IT Policy
For
IASE Deemed University

Index

INTRODUCTION

IASE security policies provide a framework for best practice that is to be followed by all employees. Information security policy defines the organization's attitude to information, and announces internally that information is an asset, the property of the Organization, and is to be protected from unauthorized access, modification, disclosure, and destruction.

This security policy is a strategy for how IASE will implement Information Security principles and technologies. This policy document provides both high level and specific guidelines on how to protect university's data.

Implementing this security policy indicates senior management's commitment to maintaining a secure network, which allows the IT Staff to do a more effective job of securing the university's information assets. The audience group of this policy is

- Management – all levels
- IT Technical Staff – systems administrators, etc
- End Users

Finally this security policy document will also help turn staff into participants in the IASE's efforts to secure its information assets

Computer information systems and networks are an integral part of work at IASE. The association has made a substantial investment in human and financial resources to create these systems. The enclosed policies and directives have been established in order to protect this investment, safeguard the information contained within these systems and reduce business and legal risk. Violations of this policy may result in disciplinary action in accordance with the IASE Employee Handbook.

ADMINISTRATION

The Information Technology Coordinator/Admin is responsible for the administration of this policy. Responsibilities include the development and maintenance of written standards and procedures necessary to ensure implementation of and compliance with these policy directives. Also to provide support and guidance to employees to fulfill their responsibilities under this directive.

Each employee shall be responsible for all computer transactions that are made with his/her User ID and password, not disclose passwords to others and adhere to procedures developed by the IT Department.

The IT admin shall create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy. The IT admin

shall notify the IT Coordinator promptly whenever an employee leaves the company so that his/her access can be revoked.

1. PHYSICAL SECURITY

It is IASE policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

Employee Responsibilities

- Critical computer equipment, e.g., file servers, must be protected by an uninterruptible
- Power supply (UPS). Other computer equipment should be protected by a surge suppressor.
- Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
- Employees shall not perform equipment installations, disconnections, modifications, and relocations.
- Employees shall not take shared portable equipment such as laptop computers out of the office without the informed consent of the IT admin. Employees must sign out the equipment and note the purpose for which it will be used.
- Employees shall exercise care to safeguard the equipment assigned to them.

Copyrights and License Agreements

It is IASE policy to comply with all laws regarding intellectual property. IASE and its employees are legally bound to comply with the Copyright Act and all proprietary software license agreements. Noncompliance can expose IASE and the responsible employee(s) to civil and/or criminal penalties. All installed software must be licensed according to the instructions of the software manufacturer.

This policy applies to all software that is owned by IASE, licensed to IASE, or developed using IASE resources by employees or vendors. All persons who make use of any or all of IASE software or hardware are subject to the policies defined herein.

2. IT RESPONSIBILITIES

The IT Coordinator or IT admin shall maintain records of software licenses owned by IASE and periodically scan company computers to verify that only authorized software is installed.

Employee Responsibilities

Employees shall not install software unless authorized by the IT Coordinator. Only software that is licensed to or owned by IASE is to be installed on IASE computers.
A list of free ware software shall be made by IT department and the same can be installed by any staff of IASE/GVM. No pirated version of any software shall be installed in any computer and doing so shall make the staff liable for action by the management.
If any individual or department needs any software then he/she must take authorization from his department head and then the registrar for the same and then purchase it. All purchase of software shall be logged by IT department.
Staff shall not copy or download software without proper authorization.

3. E MAIL AND INTERNET POLICY

(A) Acceptable Uses of the Internet and IASE E mail

1. Every employee or department will have his dedicated Email ID
2. IASE encourages the use of the Internet and e mail because it makes communication more efficient and effective. Occasional and reasonable personal use of IASE's Internet and email services is permitted, provided that this does not interfere with work performance. However, Internet service and e mail are IASE property. Every employee has a responsibility to maintain and enhance IASE's public image and to use IASE e mail and Internet access in a productive manner.

   We have established the following guidelines for using e mail and the Internet. Any unauthorized or improper use of e mail or the Internet is not acceptable and will not be permitted.

(B) Unacceptable Uses of the Internet and E mail :-

IASE e mail and Internet access may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or materials that are obscene or X rated. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual orientation may be transmitted or forwarded using the IASE system. No abusive, profane or offensive language may be transmitted through YOUR COMPANY's e mail or Internet system. YOUR COMPANY's harassment policy applies in full to e mail and Internet use. Employees do not have a personal privacy right regarding any matter created, received, stored or sent from or on the company's e mail or Internet system or computers.

IASE e mail and Irternet system also may not be used for any other purpose that is illegal, against IASE policy or contrary to IASE's best interest. Solicitation of non IASE business or any use of IASE e mail or Internet system for personal gain is prohibited.

(C) Rules for Electronic Communications

Each employee is responsible for the content of all text, audio, or images that he or she places on or sends over IASE's e mail or Internet system. Employees may not hide their identities or represent that any e mail or other electronic communications were sent from someone else or someone from another company or university. Employees must include their name in all messages communicated on IASE's e mail or Internet system.

Any messages or information sent by an employee to another individual outside IASE via IASE e mail or Internet system (including info of services or Internet sites) are statements that reflect on IASE. Despite personal "disclaimers" in electronic messages, any statements may be tied to IASE.All communications sent by employees via IASE's e mail or Internet system must comply with all IASE policies and may not disclose any confidential or proprietary IASE information.

If employees receive unsolicited e mail from outside IASE that appears to violate this policy, the employee should notify his or her supervisor immediately. Similarly, if any employee accidentally accesses an inappropriate web site in the normal course of work, the employee should notify his or her supervisor immediately.

(D) Downloading Software

To prevent the downloading of computer viruses that could contaminate the e mail or Internet system, no employee may download software from the Internet without prior authorization. Any and all software that is downloaded from the Internet must be registered to IASE. For authorization, please contact the system administrator or IT admin.

(E) Internet distribution

Internet will be distributed as per the grade of the employees:-

Grade 1:- All rights and unlimited access of Internet (no log will be maintained)

Grade 2:- Limited rights and limited aces of the websites (full log will be maintained)

Students: - Limited rights and limited aces of the websites

Ever user will have his dedicated user name and password for internet acces. When login

will display his rights and limitations
No user will be able to access the internet beyond allocation (for e.g. if any user is allowed to access or download 200 GB/month he will not be able to access internet if finish)

4. COMPUTER VIRUSES

The IT Coordinator/IT admin shall install and maintain appropriate antivirus software on all computers, respond to all virus attacks, destroy any virus detected, and document each incident. Employees shall not knowingly introduce a computer virus into company computers nor load diskettes or executable files unless approved by the IT Coordinator. Any employee who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY notify the IT Coordinator.

5. ACCESS CODES AND PASSWORDS

The confidentiality and integrity of data stored on company computer systems must be protected by controls to ensure that only authorized employees have access. Access shall be restricted to those capabilities that are appropriate to each employee's job duties. Passwords shall not be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved. Passwords should not identify an employee's name, address, date of birth, username, nickname, or any term that could easily be guessed by someone. Passwords are not be displayed or concealed on your workspace.

IASE's password policy will address the passwords for the following IT systems:

Network and client operating system

Administrative Passwords

Administrative passwords are only to be developed and used by the IT Coordinator/IT admin. These passwords are subject to stringent composition, frequent change, and limited access. This includes passwords for:-

- Routers/Switches
- Wider Area Network links
- Servers
- Internet connections
- Administrative level network operating system accounts and any other IT resource.

Password Reset Procedure

Implementation of ERP will enable the use of single sign-on technology for user access to various applications. ERP will require verification of an individual's identity.

ERP will be responsible for verifying an employee's identification as part of the employment process. Because the credentials (user name login and password) are now used for ERP certification, it is necessary to strengthen the process for resetting passwords.

The password reset procedure is as follows:

For employees:

- Individuals like LDC etc may request a password reset for themselves by e-mail or phone:
- They must provide their employee ID number.
- The ERP Service Desk will verify the employee ID number before processing the reset, and record it in the system which will provide an audit trail for all password resets.
- Managers, supervisors, or other trusted employees may request a password reset for another individual:
- They must provide both the employee ID number of the individual needing the password reset and their own employee ID number.
- The Service Desk will verify both employee ID numbers before processing the reset, and record them in the system which will provide an audit trail for all password resets.
  Or
- They online reset their password

For contractors:

- IASE admin or other "trusted individuals/employees" may request a password reset on behalf of a contractor:

6. POLICY FOR IASE NETWORK

The requirements apply to all MS Windows or freeware computers intending to connect to the IASE network, including those owned by IASE as well as other MS Windows or freeware computers used for University business purposes.

Desktop Computers

- Devices that fit the following criteria are subject to the minimum standards for connecting desktop and laptop computers to the IASE network.
- Single user device, such as a laptop or desktop computer, that does not perform file serving functions
- Device that operates with software that can be configured or modified from elsewhere on the network
- Device that does not contain any "restricted" data

- Device that does not provide an "essential" service

1. IT admin may specify which version of the operating system IASE computers must utilize. Older versions may be vulnerable to attacks which cannot be mitigated. Free wares and open source is highly recommended as they can be easily updated.
2. Antivirus software, e.g., quick heal, must be installed and active, and the virus definitions must be kept up-to-date. Antivirus software must either be configured to be managed by the central antivirus server or be configured for immediate virus definition update.
3. All computers must be configured to require a login upon booting or restart and before exiting "sleep" or screen-saver modes.
4. The built-in local administrator account name must be renamed (it cannot be "Administrator"), and its password and all other passwords changed to meet or exceed the requirements of IASE's password policy.
5. The built-in local administrator account shall not be used as the primary user account. Normal user accounts, e.g., the accounts used to log into the computer for normal operation, shall not be a member of the local host's administrator group.
6. The Guest account must be disabled.
7. Generic or anonymous access must be disabled.
8. All computers must be registered with the Technology Service Desk including their location, the MAC address of the NIC(s), and the names of the primary users. The computer name must follow the standard convention of department ID followed by first initial plus full last name of the primary user up to 8 characters (or a similar format that facilitates the identification of the computer's primary user). If the naming of the computer must deviate from the convention as dictated by the specific business use of the machine, it must be registered with the appropriate IT admin along with the contact information of the primary user.
9. Any server-type applications and services running on the computer must be inspected by the appropriate IT admin for appropriate configuration with respect to security compliance prior to the computer's deployment.
10. All software must be installed with prior approval of departmental IT admin. IT admin reserve the right to remove all unapproved software on IASE-owned computers.
11. E-mail, telnet, and/or FTP software shall be configured to use only encrypted transmission for authentication.

Servers

1. Servers, including any computers performing file serving functions, running the operating system(windows/ Linux) can only be connected to the IASE network if they meet both the requirements listed above for desktop and laptop computers and the following conditions:
2. Servers must have registered or licenses OS.
3. Any server running critical services or on which sensitive data resides must be in a

physically secure location, e.g., in a locked room or facility with restricted authorized access.

4. All unnecessary or unused services must be disabled.
5. Server configuration must be fully documented.
6. Servers must be configured with NTFS.
7. All NTFS file permissions must be changed to ensure that only authorized access is allowed for all files. In particular, the Everyone group must be carefully managed to prevent unauthorized access to restricted data.
8. Any change to a registered server affecting compliance with these requirements must be reported to IR&C prior to implementation.

Must follow:-

Security Requirements for IASE Networked Devices (laptop, desktop or servers etc)

The following requirements must be met for all devices connected to the data network, such as desktop or laptop computers, file servers, mail servers, and printers..

1. Passwords

All IASE networked devices must employ adequate access control measures to ensure that only authorized individuals may gain access to their resources. Electronic communications systems or services must authenticate users by means of passwords or other secure authentication processes in accordance with the IASE password policy. In addition, shared-access systems must enforce these standards whenever possible and appropriate.

IASE networked devices should also require that users change any preassigned passwords immediately upon initial access to the account. Default passwords for access to network-accessible devices are discouraged, but if used, must be changed immediately.

Passwords used by system administrators for their personal access to a service or device must not be the same as those used for privileged access to any service or device.

2. Access to Unattended Computers

Unauthorized use of an unattended device can result in harmful or fraudulent modification of data, unauthorized access to confidential information, fraudulent e-mail use, or any number of other potentially dangerous situations. In light of this, where possible and appropriate, devices must be configured to "lock" and require a user to re-authenticate if left unattended for an extended period of time.

3. Software Patch Updates

IASE networked devices must be subject to professional system and change-management practices. In particular, networked devices should run versions of operating system and application software for which security patches are made available and installed in a timely fashion(highly recommend free wares). Exceptions may be made for patches that compromise the usability of critical applications but they should be known to IASE IT admin. Implementation of additional measures may be required when exceptions are granted.

4. Anti-Virus or Anti-Spyware Software

When readily available for specific operating systems as defined in the minimum standards, anti-virus software must be running, up-to-date, and have current virus definition files installed on every level of device, including clients, file servers, mail servers, printers, and other types of

5. Authenticated E-mail Relays

IASE devices must not provide an active SMTP service that allows unauthorized individuals to send or relay email messages, i.e., to process an e-mail message where neither the sender nor the recipient is a local user. Before transmitting e-mail to a non-local address, the sender must authenticate to the SMTP service. Authenticating the machine, e.g., IP address/domain name, rather than the sender is not sufficient to meet this standard. Unless an unauthenticated relay service has been reviewed and approved by IT admin as to configuration and appropriate use, it may not operate on the IASE network.

COMPUTER HARDWARE POLICY DESKTOP / NOTEBOOK / TABLET COMPUTERS

All PCs (Desktop, Notebook, or Tablet) must be purchased according to the University PC Procurement process.

On demand of any hardware:-

- Prior to purchasing any hardware or software, an online note sheet should be submitted to initiate the review process. The form will be linked to the purchase requisition.
- When the Purchasing Department receives a purchase order, it will verify that a hardware\software acquisition form has been reviewed by IT admin and approved by the appropriate authority (VC/Registrar). If
  a) Available in stock :- Handover it to requirement department
  b) Not available in stock: - He will process the purchase order. If the review process has not been completed, the Purchasing department will wait until the review is finished.
- IT admin will work with the department to determine if:
  a) The hardware\software will be compatible with the networking infrastructure for the University.
  b) IT department will be able to provide technical support for the hardware\software being acquired.
  c) There is already a license agreement in-place to cover the software.
  d) The agreement(s) will conflict with existing agreements.
  e) The agreement(s) will need to be part of the University hardware\software license management program.
  f) Another hardware\software vendor may provide better pricing or arrangements.

- If there are discrepancies, IT admin will work with the department to document those situations. Department heads will be asked to "sign-off" on non-conforming purchases, which will be made in spite of potential conflicts with the items listed above. Once completed, IT admin will "sign-off" on the form so the procurement process can continue.
- It is expected that IT admin will initiate the review of the electronic hardware\software acquisition form within one business day of the electronic submission of the form. If there are no conflicts or questions to be answered after initial review of the form IT admin will "sign-off" on the form without needing to contact the individual or department. Purchasing will be able to view the current queue of forms to be able to determine whether or not to continue the purchase order process.

7. CHANGE MANAGEMENT POLICY (INCLUDING WEBSITE)

Purpose

The purpose of this policy is to establish standards for managing any change or updates related processes in a structured and controlled manner. It is most important to properly manage any change in the IT (hardware, software, network, utilities etc.) environment owned and operated by IASE(d) university. Effective implementation of this policy will ensure that any unauthorized, unwanted change to the IT environment will not take place.

This policy applies to the entire information technology environment owned and operated by IASE. This policy covers all the employees, third party personnel, contractors and all the concerned individuals who operate, use, manage the IT environment of IASE.

There are number of possible threats which can be materialized and cause impact to business operations of IASE resulting from changes to the IT environment of IASE whether these changes are made intentionally or unintentionally. In order to analyze any risk areas or concerns which can surface due to any change in the IT environment and initiate proactive controls to address these areas, it is advisable to devise and adopt a proper change management system.

Enforcement

Any employee found to have violated this policy and its controls may be subject to disciplinary action.

Standards

Any change in the IT environment of IASE should be executed following a proper change life cycle management. This includes various processes from change initiation to final roll-out of the change.

Standard is as follows:-

Initial user request Any change required to be done in the IT environment (hardware, software, tools, utilities, network, services etc.) should be initiated by the concerned user / department. It is required to detail out the requirement in the change request form and submitting to IT for further process.

- Approval of request the requested changes should be approved by concerned heads (VC or registrar) and the IT Head before the next actions. The approval will ensure that the requested changes are analyzed for its suitability, impact; risk areas etc. and only authorized changes are forwarded to the implementation process.
- Change Classification and Prioritization the approved changes need to be classified based on parameters like criticality to the operations, impact etc. Priority can be assigned to the change requests so as to ensure the top or high priority changes are acted upon immediately.
- Roll back from the change It is one of the best practices to devise and document the roll-back process for any change to ensure that for any unsuccessful change, the IT environment can be restored to the status before the change is implemented. This helps in reducing the business or operational impact.
- Executing and testing the change all the approved changes should be executed based on the category and priority assigned to them. Depending upon the areas where the change request is made, various teams can be assigned the responsibilities to carry out the changes. The teams involved could be IT Hardware, Software, Application, Operating system support, Help Desk, Facilities, third parties etc.
- The changes should be made in a test environment and suitably tested before implementing the same to the live business environment.
- Final Roll-out The tested and verified changes should be moved to the final roll-out process where concerned teams from IT and business functions will implement the changes in the live environment. The changes which are implemented in the live environment should be monitored for certain period to ensure the successful roll-out.
- Documenting the changes It is mandatory to maintain the necessary documentation for all the changes to ensure that the change management process is properly followed. This will also help in post change analysis such as trend analysis, time lines of change management, effectiveness of change management process etc.
- Control process for Emergency Changes It is possible that due to certain emergency situations, there would be time constraints for implementation of the change and hence the change management process could not be followed. In-spite of this it is required to follow a structured process for implementing these types of changes. A change follow-up process should be carried out for these changes and proper documentation need to be maintained for the same.

Control process for Emergency Changes

For any IT environment change requiring emergency actions and response process, and hence there are time constraints to follow the above mentioned process, then, the following procedures shall be adopted:

- In-case of emergency verbal approvals shall be obtained from respective heads and IT Head for addressing the emergency change requirements from respective functional heads.
- Functional User department representatives and the IT support personnel, in conjunction with the subject matter experts, as required (Vendors, Third parties), shall co-ordinate the process of the emergency program changes with adequate supervision.
- Once the emergency change request has been resolved, the concerned team leader shall ensure that all activities performed for the emergency program changes are documented. This documentation would include the names of program files changed, reasons for change, effect on other functionality of the application, test conducted to verify accuracy of the changes, along with the user sign-off.
- Any sub-normal procedures followed during the emergency program change (e.g. giving super-user or root password to the support personnel performing trouble-shooting etc.) should be identified and restored to the original settings and configurations.
- Even in the situation of an emergency, the 'need-to-do' principle shall be followed, with appropriate restrictions on the support personnel executing program changes.
- The testing should be carried out in such a manner so as to ensure the accuracy and integrity of live data and systems.
- The documentation recommended in documenting the changes for normal change management procedures shall also be completed after implementing emergency program changes.

8. HARDWARE MAINTENANCE AND TROUBLE SHOOTING

We have hardware and networking engineer to maintain all our hardware.
OR
University can take AMC of the same

University wil renew of take AMC of every hardware listed below:-

1. Printers
2. Scanner
3. Network devices
4. Computers
5. Laptops
6. Servers

- ✓ The vendor shall provide the following service to keep the equipment in good working condition.
- ✓ The vendor shall carry out scheduled preventive maintenance, as per mutually agreed time schedule.
- ✓ The vendor shall also be responsible for any unscheduled on call corrective and remedial maintenance services to set right the malfunctions of the system. This may include replacement of unserviceable parts.
- ✓ The vendor shall attend on call services within 12 hours (in case of major cities) and 48 hours (in case of mofussil centres) of lodging a complaint and get any error or fault corrected within 24 hours, thereafter.
- ✓ The vendor shall not sub-contract or permit any third party other than the vendor's personnel to perform any work, service or other performance required of the vendor under this agreement without the prior written consent of IASE University.
- ✓ If the machines supplied are not attended for repair or problems are not rectified within the time frame mentioned in Annual Maintenance Contract, the IASE University would get such defective machines repaired by some third party, and the amount spent for such repairs would be billed to the vendor.
- ✓ The vendor shall submit consolidated report furnishing the details of breakdown calls attended and its status on monthly basis.
- ✓ The vendor shall identify 2 Engineer as single point contact for coordinating and providing services to the offices.
- ✓ The vendor shall provide a substitute in case the engineer is not available.
- ✓ The vendor shall make AMC services available on all days as and when requested by the IASE University.
- ✓ Items covered under the contract

Mother board, RAM, monitors display, SMPS, hard disk, LAN card of PCs and connected items
Mother board RAM, monitor display, SMPS, scsi hard disk, scsi LAN servers and connected items pressure roller, logic board, Teflon sleeve, paper pick up roller for printer and connected items
Scanner assembling, scanner unit and PCB and connected items
Laptop: Motherboard, RAM, hard disk, DVD writer, LCD screen, keyboard, touch pad and connected items Printers

OBLIGATIONS OF THE IASE University

1. The IASE University will pay Annual Maintenance Charges. The maintenance charges are payable quarterly in arrears (at the end of quarter) after statutory deductions, if any.
2. The IASE University is to ensure that as far as possible, power source, air conditioning and dust free environment are provided to sites where systems are installed (only for Server Network).
3. The IASE University would intimate to the vendor, if any additional attachments, features or devices are to be directly or indirectly, connected to the equipments.
4. The IASE University would ensure that rats, insects etc., do not invade the site and damage the systems, especially cables etc.

Hardware and Software Security Policy

Procedures shall be in place to ensure that maintenance and repair activities are accomplished without adversely affecting system security. The procedures shall:

- Establish who performs maintenance and repair activities.
- Contain procedures for performance of emergency repair and maintenance.
- Contain the management of hardware/software warranties and upgrade policies to maximize use of such items to minimize costs.
- Describe how items are serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitize devices removed from the site).
- Contain the controlling of remote maintenance services where diagnostic procedures or maintenance are performed through telecommunications arrangements.

The following configuration management practices shall be documented and maintained for all LSA applications:

- Version control that associates system components to the appropriate system version
- Procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production.
- Impact analyses to determine the effect of proposed changes on existing security controls to include the required training for both technical and user communities associated with the change in hardware/software.
- Change identification, approval, and documentation procedures.
- Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes.
- Procedures for using test data "live" data or made-up data.
- Procedures on how emergency fixes are handled.