Zetta One Technologies India Pvt. Ltd.,

Success Towards Technologies...

ZettaOne IT Security Policy

Document ID **Zetta/IT-2018-01**	Title ZettaOne IT Security Policy	Print Date 21 May 2018
Revision 0.0	Prepared By Stanlin Raj D	Date Prepared 18 May 2018
Effective Date 23 May 2018	Reviewed By Suresh Kumar M	Date Reviewed 21 May 2018
	Approved By Suresh Kumar M	Date Approved 21 May 2018

ZettaOne IT

Contents

1. IT Security Policy

- This section sets forth some important rules relating to the use of ZettaOne's computer and communications systems. These systems include individual PC/Lap provided to employees, centralized computer equipment, all associated software and ZettaOne's telephone, voice mail and electronic mail systems. ZettaOne has provided these systems to support its mission. No use of these systems should ever conflict with the primary purpose for which they have been provided, ZettaOne's ethical responsibilities or with applicable laws and regulations. Each user is personally responsible to ensure that these guidelines are followed. All data in ZettaOne's computer and communication systems Including documents, other electronic files, e-mail and recorded voice mail messages) are the property of ZettaOne IT/Supervisor may inspect and monitor such data at any time. No individual should have any expectation of privacy for messages or other data recorded in ZettaOne's systems. This includes documents or messages marked "private," which may be inaccessible to most users but remain available to ZettaOne. Likewise, the deletion of a document or message may not prevent access to the item or eliminate the item from the system.

- ZettaOne's systems must not be used to create or transmit material that is derogatory, defamatory, obscene or offensive, such as slurs, epithets or anything that might be construed as harassment or disparagement based on race, color, national origin, sex, sexual orientation, age, physical or mental disability, medical condition, marital status, or religious or political beliefs. Similarly, ZettaOne's systems must not be used to solicit or proselytize others for commercial purposes, causes, outside of organizations, chain messages or other non-job-related purposes.

- Security procedures in the form of unique user sign-on identification and passwords have been provided to control access to ZettaOne's host computer system, networks and voice mail system. In addition, security facilities have been provided to restrict access to certain documents and files for safeguarding information.

1.1. ACCEPTABLE USE - COMPUTERS AND INTERNET

- Access to the Internet is provided for all users and limited to their activities in direct support of official Company business.

- In addition to access in support of specific work-related duties, the Company Internet connection may be used for educational and research purposes.

- If any user has a question of what constitutes acceptable use he/she should check with their IT Team for additional guidance. Management or supervisory personnel shall consult with the Information Services Manager for clarification of these guidelines.

1.1.1. ACCEPTABLE USER POLICY-COMPUTERS & SOFTWARE

- Do not copy or modify the software installed in your office computers without permission from IT Team. Copying or adaptation of software programs may result in violation of the license conditions and infringement in copyright.

- Do not install in your office computer (whether for office or personal use) any software licensed or unauthorized, for your personal use.

- Do not bring software to the office (even genuine copies) for carrying out your official duty.

- Do not copy for your personal use any software installed in your office computer.

- Do not download any software (including “freeware”, “shareware”, “wall paper”, “sound files” or “screen savers”) from the Internet and install it in your office computer without permission from your IT Team (whether for office or private use).

- Do not bring your own computer to office to carry out office work without Prior permission from your IT Team.

- Attempts should not be made to bypass, or render ineffective, security facilities provided by the company.

- Passwords should not be shared between users. If written down, passwords should be kept in locked drawers or other places not easily accessible.

- Individual users should never make changes or modifications to the hardware configuration of computer equipment. Requests for such changes should be directed to IT Support.

- Additions to or modifications of the standard software configuration provided on ZettaOne's PCs should never be attempted by individual users (e.g. Auto exec.bat and config.sys files). Requests for such changes should be directed to IT Team.

- Computer games should not be loaded on ZettaOne's PCs.

- Individual users should not change the location or installation of computer equipment in offices and work areas. Requests for such changes should be directed to IT support.

1.1.2. COMPUTER ELECTRONIC MEDIA

- USB ports should not be used to insert any external devices viz. USB drives, Mobiles, Data cards, DVD writers, etc.

- No electronic devices, personal laptops, I-pads, USB drives are allowed inside the Office premises without prior permission from IT.

- If anyone need USB access they should take the proper mail approval from Respective department head and IT with reason for access, duration of access.

- On mobile access provided from ZettaOne for Mails, OneNote & Skype access granted to all users from ZettaOne IT. It's strictly for official purpose.

1.1.3. MAKING COPIES OF COPY RIGHT WORKS

- You are not allowed to make copies of copyright works (including books, magazines, newspapers, periodicals or other publications) for use in the course of business of the company/organization unless appropriate licenses have been obtained from the copyright owners. Examples include making copies of newspaper articles regularly for distribution to members of the staff, making copies of certain chapters of a book as reference materials for your project. Moreover, you are not allowed to bring infringing copies of any works to the office for carrying out your official duties. Where a license has been obtained, you should comply strictly with the terms of license.

➢ Please note the making of copies in the following areas:

1.1.3.a. Electronic copies

- Copying does not only mean the making of photocopies. It includes scanning, storing information in hard disc or other electronic or optical media (e.g. optical discs, memory cards, memory sticks). Transmission of materials by fax is also considered as copying. Authorization is required for the above from respective manager/IT

1.1.3.b. Internet information

- You are permitted to send URL addresses of Internet resources to others (e.g. by quoting them in letters, memos, or e-mails). You should, however, note that copyright works on the Internet are equally entitled to copyright protection. Printing out such materials without permission of the copyright owner will infringe copyright. Storing such materials in your hard disc whether permanently or temporarily, other than automatic web-browser caching, (e.g. downloading materials from websites for inclusion in your PowerPoint presentations) are acts that infringe the rights of the copyright owner. Before you do these acts, prior permission from the webmaster of the site concerned is required.

1.1.3.c. AUDIO –VISUAL WORKS

- Do not make recordings of audio-visual works (including movies, television dramas, musical sound recordings, musical visual recordings, broadcast or cable programs) on the premises of the company/organization, whether for use in carrying out your official duties or just for private use, without authorization from the copyright owners.

- Do not download any audio-visual works from the Internet onto the company/organization's computers, whether for use in carrying out your official duties or just for private use, without authorization from the copyright owners. An example of acts that are not allowed would be the downloading of music clips from the Internet for inclusion in your PowerPoint presentation to your clients.

- Do not possess parallel imported audio-visual recordings in business if such recordings are intended to be played or shown in public in the course of business, e.g. the playing of parallel imported music CD's in the workplace of the company/ organization or business premises where the public have access e.g. shops, restaurants.

- Do not play or show audio-visual recordings, broadcast or cable programs in public in the course of business without authorization from the copyright owners.

1.2. ACCEPTABLE USE POLICY- INTERNET

- At this time, desktop access to the Internet is provided to employees when there is a necessity and the access has been specifically approved. ZettaOne has provided access to the Internet for authorized users to support its mission. No use of the Internet should conflict with the primary purpose of ZettaOne, its ethical responsibilities or with applicable laws and regulations. Each user is personally responsible to ensure that these guidelines are followed. Serious repercussions, including termination, may result if the guidelines are not followed.

- ZettaOne may monitor usage of the Internet by employees, including reviewing a list of sites accessed by an individual. No individual should have any expectation of privacy in terms of his or her usage of the Internet. In addition, ZettaOne may restrict access to certain sites that it deems are not necessary for business purposes.

- If any unofficial/public site/social media/sexual sites/illegal data transfer/personal works/download unofficial files or applications are identified from IT, IT team should be update the same to Management. Management will take strict action against the users of maximum termination.

➢ ZettaOne's connection to the Internet may not be used for any of the following activities:

- Internet access shall not be for any illegal or unlawful purpose. Examples of this are the transmission of violent, threatening, defrauding, pornographic, obscene, or otherwise illegal or unlawful materials.

- Use of Company e-mail or other messaging services shall be used for the conduct of Company business only. These services shall not be used to harass, intimidate or otherwise annoy another person.

- The Internet shall not be accessed for private, recreational, or any non-company-related activity.

- The Company's intranet or Internet connections shall not be used for commercial or political purposes.

- Employees shall not use Company network for personal gain such as selling access of a Company user login ID. Internet access through the Company network shall not be for or by performing unauthorized work for profit.

- Users shall not attempt to circumvent or subvert security measures on either the Company's network resources or any other system connected to or accessible through the Internet.

- The Internet must not be used to access, create, transmit, print or download material that is derogatory, defamatory, obscene, or offensive, such as slurs, epithets, or anything that may be construed as harassment or disparagement based on race, color, national origin, sex, sexual orientation, age, disability, medical condition, marital status, or religious or political beliefs.

- The Internet must not be used to access, send, receive or solicit sexually-oriented messages or images.

- Downloading or disseminating of copyrighted material that is available on the Internet is an infringement of copyright law. Permission to copy the material must be obtained from the publisher. For assistance with copyrighted material, contact IT Support.

- Without prior approval of the Management, software should not be downloaded from the Internet as the download could introduce a computer virus onto ZettaOne's computer equipment. In addition, copyright laws may cover the software, so the downloading could be an infringement of copyright law.

- Employees should guard against the disclosure of confidential information using Internet e-mail or news groups.

- The Internet should not be used to solicit or proselytize others for commercial purposes, causes, outside organizations, chain messages or other non-job-related purposes.

1.3. INTERNET AND E-MAIL ETIQUETTE

- Company employees shall ensure all communication through Company e-mail or messaging services is conducted in a professional manner. The use of suggestive, vulgar, or obscene language is prohibited.

- Company users shall not reveal private or personal information through e-mail or messaging services without clear and specific written approval from respective department head.

- Users should ensure that e-mail messages are sent to only those users with a specific need to know. The transmission of e-mail to large groups, use of e-mail distribution lists, or sending messages with large file attachments (attachments larger than 2 Mb) should be avoided.

- E-mail privacy cannot be guaranteed. For security reasons, messages transmitted through the Company e-mail system or network infrastructure are the property of the Company and are, therefore, subject to inspection.

1.4. COMPUTER AND INTERNET USAGE – SECURITY

- Company users who identify or perceive an actual or suspected security problem shall immediately contact the IT Person.

- Network users shall not reveal their account passwords to others or allow any other person, employee or not, to use their accounts. Similarly, users shall not use other employees' accounts.

- All use of IT assets is subject to monitoring by IT Security.

- Access to Company network resources shall be revoked for any user identified

- as a security risk or who has a demonstrated history of security problems.

- ZettaOne will not allow to carry inside of ZettaOne Premises that the user's personal laptops, CD/DVD, USB, Memory Cards, Card Readers and any of other IT Accessories.

- Visitors should inform and make proper entry to Main security gate to carry their IT Assets inside of ZettaOne Premises.

- ZettaOne will not allow visitors to carry their IT Assets/Accessories to inside of ZettaOne Office area without proper approvals taken from the respective department head and IT from the respective visitor's department. If IT identified anyone carry IT assets / Accessories without proper permissions, management will send them out with immediate effect and management will take data / policy violation action against the visitor and the respective department heads.

- ZettaOne will allow the users to carry their IT assets with appropriate permissions and ZettaOne will give only Wi-Fi access to visitors for using internet. From this Wi-Fi access no one can access ZettaOne internal network.

- USB and external drive access strictly restricted for visitors. If they need USB/external drive access request IT support to do the activity. IT support will scan the drives and IT support will copy/paste the required data. IT support will do this activity based on respective departments head requisition with management approval.

- Visitors access requests should be send to IT, thirty minutes prior by mail from the respective HOD.

1.5. PASSWORD POLICY:

- Passwords must be at least 8 characters long.

- Passwords must be a mix of Alpha-Numeric characters

- At least one character must be in CAPS, which can be skipped.

- Use of special characters such as '**! @ # $ % ^ & ***' would make your password complex for attempts of attack.

- Passwords should not be particularly identifiable with the user (e.g. first name, last name, date of birth, pet's name etc.)

- Passwords should be changed at least once in 90 days (email) and 90 days (System), without which network services are not available

- The password history is maintained for 60 iterations for systems and 45 iterations for email.

- Minimum of 5 criteria mentioned above must be followed for the policy to be in process and last two steps are in process to be followed without fail.

2. IT **Ethics**

➢ **"Note: Deviations from the following will attract severe actions against the user:"**

2.1. Individual System Security

2.1.a. User Will Not:

- Reveal the configuration of the PC and Network (including any IP Addresses), to any other user or outsider.

- Change the basic configuration or install any hardware / software which would alter the basic configuration of the Network, E-mail and Internet Browsing.

- Install any software / hardware which would in any manner enable you to gain access to unauthorized Internet Browsing

- Allow any testing for Network related issues through your node without prior permission from the I.T. Department

- Scan the Network using any "Network Sniffing" software / hardware, or permit any outsider to install similar software / hardware

- Attempt to gain access to any other computer on the Network (with or without using specialized software / hardware for this purpose), without proper authorization

- Install any illegal / unlicensed software on the PC / Laptop.

- Stop automated / scheduled scans.

- Permit others to access their systems, unless specifically authorized to do so

- Permit Outsiders / Visitors to access systems/ network (this excludes authorized PC technicians)

- Install any USB devices or CD / DVD Writers or any other hardware which would permit them to copy data from the PC, unless proper authorization from the Head of the organization has been received.

- Install or use devices other than those provided / supplied by the Company on the PC / Laptop

- Users / Visitors Carry out IT assets without respected mail approval from IT & Management.

- Users / Visitors Carry in or out IT assets without mail approval from IT & respected HOD.

2.1.b. User Will:

- Ensure that the system is Password protected with a Boot-up
- password (and maintain passwords as per suggested policy by the IT Department).

- Ensure that the system is Password protected with Windows Login Password.

- Ensure that the system is protected with a Screen-Saver Password.

- Ensure that Guest Login is disabled on their PCs / Laptops.

- Ensure that Files / Directories on their systems are NOT shareable. However, if it is necessary to make a Directory or File Shareable, then it is the responsibility of the user to ensure that it is Password protected.

- Ensure that their PC / Laptop is installed with the latest version of Anti-Virus and that latest patches provided by the Anti-Virus vendor are applied.

- Ensure that latest patches for MS Windows and MS Office are applied on their PC / Laptop.

- Deploy automatic patch management solution to ensure timely and automatic patch delivery

2.2. Network Security

2.2.a. User Will Not:

- Browse unauthorized/ fire-walled internet websites in office hours.
- Attempt to gain unauthorized access to the websites banned for browsing in office.
- Use any other wireless network connectivity other than the office wired/ wireless network to access office emails within office unless and otherwise permitted by I.T. Department
- Browse personal/ networking sites while accessing office contents/emails on the PC/ Desktop
- Use any USB/ Pen/ Thumb Drives in office. (exceptions may be permitted with the valid concurrence of the Head of Organization to use official devices only)
- Use any other wireless connectivity services not allotted by this office for accessing office contents.
- Use the Network for illegal activities, including using it against the company you belong to, and the ZettaOne in general.
- Tamper with computer software and hardware, willful vandalism and destruction of computer files shall be liable for disciplinary action
- Deliberately attempt to disrupt the performance of the Network or any other computer system / network.
- Intentionally distribute Internet Viruses, Worms, Trojan Horses and other software destructive material.

- Will not import files on systems from unknown sources.

- Permit laptops belonging to outsiders to connect to the Office Network under any circumstances

- Print unofficial documents using office printer.

- Keep the official documents in open place and above table.

- Carrying official printed documents without respected permissions from respective dept.

- Laying printed documents in printer tray and above the table as well as apart from respected user locker is not acceptable.

- Using office mails and files in unofficial devices that is non-allocated from ZettaOne.

2.2.b. User Will

- Scan thoroughly each file before downloading into the system and perform a thorough scan every time while transferring office contents to/ from authorized external storage devices.

- Utilize network shared folders to transfer files and documents internally.

- Use the office system only for official use and correspondences only.

- Use authorized wireless connectivity on Laptop to access office emails.

- "Log Off" prior to leaving browsing terminals if office emails are being accessed from any public computer/ cybercafe.

- Print documents using office printer for official documents.

3. Right to Inspect

- IT department has been right to inspect any office machine at its discretion. This authority has been granted by Management

4. Physical Security

- Prior permission of IT department will be sought before allowing external machines and devices.

- The Management has authorized the administration to physically check the machine and devices (including removable storage media) of personnel to this office.

- In case any external machine or device is required to be brought into office premises, the administration is required to inform the IT department for necessary sanitization and permission. One machine will be allocated for this duty and will be placed under the IT department.

5. Identification **AND** TRACEABILITY:

- Asset number is allotted, printed and pasted to all the IT assets.
- The Asset register format is given below.

Sl. No	User Name	Location /Dept	Category	System Name/ IP	Device Tag	Sr. No	Specification	Model	Brand	Accessories	Device Tag	Serial No	OS & License	Software	Issued On	Recovered On	Remarks
1	Stanlin	IT Desk	Laptop	ZLT-B37	ZOB-L-2018-001	CNU1502YZX	64bit i7 2ndGN 4GB 500GB HDD	Elitebook 8460p	Hp	Mouse, Battery & Charger		WBGUF0B1RZB1FY	Windows 7		09 Apr 2018		With Back Bag

6. COMPUTER AND INTERNET USAGE – PENALTIES

ANY USER VIOLATING THESE POLICIES OR APPLICABLE LOCAL, STATE, OR FEDERAL LAWS WHILE USING THE COMPANY NETWORK SHALL BE SUBJECT TO LOSS OF NETWORK PRIVILEGES AND ANY OTHER DISCIPLINARY ACTIONS DEEMED APPROPRIATE, POSSIBLY INCLUDING TERMINATION AND CRIMINAL AND/OR CIVIL PROSECUTION.

7. COMPUTER AND INTERNET USAGE – CONCLUSION

- **All terms and conditions as stated in this document are applicable to all users of the Company network and the Internet. These reflect an agreement of all parties and should be governed and interpreted in accordance with the laws of IT.**

- **Note-If you have any questions regarding any of the policy guidelines listed above, please contact your IT Support.**

- **ZettaOne IT request all users to follow and support to prevent data violation and IT Security.**

Thank you

Team IT

ZettaOne