

AMR Tech Park II A, First Floor,

Hosur Road, Next to Oxford Institutions,

Opp.BOSCH office, Bengaluru, Karnataka 560068

**IT – Policies**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Date** | **Version** | **Prepared By** | **Approved By** | **Description** | **Sections Revised** | **Pages Revised** |
| **12-07-2018** | **1.0** | **Shashank Jannu** |  |  |  |  |
|  |  |  |  |  |  |  |

**TABLE OF CONTENTS**

Contents

[OBJECTIVE 3](#_Toc388451972)

[SCOPE AND APPLICABILITY 3](#_Toc388451973)

[DEFINITIONS/ GLOSSARY 3](#_Toc388451974)

[POLICY STATEMENTS 3](#_Toc388451975)

# OBJECTIVE

The objective of this policy is to ensure safety and security of information systems

# SCOPE AND APPLICABILITY

This policy is applicable to IT department of the organization.

# DEFINITIONS/ GLOSSARY

|  |  |
| --- | --- |
| **Term/Abbreviation** | **Definition/Expansion** |
| Secured Areas | Work Floor, Server Room, Directors’ Cabin |
| Common areas | Cafeterias, conference rooms |
| Mobile devices | Laptop, Tabs, Smart Phones |
| Removable Media | CD, Pen Drive, External Hard Disk etc. |

# POLICY STATEMENTS

1. **IT HOUSEKEEPING POLICIES**

* **IT House Keeping Policies**

1. All operating procedures including those for Daily, weekly and monthly maintenance activities shall be documented and adhered to.
2. Duties and areas of responsibility shall be segregated wherever possible, in order to reduce opportunities for unauthorized modification or misuse of information or services.
3. All computer clocks will be synchronized at log on time using active directory services

* **Operating System Access Control Policies**

1. Access to information services shall use a secure log-on process using Microsoft active directory services.
2. All users shall have unique user id from active directory such that activities can be traced to responsible user.
3. The operating systems have following capabilities

* identifying and verifying the identity, and if necessary the terminal or location of each authorized user
* recording successful and failed system accesses
* ensuring quality passwords
* restricting the connection times of users, if necessary
* restricted Admin privileges to the users
* **Use of System Utilities**

1. The use of system utilities shall be restricted, require approval and be made available for limited period usage. There will be segregation from applications software.
2. All use of system utilities shall be logged. All unnecessary software based utilities and system software shall be removed

* **Safeguarding of Organizational Records**

1. Important documents of an organization shall be protected from loss, destruction, and falsification.
2. Consideration shall be given to the possibility of degradation of media used for storage of records.
3. All classified documentation shall be disposed appropriately.
4. **BACKUP POLICY**
5. Full backups of the server hard-disks , will be taken on weekely basis .
6. Firewall backup will be taken on daily and as and when changes are made to firewall policies.
7. Incremental backups will be scheduled every day except on the day the full backup is performed
8. Backups shall be stored at a secured storage location. Backup procedures shall be documented, scheduled, and monitored.
9. Backup procedures and retention periods shall be in accordance with the criteria approved by IT Head and project Manager
10. Backup shall be restored on once in 3 months to test integrity and readability of the information stored. A log of all storage and retrieval of backups shall be maintained.
11. Copies of essential documents, such as contracts shall be protected as well. All user activities for system maintenance, errors reported and solved shall be logged.
12. **ANTI-VIRUS POLICY**
13. IT Department shall ensure that all systems in the organization are protected against virus attacks. Appropriate recovering mechanism from virus attacks shall be established.
14. All computer-based information coming into or going out of organization’s network shall be scanned for virus.
15. Regular reviews shall be conducted of the software and data content of systems supporting critical business processes.
16. Necessary tools and procedures shall be in place for virus control.
17. This includes detection and prevention controls to protect against malicious codes.
18. Procedures shall be established to assist the user on the necessary actions if a malicious code has been detected or suspected.
19. Procedures shall be established to enable qualified employees to deal with such incidents.
20. All users shall be made aware of information security issues.
21. **INTELLECTUAL PROPERTY RIGHTS POLICIES**
22. Unauthorized software shall not be kept and installed in organization’s network.
23. IT Manager shall maintain a list of authorized software.
24. IT manager shall not approve any request to install unauthorized software.
25. Use of unauthorized software copies shall not be permitted under any circumstances.
26. All users shall comply with all licensing terms and conditions regulating the use of any software that is acquired. Software shall be obtained from legitimate source.
27. **PASSWORD MANAGEMENT POLICY**
28. **Password Management Policies**
29. The use of sign-on passwords shall be implemented.
30. New temporary passwords shall be provided only after positive identification of the user.
31. Temporary passwords shall be changed immediately. Passwords shall be distributed securely wherever feasible
32. Passwords shall be encrypted in storage wherever possible
33. Passwords shall be changed periodically according the sensitivity of systems accessed.
34. All users shall adopt strong passwords in selection and use of passwords.
35. Default vendor passwords shall be changed after installation of software wherever feasible
36. **The Password Management System Policies**
37. Shall enforce the use of individual passwords to maintain accountability
38. Shall allow users to select and change their own passwords
39. Shall enforce choice of quality passwords
40. Shall force users to change temporary passwords at the first log-on
41. Shall maintain a record of 3 previous user passwords, and prevent re-use
42. Shall not display passwords on the screen when being entered
43. Shall store passwords in encrypted form wherever feasible
44. In case of 3 unsuccessful attempts to log on, the user account will get locked out. In such a situation, the user should contact the IT manager to get the account unlocked and the password reset.
45. **The Password Management for Network and Servers**
46. Shall enforce the use of individual passwords to maintain accountability
47. Shall enforce choice of quality passwords
48. Shall maintain a record of 3 previous user passwords, and prevent re-use
49. Shall not display passwords on the screen when being entered
50. Shall store passwords in encrypted form wherever feasible
51. The password shall be changed every 45 days.
52. **LOGICAL ACCESS CONTROL POLICIES**
53. All users shall have their own User ID for the system they work with. All employees and third party vendors shall sign the confidentiality agreement before they are allowed to use organization’s information systems.
54. On behalf of System owners, IT Department shall maintain a formal record of all registered users and their access rights.
55. On behalf of System owners, IT Department shall conduct review at regular intervals to review user access rights or on a need basis.
56. Employees shall be uniquely identified on the systems and shall be held accountable for every action carried by his/her user id.
57. Approval shall be obtained from system owner and management, if need be, before providing access.
58. Approval from IT Manager is required for group/generic user IDs.
59. Ensure access granted is appropriate to business purpose and is consistent with organizational security policy.
60. Ensure service providers are not provided access until authorization procedures have been completed
61. Formal record of all persons registered to use the service should be maintained.
62. User IDs shall not indicate user’s privileges level
63. Suspended or inactive accounts should be escalated to respective Department heads if it is found being used during auditing of Information systems.
64. Sensitive Information system has a dedicated and/or protected computing environment
65. The allocation and use of privileges that enables users to override system or application controls shall be restricted and controlled.
66. The privileges associated with each system product, e.g. operating system, and the categories of staff to which they need to be allocated shall be identified.
67. Privileges shall be allocated to individuals on a need to use basis and on an event by event basis
68. **NETWORK MANAGEMENT POLICIES**

* **Internal Connectivity**

1. All network devices, such as Firewalls, Ethernet Switches, Ethernet Hubs, Leased line modems and others are to be managed and controlled by IT Department.
2. Network devices shall be configured to provide access control and auditing of external traffic information.
3. No network device shall be connected to the company network without prior approval of IT Department
4. Security shall be ensured by segregating networks to appropriate set of users, services and information systems (if required).

* **External Connectivity**

1. All access to Internet shall go through a Firewall. All connections to external hosts or networks shall be approved.
2. A security review shall be conducted to assess the adequacy of security measures for any connection with external hosts or networks.
3. Devices protecting the network shall be audited periodically.
4. Ensure that computer connections and information flows do not breach the access control policy of the business applications

* **Terminal Log on**

1. System or application identifiers shall not be displayed until the log-on process has been completed
2. A general notice warning that the computer only be accessed by authorized users can be displayed
3. No help messages should be provided during the log-on procedure.
4. If an error condition arises, the system should not indicate which part of the data is correct or incorrect
5. System log shall be maintained of unsuccessful attempts. Authorization will be required for reactivating the account after account gets locked.
6. Maximum and minimum time allowed for the log-on procedure should be limited
7. **IT ASSEST MANAGEMENT POLICIES**

* **System Planning and Acceptance**

1. Capacity demands shall be monitored and projections of future capacity requirements shall be made to ensure that adequate processing power, storage, and network bandwidth are available.
2. Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system shall be carried out prior to acceptance. Requirement and acceptance criteria for all new systems are clearly defined, agreed, documented, and tested. Training shall be provided in the operation or use of new systems.

* **Assets Procurement**

1. Any asset procurement shall have suitable management approval. Compatibility requirements shall be taken care of

* **Protection of Critical Information Assets – Server Room**

1. The servers and network switches shall be housed in a server room to protect against vandalism and theft.
2. A server room shall be equipped with fire protection and access control systems. Server room environmental condition shall be monitored.

* **Wiring Closet**

1. Communication equipment and cabling distribution points shall be housed within lockable cabinets or rooms, and are routinely checked. These areas are to be accessed by authorized personnel only.

* **IT Equipment Security**

1. All information assets shall be located or protected to reduce the risks from environmental threats and hazards, and from unauthorized access.
2. Employees shall ensure that unattended equipment is protected from unauthorized use.
3. Critical information assets shall be protected from power failures and other electrical anomalies.

* **Cabling Security**

1. Power and telecommunication lines into information processing facilities shall have adequate protection.
2. Network cabling shall be protected from unauthorized interception or damage.
3. Power cables shall be segregated from communications cables.

* **IT Equipment Maintenance**

1. Equipment shall be maintained in accordance with manufacturer’s instruction and/or documented procedures to ensure its continued availability and integrity.
2. Only authorized maintenance personnel shall carry out the repairs and service equipment
3. Records shall be kept of all suspected or actual faults & all preventive and corrective maintenance.
4. Adequate care shall be taken to reduce the risk of compromise of organization’s information systems during maintenance.

* **Security of off-site IT Equipment**

1. Authorization shall be required before allowing equipment to leave the premises.
2. This shall be logged out and logged back in when returned.
3. Manufacturer’s instructions for protecting equipment shall be observed at all times.

* **Inventory of IT Assets**

1. All assets (information, software, physical and services – computing, communication, utilities) shall be clearly identified, their ownership, security classification agreed, documented between system owner and Security Steering Committee, together with its current location.
2. IT Department staff shall maintain a register of all software licenses owned by the organization.

* **IT Asset Movement**

1. All organizational assets which are to be moved outside the physical security premises needs to be moved under controlled and protected conditions. Organization shall ensure that assets which contain sensitive information (E.g. computer hard disks, data cards, laptops and other mobile devices) are screened and sensitive information is retained with organization before moving the information asset.
2. Asset movement shall be tracked with a materials movement register with details of reason for asset movement, responsibility and ownership of assets. Security guard and IT Manager shall sign the material movements register on sending or receiving of asset confirming the asset movement.

* **IT Asset Disposal**

1. Any storage media shall be sanitized, to permanently remove any licensed software and information present, prior to disposal
2. **IT CHANGE CONTROL POLICIES**

* **IT Configuration Management**

1. The configuration of system infrastructure and software such as switches, servers, firewalls, server, application software and other devices shall be kept documented and validated.
2. Any changes to the configuration shall be reviewed and documented before they are applied.

* **IT Change Control**

1. Changes to information processing systems shall be controlled.
2. Production (operational) programs shall be subject to strict change control.
3. IT Department staff shall be responsible to maintain change control of systems and applications on behalf of the system owners.
4. Users shall not be allowed to install any software onto their computers. Any such requirement shall go through formal approval process. All software installations to be done by system administrator.
5. System owners shall be responsible for ensuring that the integrity of the systems, application software and documentation is maintained. This includes the functions of:

* Providing necessary user authorization for accessing the Information resources.
* Providing the first point of contact regarding configuration management problems.
* System owners and users shall be notified of all changes made to production system that may affect the processing of data.

1. It shall be ensured that change control does not disrupt regular business activities.
2. It shall be ensured operating procedure and user procedures are changed as necessary.
3. **MEDIA MANAGEMENT POLICIES**

* **Removable Media**

1. Employees are not authorized to bring any removable media to the organization.

* **Media Labelling**

1. Media shall be labeled according to the highest classification of the stored information.
2. All media labels shall include

* classification of the information present on the media
* Asset ID
* **Media Handling**

1. Management of removable computer media such as hard disks and printed reports shall be controlled.
2. Media shall be disposed of securely and safely when no longer required. All such transactions are logged.
3. The access list for system documentation shall be kept to a minimum.

* **Media in Transit**

1. Only reliable transport or couriers shall be used for transit of confidential information.
2. Packaging shall be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturer’s specifications.
3. Special controls shall be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification.
4. **MONITORING AND AUDIT**

* **Monitoring and Audit**

1. Audit logs will be retained to enable investigation to be carried out as and when necessary. The audit log to contain user id, date and time for log-on and log-offs, records of successful and unsuccessful access attempts, programs/utilities used to include all privileged operations.
2. All server logs will have a retention period of 2 years
3. Audit logs will be protected against unauthorized access and corruption.
4. Audit trail will be regularly monitored either automatically or manually.
5. Suspicious activities will be reported directly to SSC.
6. Access to system audit tools shall be restricted and protected to prevent misuse or compromise.
7. **BCP & DISASTER RECOVERY**

**Locations – All Locations (Bangalore )**

* + 1. All Location work independently without any dependencies with other locations, Location is configures with Primary and backup Internet Links.