a) Feedback from business stakeholders shall be used to continually improve services quality. All proposals for improvements shall be recorded and evaluated.

   b) Service management shall be improved based on continual monitoring of process performance and effectiveness.
4. Through trainings and awareness measures, it shall be ensured that staff involved in service management activities can perform effectively according to their assigned roles.

5. Top management is committed to this policy and its implementation. It provides the resources required to implement and improve service management and enhance customer satisfaction with services.
6. Top management and services management implementation team shall ensure that all applicable legal requirements shall be abide by the organization.

Ref Doc: Policy Definition IT Service Management_2019

4. INFORMATION SECURITY POLICY STATEMENT:

The purpose of the information security policy is to provide direction and support for all information security activities in accordance with business requirements and relevant laws and regulations.

Systems Limited aims that:

1. A management structure shall be established to initiate and control the implementation of information security, data privacy and protection from malware and intrusion.
2. Annually or need basis management review shall conduct for improvement and based on evolving threats.
3. Access to the Company's information and associated processing facilities shall be controlled.
4. Information shall be classified to indicate the need, priority, Privacy and degree of protection required.
5. All requirements related to Human Resource security shall be fulfilled at the recruitment stage, and, thereafter, all information security responsibilities as defined in the Company's information security policies and procedures shall be monitored during an individual's employment.
6. All staff shall be trained in security procedures and the correct use of information systems facilities. Shall be given security awareness session at the time of joining and each employee / 3rd party have to sign NDA to ensure privacy, integrity and confidentiality of SL and Clients data and information.
7. All SL employees 3rd parties are trained and advised to ensure the integrity and confidentiality of client data.
8. Incidents affecting security shall be reported promptly through the defined management structure.
9. Business information and information processing facilities shall be protected from security threats and environmental hazards in a manner commensurate with the associated risks. Quarterly or as per requirement / business need scans / VAPT should be conducted and fix the issues. Privacy of business information and information processing facilities supporting critical or sensitive business activities shall be housed in secure areas with appropriate entry controls.
10. Responsibilities and procedures shall be established for the management and operation of all information processing facilities.
11. Projections of future capacity shall be made and operational requirements of new systems shall be established, documented and tested prior to their acceptance and use.
12. Controls shall be established to prevent and detect viruses and other malicious software.
13. Routine procedures shall be established for taking back-up copies of information and system software, logging events and faults (e.g. all type of server logs, etc) and, where appropriate, monitoring the equipment installed for this purpose (e.g. camera recording and its audit logs, etc.).
14. Information within networks and passing over public networks shall be secured and protected from unauthorized access.
15. Procedures shall be established for the proper handling, storage and disposal of documents and computer media.
16. Controls shall be established to protect exchanges of information and software with other organizations including information transfer through FTP or CD's.
17. Security shall be applied on operating system to restrict unauthorized access to computer resources.
18. All security control systems shall be monitored to detect deviation from access control policy.
19. All information systems and related facilities shall be regularly monitored to identify the deviations, violations and inconsistencies with defined information security policies and

procedures.

20. Controls shall be established to mitigate the additional security risks associated with mobile computing and wireless networks.
21. Security requirements shall be identified and agreed prior to the processing of information system activities.
22. Business continuity plans shall be established to protect critical business processes from the effects of major failure or disasters.
23. All legal, regulatory, contractual requirements shall be identified and adhered by management.
24. Information systems shall be audited for compliance.
25. Effectiveness of implemented security controls shall be measured and shared with the interested parties.
26. SL user can only authorised send and receive email within the organization. In case user required to send mails to external domain, he has to create a ticket with business justification and after approval access can be granted.

Ref Doc: Policy Definition Information Security_v2.2 / 2020

5. QUALITY MANAGEMENT POLICY STATEMENT:

Our Top management has created following quality policy

1. At Systems Limited our goals are to meet or exceed our customers’ needs through timely delivery of high quality software and services and to increase productivity and profitability.
2. To achieve these goals we have adopted Quality Management approaches that include well-defined management and software development processes and mechanisms for continuous improvement of our products and services.
3. We focus also on the professional growth of our human resource and on our work environment. This helps us to attract and retain the best professionals and keep the company abreast of innovations in technology.

Ref Doc: QMS - Quality Manual-Latest_2019 v1.7

5.1 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.