Acceptable Usage Policy

DOCUMENT SUMMARY:

AUTHOR	RENUKA PRASAD	
REVIEWED BY	SAMSON JUDSON	
CURRENT VERSION	4.0	
DATE OF CURRENT VERSION	31/8/2015	
DATE OF ORIGINAL VERSION	06/10/2009	
DOCUMENT TYPE	INFORMATION SECURITY MANAGEMENT SYSTEM MANUAL	
DOCUMENT CIRCULATION	CEO, HEAD-IT, HEAD ADMIN, HR & ITIS TEAM	
OWNER	CISO	
APPROVED BY	NAME:	THIMMAIAH BIDDANDA
	DESIGNATION	CHIEF INFORMATION SECURITY OFFICER

Revision History

Version	Revision	Issue Date	Changes
1	0	06/10/09	Final
2	1	06/09/2010	Change in the webmail access policy
2	2	13/07/2011	TEK logo changed
3	0	10/04/2012	Logo changed, reporting personals and their information security roles added, TEKsystems replaced with TEK-EASi
3	1	5/4/2013	FTP password change policy added
3	2	07/03/2014	TEK log changed
3	2	25/7/2014	Reviewed. No changes done
3	3	15/6/2015	New EASi logo updated. Prasanna name removed and added Samson as Reviewer in Document summary section. Replaced Samson

			with Renuka Prasad as Author in Document summary section.
4	0	31/8/2015	Disciplinary actions – severity and examples added

Table of Contents

1. INTRODUCTION 5

1.1 PURPOSE 5

2. WORK STATIONS SECURITY POLICY 5

2.1 USE OF DESKTOP SYSTEMS 5
2.2 PERSONAL WORK 5
2.3 RESOURCES SHARING 6
2.4 USE OF PRIVILEGED ACCESS 6
2.5 SOFTWARE COPYRIGHT AND LICENSES 6
2.6 UNACCEPTABLE USAGE ACTIVITIES 6
2.7 UNAUTHORIZED ACCESS 7

3. LAPTOP SECURITY POLICY 7

3.1 PHYSICAL SECURITY 7
3.2 DATA BACKUP 8
3.3 MONITORING & AUDITS 8

4. CLEAR DESK AND CLEAR SCREEN: 8

5. GENERAL USE AND SECURITY OF INTERNET ACTIVITIES 9

5.1 USE OF INTERNET RESTRICTED TO BUSINESS USE ONLY 9
5.2 REPRESENTATION OF TEK-EASI POSITION 9
5.3 INTERNET E-MAIL COMMUNICATIONS CONSIDERED PUBLIC 10
5.4 INTERNET RULES OF BEHAVIOUR 10
5.5 PROHIBITIONS ON USER INTERNET ACTIVITIES 10
5.6 UNAUTHORIZED CONNECTIONS TO INTERNET 11
5.7 RESTRICTION ON INTERNET TRANSMISSION OF SENSITIVE COMPANY INFORMATION 11
5.8 RESTRICTIONS ON INTERNET TRANSMISSION OF SENSITIVE INFORMATION 11
5.9 RESTRICTIONS ON EMPLOYEE PRODUCTION OF WWW PAGES 11
5.10 VIRUS SCANNING OF DOWNLOADED INTERNET INFORMATION 12
5.11 RESTRICTIONS ON USAGE OF WEB MAIL 12

5.12 RESTRICTIONS ON POSTING COMPANY MATERIAL TO ANONYMOUS FTP SYSTEMS 12

6. USAGE OF EMAIL AND COMMUNICATION ACTIVITIES 12

6.1 BUSINESS USE ONLY 12
6.2 TREATMENT OF E-MAIL AS CONFIDENTIAL INFORMATION 13
6.3 MANAGEMENT RIGHTS TO REVIEW E-MAIL CONTENT 13
6.4 RESTRICTIONS ON TRANSMISSION OF SENSITIVE INFORMATION VIA E-MAIL . 13
6.5 RESTRICTIONS ON USE OF E-MAIL SERVICES BY THE EMPLOYEES OTHER THAN ASSIGNED INDIVIDUALS 13
6.6 PROHIBITIONS ON AUTOMATIC FORWARDING OF E-MAIL 13
6.7 PROHIBITIONS ON BLANKET FORWARDING OF E-MAIL 13
6.8 PROTECTION OF E-MAIL DUE FOR LEGAL PURPOSES 14
6.9 DISPOSAL OF UNNEEDED INTERNAL CORRESPONDENCE 14
6.10 USAGE OF FTP 14

7. PASSWORD SECURITY POLICY 15

7.1 PASSWORD MANAGEMENT 15
7.2 PASSWORD SELECTION RULES 16

8. PHYSICAL SECURITY POLICY 17

8.1 PROXIMITY CARDS FOR GENERAL ACCESS 17
8.2 ACCESS CARDS RETURN 17
8.3 INSPECTION OF INCOMING AND OUTGOING PACKAGES 17
8.4 DISPOSAL OF MEDIA 18
8.5 SERVER ROOM ACCESS 18

9. INFORMATION SECURITY INCIDENTS AND WEAKNESS 18

9.1 SECURITY INCIDENT 18
9.2 SECURITY WEAKNESS 19
9.3 REPORTING 19

10. GENERAL 20

10.1 ILLEGAL USAGE 20
10.2 SECURITY 20
10.3 USAGE OF STORAGE MEDIA 21

11. DISCIPLINARY ACTION BY TEK-EASI 21

11.1 SEVERITY CATEGORIZATION AND DISCIPLINARY ACTIONS LEVELS 21
ANNEXURE: DISCIPLINARY ACTIONS AND SEVERITY MATRIX - CATEGORIZATION OF VARIOUS VIOLATIONS (SOME EXAMPLES) 22

1. Introduction

This policy addresses the intent of TEKsystems Global Services and EASi, divisions of Allegis Services (India) Private Limited. (Hereinafter referred to as TEK-EASi), to safeguard computing resources from Internet and email based threats. This policy shall underline appropriate user etiquette for workstation, Internet and email usage and define procedures for safeguards from Internet and email borne threats.

1.1 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment, software, operating systems, storage media, and network accounts providing electronic mail, WWW browsing, and FTP, which are the property of TEK-EASi. These systems are to be used for business purposes in serving the interests of the TEK-EASi, and of their clients and customers in the course of normal operations. These rules are in place to protect the interest of TEK-EASi and its employees. Effective security is a team effort involving the participation and support of every TEK-EASi employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Work Stations Security Policy

2.1 Use of desktop systems

Employees are responsible for the security and integrity of information stored on personal desktop system. Users should be aware that the data they create on the corporate systems remains the property of TEK-EASi. User responsibility includes regularly saving work onto the shared network drive (Ex: \\10.188.10.50). All the process related business data should be kept in the assigned process folders (network shared folder), thereby enabling the IT staff to take backup of these critical business data.

2.2 Personal Work

Computing facilities, services, and networks may not be used for work other than that of TEK-EASi.

2.3 Resources Sharing

There should not be any shared folder created on the local desktops provided to individual users. Users shall be advised not to create any shared folder in their respective desktops. Data on the network shares are secured using Windows permissions and access level controls. All directories and sub-directories, which are shared, shall be protected by proper user authentication and permissions to access with relevant access rights.

Avoid storing passwords or other information that can be used to gain access to other network resources. Computer accounts, passwords, and other types of authorization are assigned to individual Employees who are responsible for its security. Revealing user account password to others or allowing use of user account by others is strictly prohibited. This includes family and other household members when work is being done at home.

2.4 Use of privileged access

Special access to information or other special computing privileges is to be used during official duty only. Information that is available through special privileges is to be treated as private & confidential. A deliberate attempt to degrade the performance of a computer system or network or access to any restricted IT Infrastructure is prohibited.

2.5 Software Copyright and Licenses

All software licensing is controlled by TEK-EASi, wherein use of such software is to be agreed by TEK-EASi for use in TEK-EASi. Otherwise, TEK-EASi shall procure Software licenses to be used in TEK-EASi for facilitating its operations. The same needs to be evaluated and approved by Information Security Steering Committee for procurement and use in TEK-EASi.

2.6 Unacceptable Usage activities

- The harmful activities such as creating or propagating viruses; disrupting services; damaging files; intentional destruction or damage to equipment, software, applications, data belonging to TEK-EASi or clients; and the like are strictly prohibited.
- Port scanning or security scanning is expressly prohibited unless prior notification to Security Team.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty, is prohibited.

- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack) and providing information about, or lists of, TEK-EASi employees to parties outside TEK-EASi, are prohibited.
- Security breaches or disruptions of network communication, include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties, is prohibited. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Using TEK-EASi computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction is strictly prohibited.
- Leaving confidential or sensitive information on printing facilities, photocopiers, and facsimile machines.

2.7 Unauthorized access

TEK-EASi employees shall not:

- Damage computer systems
- Obtain extra resources which are not authorized to an individual
- Deprive another user of authorized resources
- Gain unauthorized access to systems

By using knowledge of:

- Vulnerabilities in information systems
- Another TEK-EASi user's password
- Accessibility of a TEK-EASi user during a previous position or role

3. Laptop Security Policy

3.1 Physical Security

The physical security of the laptop is the responsibility of the user to whom the laptop is provided. The following precautions to be ensured

- OS password to be enabled
- Clear screen policy to be invariably followed.

- While travelling the user shall ensure that the bag containing laptop is physically secured under lock and key.
- While travelling via flight the user should carry the laptop as personal baggage.
- While using the laptop at external locations cable lock shall be used to secure the laptop.
- Users should not install/uninstall any software without IT notification.

3.2 Data Backup

Data on the laptop is more expensive to replace than the hardware. The following must be followed –

- If the user is travelling for an extended period of time, the data on the laptop should be backed up.
- The concerned user should contact the System Administrator for backing up of the data on the laptop.
- If a user is travelling, the user can work on the laptop provided by company. However once the user is back in office, he / she should copy the updated files on the file server.
- Anti Virus should always be updated immediately after the return of the user.

3.3 Monitoring & Audits

All the data residing on the laptops is the property of the company. TEK-EASi reserves the right to install any monitoring software on the laptops and the right to monitor or audit the company laptops for any inappropriate, abusive or unethical use. Employees who carry out any inappropriate, abusive or unethical use of the laptops can be held responsible and legal and / or disciplinary action will be taken up against them.

4. Clear Desk and Clear Screen:

Employees are supposed to follow the following principles while operating in their workstations:

Clear Desk

- The workspace of the employees should be maintained clutter free.
- The workspace should not have any extra things/ objects unattended. For e.g. important documents, file binders, printouts etc., which are not being used.

- Sensitive information on paper or electronic storage media should be locked when not required and after office hours.
- There should be no business critical documents kept open on the screen
- Incoming and outgoing mail points to be protected and care should be taken to prevent access to mail by other persons.
- Documents of sensitive nature near printers, fax, photo copier, scanner etc. should be immediately removed.
- Unauthorized use of photocopiers, scanners, digital camera etc. should be avoided

Clear Screen

- TEK-EASi users shall either log off or lock the system if they will be away from their desk for any length of time. (Shortcut combination -  + L - may be used.)
- The system is configured to lock automatically using a secure screen saver if it is not used for a period of 5 minutes.

Banned Activities at Workspace

- Smoking, Eating, and Drinking
- Photography using mobile camera, digital camera
- Photography of desktop/laptop screens
- Photography of all sensitive documents not limited to software code, drawings, customer information, ODC, server room, etc...
- Usage of printers, scanners, copiers and other office equipment's for personal use

5. General Use and Security of Internet Activities

5.1 Use of Internet Restricted to Business Use Only

The Internet should be used as part of the normal execution of a user's job responsibilities.

5.2 Representation of TEK-EASi Position

Internet connections should only be used for valid business purposes. As such, any information posted to discussion groups bearing the company address should only reflect the company positions on approval from CISO.

5.3 Internet E-mail Communications Considered Public

Any messages sent over the Internet are not considered secure unless additional measures are taken to protect such information (e.g., encryption). Users should communicate via e-mail as they would in a public place (e.g., if you are not comfortable saying something to a room of people, it should not be said via e-mail).

5.4 Internet Rules of Behaviour

Using TEK-EASi facilities or equipment to make abusive, unethical or "inappropriate" use of the Internet will not be tolerated and may be considered grounds for disciplinary action, including termination of employment. Examples of inappropriate employee Internet use include, but are not limited to, the following:

- Conducting or participating in illegal activities, including gambling
- Accessing or downloading pornographic material
- Solicitations for any purpose which are not expressly approved by company management
- Revealing or publicizing proprietary or confidential information
- Representing personal opinions as those of the company
- Making or posting indecent remarks
- Uploading or downloading commercial software in violation of its copyright
- Uploading or mailing of company's confidential documents without the permission/authorization of the concerned parties.
- Downloading any software or electronic files without reasonable virus protection measures in place
- Intentionally interfering with the normal operation of Internet gateway

5.5 Prohibitions on User Internet Activities

To prevent any appearance of inappropriate conduct on the Internet and to reduce risk to the organization, users should not:

- Enter into contractual agreements via the Internet; e.g. enter into binding contracts on behalf of the company over the Internet
- Use the company logos or the company materials in any web page or Internet posting unless it has been approved, in advance, by the company management
- Use software files, images, or other information downloaded from the Internet that has not been released for free public use

- If a business need exists, then protective methods and software must be installed on the user's work-station to prevent hackers to get access to the data on the user's work-station
- Introduce material considered indecent, offensive, or is related to the production, use, storage, or transmission of sexually explicit or offensive items on the company network or systems
- Attempt to gain illegal access to remote systems on the Internet
- Attempt to inappropriately telnet to or port scan remote systems on the Internet
- Use or possess Internet scanning or security vulnerability assessment tools without the permission of the ISSM/CISO.
- Post material in violation of copyright law
- Establish Internet or other external network connections that could allow other company users to gain access into TEK-EASi systems and information assets.

5.6 Unauthorized connections to Internet

Users of any computer within the TEK-EASi network is not permitted to connect to Internet through unauthorized means of connectivity.

5.7 Restriction on Internet Transmission of Sensitive Company Information

Restricted or sensitive information should not be transmitted over Internet without reasonable security measures (such as encryption or other appropriate method) in place.

5.8 Restrictions on Internet Transmission of Sensitive Information

Credit card numbers, telephone calling card numbers, login usernames and passwords, and other parameters that can be used to gain access to systems or services should not be sent over the Internet in plain text format.

5.9 Restrictions on Employee Production of WWW Pages

Employees are not allowed to produce web pages or sites that reference the company or affiliates, masquerade as the company, or in any way disclose any other information about the company without the written permission of the company management. Employees are not allowed to host personal sites on the company facilities.

5.10 Virus Scanning of Downloaded Internet Information

All information downloaded to the company computing resources via the Internet should be screened with virus detection software prior to use. Refer to Antivirus Policy.

5.11 Restrictions on Usage of Web mail

Use of public webmail services like Gmail, Yahoo etc. poses a security risk. Webmail is allowed to be used only in case of business needs and at present is allowed only to the following categories

- Directors
- Business Heads
- Managers
- Team Leads

Other users requiring webmail services for Business needs are required to take up with IT team through SRP ticketing system for enabling the service duly recommended by department heads. IT team will enable webmail after taking approval from ISSM/CISO. IT team shall also maintain a list of persons authorized to use webmail. Any user not appearing in this list is not permitted to use webmail services.

5.12 Restrictions on Posting Company Material to Anonymous FTP Systems

Users should not place the company material (software, internal memos, etc.) on any publicly accessible Internet computer, which supports anonymous FTP or similar services, unless the Information Security officer has first approved the posting of these materials.

6. Usage of Email and Communication Activities

6.1 Business Use Only

Electronic Mail systems should be used for business purposes only, unless management has specifically approved the non-business use. The language used should be in consistent with other forms of business communication.

The size of file which can be attached to the email is restricted to 10 MB.

6.2 Treatment of E-mail as Confidential Information

TEK-EASi employees should treat electronic-mail messages and files as confidential information. Electronic mail should be handled as a confidential and direct communication between a sender and a recipient.

6.3 Management Rights to Review E-mail Content

At any time and without prior notice, TEK-EASi management, Information Security officer or Audit team reserve the right to examine e-mail, personal file directories, and other information stored on TEK-EASi computers. This examination assures compliance with TEK-EASi Security Policy, supports the performance of internal investigations, and assists in the management of TEK-EASi information systems.

6.4 Restrictions on Transmission of Sensitive Information via E-mail

Users should not send confidential or sensitive information via E-mail unless the material is encrypted using a company approved encryption technique. In case an encrypted channel is not possible for communicating sensitive information, prior management approval on the transmission of the same shall be taken.

Examples include:

- Company's Confidential Information
- Passwords
- Other confidential or sensitive information

6.5 Restrictions on Use of E-mail Services by the Employees Other than Assigned Individuals

Employees of TEK-EASi accessing company electronic-mail services should not use or access an electronic-mail account assigned to another individual to either send or receive messages. If there is need to read another's mail (while they are away on vacation for instance), message forwarding and other facilities should be used instead.

6.6 Prohibitions on Automatic Forwarding of E-mail

Unless the information owner / originator agree in advance, or unless the information is clearly public in nature, employees should not automatically forward electronic mail to any address outside company networks.

6.7 Prohibitions on Blanket Forwarding of E-mail

Blanket forwarding of electronic-mail messages to any outside address is prohibited.

6.8 Protection of E-mail due for Legal Purposes

Tape rotation or log destruction of both logs and the referenced electronic-mail messages should be postponed whenever a summons, discovery motion, or other legal notice is received. Such destruction should also be postponed if the material might be needed for an imminent legal action.

6.9 Disposal of unneeded Internal Correspondence

While management encourages periodic back-ups of computer-resident information, internal correspondence should be disposed of when no longer needed. Electronic-Mail messages relevant to current activities or that would be expected to become relevant to current activities, should be saved as separate files and retained in accordance with company information retention policies. TEK-EASi users must not use email services for any of the following purposes:

- Initiating or propagating 'chain' email or 'pyramid' emails.
- Sending bulk or unsolicited emails, especially of a commercial nature.
- Using their account as a mail-drop for responses for any of the above actions

The following disclaimer shall be displayed on all e-mails send outside TEK-EASi domain:

"This electronic mail (including any attachments) may contain information that is privileged, confidential, and/or otherwise protected from disclosure to anyone other than its intended recipient(s). Any dissemination or use of this electronic mail or its contents (including any attachments) by persons other than the intended recipient(s) is strictly prohibited. If you have received this message in error, please notify us immediately by reply e-mail so that we may correct our internal records. Please then delete the original message (including any attachments) in its entirety. Thank you."

6.10 Usage of FTP

Anonymous Login is not allowed in FTP servers.

- User name and Password shall be given only to client/PM/TL on request.
- It shall be used for official use only and not for any personal use.
- After completing the projects Users/PM/TL shall inform IS department to disable that FTP user /Folder.
- Prior permission shall be obtained from IS department prior to upload or download more than 200 MB.
- Any browsers or standard FTP client software like Filezilla etc. can be used.
- FTP account passwords shall be changed once in a month.

7. Password Security Policy

7.1 Password Management

Confidentiality of Passwords

User passwords should remain confidential and not shared, posted or otherwise divulged in any manner. Passwords shall not be displayed in any environment (including on office walls, desks and workstations) at any time, including during sign-on procedures

Password Composition

Passwords used by TEK-EASi employees shall have the following characteristics

1. A minimum of 8 characters.
2. At least one Numeral and one special character (* ,@ %,$)
3. No portion of the user name as part of the password

Password Expiration

Passwords should expire after a maximum period of 30 calendar days. Additionally, the same password should not be repeated within a cycle of 5 password changes.

One Time Use of Initial Passwords

If the administrator provides a user with an initial password, the user should change it immediately after the first time log – in to the system. (One-time password).

User Capability to Select Passwords

Users should be provided with the capability to change their password on the login interface (after authentication).

Password Reset

User password resets will be performed when requested by the user, after verification of identity. The 'Password reset request' form should be filled up by the user. The new password should be a one-time password. Only the individual to whom the user-ID is assigned should request for user password reset. LAN and Desktop Security Administrator/ISSM systems should be informed whenever a password is reset for a particular user. In case of request for change of password sent through another user's login ID, a cc of the mail needs to be sent to the person whose password is being reset.

Screen Saver Password

All users should use the screen saver with password, which should be activated within 5 minutes of inactivity.

Responsibility

It is the responsibility of IT users to rigorously follow the password security policy. The IT users should formally inform the LAN and Desktop Security Administrator about any lapse on the password security either orally or by e-mail.

7.2 Password Selection Rules

Prohibition of Easy Guess Passwords

Users should be encouraged to create passwords that will prohibit easy guessing (i.e., passwords such as spouse's first name, Children name, etc.).

Examples of good passwords

- Lap$top3
- you@Us1

Passwords should not be based on any of the following: (Best practices)

Bad Examples of password as mentioned below to be avoided as these are easily guessable by any person with malicious intent.

- Months of the year, days of the week or any other aspect of the date (like date of birth, date of joining etc.)
- Name of your spouse, parent, colleague, friend, pet, towns, months, days.
- Birthdays – of the user or near and dear ones
- Number of car/motorbike registration, telephone.
- Employee No. / Employee Id or designations
- Project or department name or references
- Company names, identifiers or references
- Telephone numbers or similar all-numeric groups
- User ID, user name, group ID or other system identifier
- More than two consecutive identical characters
- All-number or all-alphabetic groups
- Common dictionary words
- A series of identical numbers/letters like abcd1234
- Obvious keyboard sequences like asdfgh, qwerty

- Any of the above in inverse or with a number before or after.

Password rule enforcement procedure

- Passwords of less than 8 characters (10 characters for privileged users) and not containing special characters, CAPS, numerals is not allowed
- Password minimum duration is 24 hours
- Validity of password is set to 30 days
- The previous 5 passwords is not allowed to reuse
- Automatic account lockout occurs after 5 consecutive unsuccessful logon attempts by any user.

8. Physical Security Policy

8.1 Proximity Cards for General Access

Access Cards are provided to all personnel inside TEK-EASi. These Access cards can be used to provide access to the various departments including IT Department. The access rights are to be defined for employee as per his/her job function. These cards should also be provided to 3rd party vendors placed in-house for support services.

8.2 Access Cards return

All representatives of the concerned 3rd party vendors who have completed their tenure at TEK-EASi must return their access cards to the Administration Department. The concerned Administration Department personnel will then disable the access for those cards.

Any employee of TEK-EASi who quits the organization must return his / her access card to the IT Department. The IT Department personnel will then disable the access for the card.

8.3 Inspection of incoming and outgoing packages

Inspection of incoming and outgoing packages (e.g. bags, briefcases, boxes, laptop computers, etc.) must be conducted to ensure the unauthorized materials are not brought in or taken out of TEK-EASi premises. All incoming material should be declared at the security office and a gate-pass document given for clearance of the same. A gate pass duly approved by the respective authority should support any material/ article belonging to TEK-EASi, taken out of TEK-EASi.

8.4 Disposal of Media

Equipment which contains sensitive material should be properly discarded or destroyed at the end of its functional life. The equipment used in storing TEK-EASi's data, when disposed of, should be done with due consideration and care. Sensitive data, licensed software, and other material should be properly erased or overwritten when destroying or refurbishing and protected when under repair.

Following is the list of items that require secure disposal and mode of secure disposal:

- Paper documents: paper shredders should be used it should be physically destroyed
- Carbon paper: paper shredders should be used or it should be physically destroyed
- Floppy Diskettes: the floppy should be formatted and then media from the protective covering should be removed and physically broken
- Hard Disk Drives: the HDD should be degaussed/ erased using tools like DBAN
- Tape Medias: Shredders should be used.
- Compact Disks & DVDs: these should be physically broken or destroyed by means like shredding or incineration.

8.5 Server room access

Access to server room is restricted, monitored and on permission by CISO.

Banned Activities

- Smoking, Eating, Drinking
- Photography

Banned Items

- Bags of any type.
- Mobiles
- Cameras
- Removable Memory Devices (Pen Drives, External HDD etc.)
- Personal Laptops
- Electronic Messaging Devices

9. Information Security Incidents and Weakness

9.1 Security Incident

'Incident' is a term related to exceptional situations or a situation that warrants intervention of senior management. An incident is detected in day-to-day operations and management

of the IT function. This may be result of unusual circumstances as well as the violations of existing policies and procedures of TEK-EASi.

Some examples of Information security incidents

- Suspected hacking attempts
- Successful hacking attempts
- DoS attacks, Ping of Death attacks,
- Port scanning
- Loss of information due to unknown reasons
- Hardware resources and components lost / stolen
- Virus incidents regarding e-mail, Internet, CD, diskette and others
- Failure / crash of IT equipment
- Power problems and loss of data
- Natural calamity or disaster
- Hardware, Software, and Operational errors that results in erroneous data

9.2 Security Weakness

An information security weakness is a condition or circumstance that poses a risk of unauthorized access to confidential information, unauthorized access to TEK-EASi computers or networks, damage to or interference with TEK-EASi computers or networks, or loss of information.

Some examples of Information security weaknesses

- Known uses of insecure (weak) passwords or sharing of passwords
- Suspicious data flows in or out of a system
- Key logger(s) installed on a desktop or laptop computer
- Systems that are known to be configured in an insecure manner

9.3 Reporting

Any security incidents coming to the notice of TEK-EASi employees has to be reported to

- IT Helpdesk
- Information security Manager/Officer
- CISO

by the following modes of communication

- Email or through SRP ticketing system to IT helpdesk
- Verbally in person or phone to ISSM/ISSO/CISO

The person receiving the information shall fill the incident report form and forward to ISSM/ISSO for necessary action. The ISSM/ISSO must notify the same to the CISO and corrective action must be initiated with the help of IT Dept. / Administration team / Security Incident Response Team.

Information Security events should be reported to outside authorities whenever this is required to comply with legal requirements or regulations. This shall only be done by the ISSM or persons authorized by ISSM in consultation with the legal department.

Suspected Information Security events shall be reported promptly to the IT team or directly to ISSM if found critical.

Information Security events shall be reported to outside authorities whenever this is required to comply with legal requirements or regulations. This shall only be done by the ISSM or persons authorized by ISSM in consultation with the legal department.

	Name	Organizational Role	Information security Role
1	Thimmaiah Biddanda	Director	CISO
2	Samson Judson	Manager - IS	ISSM
3	Renuka Prasad	Asst.Manager - IS	ISSO

10. General

10.1 Illegal Usage

Transmission, storage, or distribution of any information, data or material in violation of any applicable law or regulation is prohibited. This includes, but is not limited to: copyrighted material, trademark, trade secret or other intellectual property used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat.

10.2 Security

Violations of system or network security are prohibited, and may result in criminal and civil liability until unless they are authorized to do so. Examples include, but are not limited to the following: Unauthorized access, use, probe, or scan of a systems security or authentication measures, data or traffic; Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to

overload a system and broadcast attacks; Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting.

10.3 Usage of Storage Media

Any storage media, not limited to Floppy, CD-ROM, Pen/USB drive, should be used only after the prior approval of CISO. Use of camera is strictly prohibited on operation floors.

11. Disciplinary action by TEK-EASi

The acceptable usage policy must be adhered to by all employees of TEK-EASi. Any breach, whether intentional or unintentional, shall be viewed seriously by TEK-EASi. TEK-EASi reserves the right to take necessary disciplinary action against the employee in breach of this policy. Depending upon the seriousness of the breach, TEK-EASi may in its sole discretion, decide upon the type of disciplinary action which may include summary dismissal without notice.

11.1 Severity Categorization and Disciplinary Actions levels

TEK-EASi has classified the severity of breach into three levels namely High, Medium and Low and has defined the disciplinary actions for each category of the violation. The disciplinary action will be decided on a case-to-case basis depending on the impact of the violation on the information systems resources of TEK-EASi. In making the decision, the CISO and ISSC will also refer to the HR policies of TEK-EASi.

The list mentioning the type of violation shall be maintained and updated by CISO, HR and IT teams and will be reviewed and approved by ISSC. For all new type of violation, disciplinary actions will be defined by CISO, HR and IT teams in consultation with ISSC.

The CISO and ISSC will decide disciplinary actions for violations of High, Medium and Low severity. If any Low or Medium is repeated more than once it will be considered to the next higher severity (for e.g. Two Lows will be considered to One Medium & Two Mediums will be considered as High). Following are the disciplinary actions for each category of violation:

	Severity Category	Possible Disciplinary Action
1	High	Suspension from Service / Termination of Employment / Cancellation of Contract / Severe Reprimand (if Management agrees)
2	Medium	Severe Reprimand / Suspension from Service
3	Low	Reprimand / Warning

Annexure: Disciplinary Actions and Severity Matrix - Categorization of Various Violations (Some examples)

Type of violation		Severity		
		High	Medium	Low
	Physical Security			
1	Making or allowing an unauthorized entry into restricted areas	✓		
2	Smoking, eating or drinking in the server room	✓		
3	Improper handling of DVDs, Hard Drive, Tapes etc. (e.g., bringing magnetic material near such storage media, not ensuring proper atmospheric conditions for their storage, etc.)		✓	
4	Unauthorized removal of equipment from the premises	✓		
5	Unauthorized relocation of equipment inside the premises			✓
6	Leaving laptops unattended in common areas while in office.			✓
7	Non -adherence to environmental precautions for server room	✓		
8	During exit/entry frisking if found any unauthorised materials like Camera, Pen/USB Drives, Sensitive printouts etc.	✓		
	E-Mail Security			
8	Unauthorized use of another person's e-mail	✓		
9	Sending viruses through e-mail attachments	✓		
10	Using e-mail in a manner that: • Interferes with normal business activities or hampers employee productivity, • Embarrasses TEK-EASi. • Consumes TEK-EASi resources in excess • Involves solicitation • Is associated with any for-profit outside business activity	✓		

Type of violation		Severity		
		High	Medium	Low
11	Transmitting confidential or sensitive TEK-EASi information in an unencrypted form	✓		
12	Inappropriate auto forwarding of e-mail		✓	
13	Forwarding of confidential e-mail		✓	
14	Sending profane, obscene or derogatory e-mails	✓		
	Password Policy			
15	Re-use of same passwords or using the same password across different systems			✓
16	Password sharing / disclosure	✓		
17	Insecure conveyance / storage of passwords by users		✓	
18	Insecure conveyance / storage of critical passwords	✓		
19	Requesting / making unauthorized password resets of other users in their absence	✓		
20	Requesting / making password resets of other users in their absence for emergency business purposes		✓	
21	Disabling of screen saver password by users			✓
22	Not disabling/changing default passwords		✓	
24	Sharing of passwords by users		✓	
	IT Security			
25	Surfing obscene sites	✓		
26	Using pirated software	✓		
27	Bringing outside Media	✓		
28	Transferring TEK-EASi Data / Information outside	✓		
29	Taking photography using Mobile/digital camera inside office, ODC, Customer ODC (If working from customer location)	✓		
30	Usage of printers, scanners, copiers and other office equipment's for personal use		✓	