VISAKA INDUSTRIES LIMITED

Information Technology – Acceptable Use Policy

Version 0.2, Date: 01-11-2019

Document Information:

Version: 0.2
Last Updated: 1st November 2019
Documented Information Owner: Visaka Industries Limited
Approval Authority: Visaka Industries Limited

Document Information

Document Title: Information Technology – Acceptable Use Policy

Abstract: This is Visaka Industries Limited's (VIL) Information Technology Policy. The policy has been issued with the approval of management of Visaka Industries Limited and compliance with its principles which are applicable for all Internal, External, and authorized Third-Party users accessing any computing facilities owned or operated by VIL.

Document Version History:

Type of Information	Details
Document Version	0.2
Date of Release	1st November 2019
Last Revision Date	1st November 2019
Document Owner	IT Department
Document Author(s)	
Document Change Reviewer	Niranjan Bakre
Verified by	Sankaran Vangili, Rajasekhar Kommineni
Document Classification	Internal Use
Document Status	Final

Type of Information	Details
Document Version	0.1
Date of Release	1st January 2018
Last Revision Date	1st January 2018
Document Owner	IT Department
Document Author(s)	
Document Change Reviewer	Krishna Moorthi
Verified by	Sankaran Vangili
Document Classification	Internal Use
Document Status	Final

Approver List:

S. No.	Version No.	Approver	E-mail ID	Date Approved	Signature
1.	0.1	Krishna Moorthi	krishnamoorthi@visaka.in	1st Jan 2018	
2	0.2	Niranjan Bakre	niranjan.bakre@visaka.in	1st Nov 2019	N Bakre

Document Change History:

S. No.	Version No.	Revision Date	Nature & Details of change	Affected Section
1.	0.1	1st Jan 2018	Initial version	
2.	0.2	1st Nov 2019	Modifications in Initial version	All
	1.0		Approved	

Visaka Industries Ltd. (hereinafter referred to as "VIL") is committed to have an Information Technology Policy to make the Information systems more secure, reliable, and efficient for the organization as a whole. The IT policy is applicable all the Manufacturing units, Associated units, and Corporate Office at Hyderabad.

The objective is to create an awareness and better understanding of the IT infrastructure and Information Security Policy among the all users in VIL.

It applies to all users of IT including employees, contractors, consultants, and temporary workers / staff of VIL. All are expected to be familiar with the IT policy and comply with it.

Effective Date

1st November 2019

Vamsi Krishna G

Joint Managing Director

2. IT Acceptable Use Policy

2.1. Overview

VIL is committed to protecting employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet / Intranet / Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and FTP, are the property of VIL. These systems are to be used for business purposes in serving the interests of the company, and of our customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

2.2. Purpose

The purpose of this policy is to outline the acceptable use of information systems at VIL. Inappropriate use exposes the company to risks including virus attacks, compromise of network systems and services, and legal issues.

The acceptable use policy establishes a set of standards to govern the employee and user behavior with respect to VIL information systems and resources. Non-adherence to the policy also carries a disciplinary action associated with it.

2.3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by VIL, the employee, or a third party.

All employees, contractors, consultants, temporary and other workers / staff at VIL are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with VIL policies and standards, and local laws and regulation.

2.4. Policy Details

All employees of VIL shall abide by the guidelines mentioned below to comply with VIL Information Technology Policy.

2.4.1. Physical and Environmental Security

Acceptable Usage:

(i) VIL's Identity Card shall be displayed all times within company's premises.
(ii) Users should ensure that visitors are always escorted while visiting the sensitive areas such as data centers, storage areas where confidential documents are maintained, etc.
(iii) Users (internal employees, contract employees, third-parties) shall participate in safety drills organized by the company.

Unacceptable Usage:

(iv) Users shall not lend or borrow Access Cards.
(v) Users shall not tailgate or allow tailgating in secured areas like server rooms, etc.
(vi) Users shall follow safety instructions.

2.4.2. Desktop and Laptop Usage

Acceptable Usage:

(i) Desktops / laptops or any other IT resources provided to employees shall be used only for official purpose
(ii) Users shall only use approved software on the Desktops or Laptops.
(iii) Users shall always keep their desktop or laptop suitably fastened or locked when they are not at their desk.
(iv) Laptops shall always be carried with adequate precautions during travel.
(v) In the event of a laptop being stolen, the concerned personnel shall file a police report and subsequently inform the IT department immediately.
(vi) Users shall declare personal computing equipment (like CDs, pen drives, laptops etc.) to the security guard before carrying them inside the company's premises
(vii) Classified data shall not be copied to external portable media like USB's, CDs, etc. without the permission of HOD and Head-IT.

Unacceptable Usage:

(viii) Users shall not connect their personal laptops or mobile devices to the VIL's Network
(ix) Users shall not install freeware or shareware which are not provided by VIL
(x) Users shall not use external devices unless it is approved by the HOD and Head-IT.

2.4.3. User Access Control

Acceptable Usage:

(i) All Employees including contract and third-party users shall use their user ID assigned to them for accessing VIL's information assets.
(ii) All users shall adhere to the password policies of VIL.

Unacceptable Usage:

(iii) Users shall not use shared accounts for accessing VIL's information assets.
(iv) Users shall not share their passwords with anyone.
(v) Users shall not write or paste passwords in public spaces or at the workplace.

2.4.4. E-mail Account Usage

Acceptable Usage:

(i) Users shall use only VIL's e-mail for official purposes
(ii) Users shall exercise caution in disclosing VIL's e-mail address to strangers
(iii) Users shall report suspicious e-mails to the Head-IT.
(iv) Users shall archive mails and take regular backups.
(v) Users shall follow the controls specified by VIL while accessing emails from mobiles.
(vi) Users shall report about spam to the IT team.

Unacceptable Usage:

(vii) Users shall not use e-mails within the organization to abuse or harass other employees
(viii) Users shall not open attachments from suspicious or unknown e-mail addresses.
(ix) Users shall not send unwanted e-mails to the outside world that project a wrong image of VIL.
(x) Users shall not communicate with any third party which may potentially invite involvement of law enforcement agencies
(xi) Users shall not participate in chain e-mails

(xii) Users shall not forward sensitive e-mails containing VIL's information to the external world.
(xiii) Users shall not register VIL e-mail addresses on external websites.
(xiv) Users shall not use personal e-mail accounts such as Gmail etc. for official communications.

2.4.5. Internet Access Usage

Acceptable Usage:

(i) Users shall use Internet access for business-related activities only, i.e., to communicate with customers and suppliers, to research relevant topics and obtain useful business information.
(ii) Users shall exercise caution while accessing external websites with official internet connections provided by VIL
(iii) Internet / Email traffic logs may be maintained by the company without prior notice. This information can be used by the company to take disciplinary action against employees who have misused VIL internet services, which may result in termination of services.
(iv) Users with Internet access are expected to conduct themselves honestly and appropriately on the Internet, and respect the copyrights, software licensing policies, intellectual property rights, and privacy.
(v) Access to social networking sites (such as Facebook etc.) and Audio / Video streaming sites shall be restricted, in order to safeguard the internal network from potential malicious content.

Unacceptable Usage:

(vi) Users shall not send/receive/view racial, sexually threatening, defamatory or harassing messages.
(vii) Users shall not upload and download large files not related to business.
(viii) Users shall not introduce computer viruses, worms, or Trojan horses, etc.
(ix) Usage of any kind of Internet chat services like Google messenger, Yahoo chat, etc., and social networking sites like Face book, Twitter etc. is restricted.
(x) Users shall be strictly prohibited from using any tools or any other means for gaining unauthorized access to any third-party systems or VIL systems or any resource over the Internet to which they do not have authorized access rights.
(xi) Users are further prohibited from engaging in any activity that may result in disruption in operations of either VIL or any third-party computer systems.

2.4.6. Mobile Usage

Acceptable Usage:

(i) Users requiring information access on handheld devices shall obtain necessary authorization prior to use.
(ii) Users shall report to IT helpdesk and change their AD password immediately on the loss of devices.
(iii) Users shall store confidential business information in encrypted form.
(iv) Users shall keep the unused connectivity options such as Bluetooth, Wireless LAN in switched off mode and enable on need basis. Access to corporate wireless network should be done only after authorization
(v) In case of loss or misplacement of the Device, change or disposal of the device, separation from VIL for any reason, Employees (including Contract and Third-Party employees) will be solely responsible, or authorize VIL, to immediately wipe the entire data contents (personal and official) off the device.
(vi) Users shall install applications on smart phones, tablets only from trusted and authorized source.
(vii) Users shall install a trusted anti-virus and update them regularly.
(viii) User is solely responsible for protection of all forms of VIL information including customer's Information that may be contained in the device.

Unacceptable Usage:

(ix) Users shall not send business confidential information through short message service (SMS) or equivalent.
(x) Users shall not use jail broken, rooted devices.
(xi) Users shall not use camera, or any other device embedded with camera, for taking photographs / shooting video clippings inside any of the identified sensitive areas.
(xii) Users shall not use camera, through remote access mechanisms, for taking photographs/shooting video clippings of information available
(xiii) Jail broken, rooted devices shall not be connected to the VIL network.

2.4.7. Data Privacy and Protection

Acceptable Usage:

(i) Users shall classify information assets according to their level of sensitivity and handle the same accordingly.
(ii) Users shall protect vital physical records which contain business related information.
(iii) Users shall understand business/contractual requirements of data protection from their respective HOD

Unacceptable Usage:

(iv) Users shall not send any internal business data related to the department to any third party without approval of their respective HOD.
(v) Users shall not use camera mobile phones in secured areas like server rooms, datacenters, etc.
(vi) Users shall not leave confidential documented information on the desk; instead it should be kept in a locked cabinet.
(vii) Users shall not leave printouts unattended at the printer machine.
(viii) Users shall not reveal information about VIL's business details in white papers or presentations.
(ix) Users shall not discuss official matters in public places unless otherwise authorized to do so.
(x) Users shall ensure that no material which is obscene is published or transmitted.

2.4.8. Reporting Security Breaches, Incidents, or Events

(i) Users including contract and third-party employees shall communicate any observed or suspected information security incidents and/or weaknesses to the IT team or Head-IT.
(ii) Users shall be informed that they should not, in any circumstances, attempt to prove a suspected weakness. Any action in testing the weakness shall be interpreted as a potential misuse of the system
(iii) Users shall not discuss with colleagues about the suspected weakness once it is reported to higher authority for investigation

2.4.9. Exceptions

Any exception to the policy must be approved by the Head-IT in advance.

2.4.10. Disciplinary actions

(i) Violation of the above directives may lead to legal and/or disciplinary action up to and including termination of employment. The actions may include Suspension, Remarks in personal file, Dismissal, Criminal and or Civil action.
(ii) Any act of disciplinary actions shall precede with an investigation by the HR, concerned HOD and IT, based on which the course of the action shall be decided.

Glossary

Below is the listing of abbreviations and acronyms used in the above document.

S. No	Abbreviation / Acronym	Explanation
1.	ERP	Enterprise Resource Planning
2.	IT	Information Technology
3.	AD	Active Directory
4.	E-mail	Electronic mail
5.	TCL	Tata Communications Limited
6.	EAM	Enterprise Asset Management
7.	DC	Domain Controller
8.	Oracle EBS	Oracle's E-Business Suite
9.	CC TV	Closed Circuit Camera
10.	PLC	Programmable Logic Controller
11.	MS Office	Microsoft Office
12.	SQL	Structured Query Language
13.	HR	Human Resource
14.	HOD	Head of Department
15.	EDP	Electronic Data Processing
16.	SLA	Service Level Agreement
17.	SCCM	System Center Configuration Manager
18.	SAN	Storage Area Network
19.	DBA	Database Administrator
20.	NDA	Non-Disclosure Agreement
21.	NOC	Network Operations Center
22.	CD	Compact Disk
23.	IP	Internet Protocol
24.	DNS	Domain Name System
25.	VPN	Virtual Private Network
26.	ftp	File transfer protocol
27.	http	Hypertext transfer protocol
28.	OS	Operating System
29.	HDD	Hard Drive Disk
30.	RAM	Random Access Memory
31.	NAS	Network-attached Storage