Policies & Procedures on Information System Resources

Purpose

Information Systems Resources are valuable assets of the Institute and therefore they must be treated accordingly. This Policy & Procedures statement establish policies and procedures for dealing with Information Systems Resources of the Institute and must be reviewed at least once a year.

I. Policies

1. Information Systems' Resources must be kept in a state satisfying all following conditions:

- Maintenance of application and data integrity.
- Assurance that automated information systems perform their critical functions correctly, in a timely manner, and under adequate controls.
- Protection against unauthorized access of information.
- Assurance of the continued availability of reliable and critical information.

2. Information Systems' resources include the following

- Network resources
- Hardware resources
- Software resources
- Data resources

II. Procedures

1. Applicability:

These procedures apply to all faculty, staff, students and guests accessing Information Systems applications of the Institute. The procedures are intended to allow proper use of all Information Systems' resources, effective protection of individual users, equitable access and proper management of those resources.

2. Use of Information System:

Proper use of Information Systems' resources must adhere to the following criteria:

- To be used for official functions and work of the Institute

- Upheld of intellectual property rights.
- Protection of software licensed or owned by the Institute.

3. Confidentiality:

3.1 General rules

Information unless it is declared as public and accessible openly from the Institute's web sites, is confidential, and therefore must be protected from unauthorized access or modification. Confidential information must be accessible only by relevant persons who are authorized by the owner in the performance of their duties. Data containing any confidential information must be readily identifiable and treated as confidential in its entirety. Disclosure of confidential data to unauthorized persons in any format is strictly prohibited.

3.2 Password rules

- The password must consist of at least 8 characters; uppercase, lowercase, digit and special character; cannot include space and control character, and be based on any word found in a dictionary or on any name (, e.g. person, project), neither be based on these reversed
- Automatic logout of the account after 3 unsuccessful attempts and the locked account can only be reset by the System Administrator.
- For change of password, 5 past passwords cannot be reused.
- Passwords must be hashed using the most secured hashing algorithm available.

3.3 Network access

- All client/server applications can only be accessed from campus network without any exception.
- Web based applications in general must be accessible from campus network only, however exception may be made if it is necessary.
- All applications must be accessed using secure communication over Internet or network (e.g. https)
- Wireless communication must use security protocol which requires authentication and includes encryption

3.4 User Access Management

- Any request for creation, modification, and deletion of user access account must be requested using appropriate form and approved by the head of the

data owner's department or person delegated by the head department concerned and then submitted to the IT department for further action. The request must include the access rights to be granted to the account.

- Review of the user accounts, together with the granted access rights, must be conducted at least once a year, and documented.

3.5 General server security

- Access by high-privileged to the application and database server must be logged and the logs must periodically of at least once a month be monitored for unauthorized access or unusual activities.
- Only ports required by application or database servers are to be opened and wherever possible restrict the access to designated authorized clients/servers only
- Disable default unused accounts in the operating system, database and application
- Apply multi-tier architecture for each application by using a demilitarized zone (DMZ) in order to separate the server accessed by public and backend server (i.e. database server)

3.6 Database server security

- Access by high-privileged to the database server must be logged and the logs must periodically of at least once a month be monitored for unauthorized access or unusual activities.
- Only ports required by database servers are to be opened and restrict the access to particular clients/servers within the campus only
- The database server's audit trail of at least critical unusual activities such as logon attempts, changes to user master records, unsuccessful transaction starts, and changes to the audit configuration, must be enabled. The audit log must regularly of at least once a month, be reviewed to timely detect unusual activities or events. The review must be carried out by a person independent from the operation and security functions. Appropriate follow up must be in case such unusual activities or events are detected.

4. Physical access:

- All information processing hardware, including printers, which contains, or can be used to access confidential information must be located in areas which are secured from access.
- Physical access to these areas, including the Data Center, must be restricted to authorized personnel. Request for such access must be submitted using appropriate

form and approved by the person in-charged for the area. The person in charge must ensure that the access must be immediately revoked as soon as such access is no longer required.

5. Workstation security:

Workstations used for sensitive or critical tasks in dealing with Information Systems must have adequate physical and electronic controls to provide continued confidentiality, integrity, and availability of data stored on the system:

- All workstations must have updated virus protection software installed and enabled as well as all critical patches of the Operating System.
- Users with workstations running Operating Systems with some sorts of "Lock Workstation" capability, must execute this function anytime they leave their immediate work area unless the workstation is running a password protected screen saver or is in a "locked-down" environment.
- All other workstations will employ similar security procedures.

6. Data Ownership:

Data is owned by the unit(s) having primary responsibility for creation and maintenance of the data content. Data custodian is the person of the owner's unit having administrative control of that record and has the responsibilities to:

- Maintain the information in the databases.
- Determine how the data may be used within existing policies.
- Authorize who may access the data.

7. Information Service Provider's responsibilities:

IT department acts as Information Service Provider, provide Information Services as required by the data owner. IT department is the administrator of the computer systems, servers, workstations and network required for providing such services. As Information Service Provider, IT department, provides services in accordance with the directions from the owner and is responsible for:

- Implementing owner's specified controls over the data.
- Providing a general security access system.
- Ensuring compliance of its users with security procedures.

8. User's Responsibilities:

The user is the person who has been granted explicit authorization to access the data by the owner. This authorization must be granted according to established procedures. The user must:

- Use the data only for purposes specified by the owner.
- Comply with security measures specified by the owner or custodian.
- Not disclose information in the data nor the access controls over the data unless specifically authorized in writing by the owner.

9. Application Development/Changes & Technical Support:

Application development & technical support are provided by IT department and following procedures are applied:

- IT department provides development and technical support to Information Systems used by the Institute. For Information Systems developed by IT department, IT department carries out analysis, design, development, documentation and user training. For Information Systems acquired from other vendors, IT department supports in implementation; maintenance and administration of hardware, network, Operating System, database and application software; solves IT related technical issues; as well as provides customization of input/output as required.
- IT department handles security authorization as defined and approved by the data owner.
- Appropriate analysis of security risks and access control must be made by IT department and data owners for all Information Technology services and systems developed by or acquired by the Institute.
- Any change of application's program or customization as well as development of in-house Information Systems is to be initiated by the owner with appropriate authority approvals, documented using standard forms and submitted to IT department as the Information System Service provider.
- Changes and development must be made in a test environment and confirmed with the requester for correctness and completeness. Staff used for development and testing/QA must be different than those used for deployment in the production environment. Upon agreeing on the work done by IT department, requester signs his/her acceptance with appropriate hierarchy approvals. Then IT department migrates the changes or new products from the test to the production environment. To ensure good control, program development and migration has to be performed by different IT staff.

10. Source code protection

- Source codes must be kept in a secured repository within the campus network.

- User accounts must be synchronized with the centralized corporate directory service or single sign-on system so that termination of an account in the central systems results in termination of the associated account in the source code repository
- Source code repositories must only allow access to users who have been explicitly approved and granted access
- Users must be given only the minimum source code access needed to perform the duties of their work and every activity must be logged
- Source code repositories must retain records of source code changes. The records must associate code changes with the user who committed the change and a timestamp.
- Backups of source code repositories shall be performed at least once a week. A sample of data must be restored from backups at least once a quarter to validate the backup's integrity and test the restore processes.

11. Backup, restore, disaster recovery and archiving.

11.1 Backup/Restore

11.1.1 Data backup

- Each application must have its own backup
- Full backup has to performed on each Tuesday followed by incremental backup on Wednesday-Saturday using different removable media or network/cloud folder/file for one week period (i.e. 5 removable media or 5 folders/files are required for one week) and label mentioning the application and the day where the backup is performed (i.e. ERP Monday, ERP Tuesday, etc. or SIS Monday, SIS Tuesday, etc.), however the backup sets cannot be reused for 2 weeks periods. The media or folder/file must be password protected, and data containing sensitive information must be encrypted.
- The backup media must be stored off-site in a secured (e.g. fire-, flood-proof) place and the backup network folder/file must be provided from an external reliable cloud service provider.
- Backup log must be immediately viewed. If there is any error, the backup process has to be repeated. If error still occurs, then system administrator has to be notified.

11.1.2 System backup

Full backup of the system parts (Operating system, database and applications software and setup) is to be carried out once a month.

11.1.3 Restore

Restore exercise from removable media has to be performed once in each 6 months. The restore process includes restore from the system and data backup. Correctness of the restore process must be immediately assessed.

11.2 Disaster Recovery (DR)

For disaster recovery (DR) purposes, such as the production system does not function, following actions will be taken:

- DR machine must have the Operating System, Database and application software installed and is placed in a location outside the Data Center or on cloud provided by an external reliable cloud provider.
- The DR machine will replace the production machine as temporary production platform. Restore data from the latest removable media daily backup. The DR machine will then assume its function as the production replacement machine, however, data entered on the same day need to be re-entered.
- Prepare immediately another temporary DR machine.
- Once the main production machine is ready again, rsync process from the production replacement to the main production machine need to be done on the evening/night of the same day so that the main production machine can be used on the next day, and then the temporary production machine will reassume its function as DR machine again and the temporary DR machine can be released.
- DR exercise need to be carried out at least once a year
- Roles and responsibilities:
  DR Manager: Responsible for development and success of the DR plan and operation as well as well as oversee the maintenance and execution of DR process.
  DR infrastructure team/person: Responsible for DR server machines as well as operating system, database and application software on the machines
  DR data team/person: Responsible for restoring data from the backup media to the DR machines and the rsync back from the DR machine to the restored production machine software

11.3 Archiving

Data archiving is required for seldom used or old data however those data cannot be deleted or purged for business or legal conformity reasons. Due limitation of on-line storage capacity, those data need to be put on off-line, but can still easily and quickly be made on-line, if required.

Removable media will be used for this purpose.

- Before removal any data from on-line storage, it must be archived on removal media. Each removal media contains archive of no longer than one year duration.
- The removable media must be labeled with the application, the word "Archive" and the archive year such as "ERP Archive 2003". In each removal media there must be index describing the content of the media specifying the type of the data and more specific duration period such as "AP November 2003" if the media cannot hold the full data as described on the label
- Duplicate media must be created for each archive media and label it as the original archive media but add the word "Copy" such as "ERP Archive 2003 Copy"
- The media must be password protected.
- Archive media cannot be reused unless it is no longer required in the business or legal procedures and its deletion is confirmed in writing by owner of the data.
- Both archive media and their duplicates must be kept off-site in a secured (e.g. fire-, floodproof) area

11.4 Media Library

Library of removable media serving all application servers need to be maintained which records:

- Media Identity No.
- Label
- Location on the shelf
- Other information as required

12. Review of the Policies & Procedure

These Policies & Procedures have to be reviewed by the IT department and all data owners at least once a year, and the review has to be documented,