INFORMATION TECHNOLOGY POLICY

BEST CAPITAL SERVICES LIMITED

Registered Office:

701, 7TH Floor, Luhadia Tower, Ashok Marg,
C-Scheme, Jaipur 302001.INDIA
CIN NO: U67120RJ1995PLC009942.

INFORMATION TECHNOLOGY POLICY

BEST CAPITAL SERVICES LIMITED (‘Company’) being an NBFC having asset size below 500 crores and is governed by directions contained in Section-B of the Master Direction RBI/ DNBS /2016-17/53- Master Direction-DNBS.PPD. No.04/ 66.15.001/2016- 17, Dated: June 08, 2017) issued by RBI. This IT Policy is finalized taking into account the said Directions. The entire IT system is being used in house by the Company, Management will be responsible to make sure that proper system procedures are in place as detailed in the policy.

IT Policy of the Company is a collection of various Policies and includes the following:

I. ACCESS CONTROL POLICY

1. Purpose

This policy defines the control requirements surrounding the management of access to information on Company’s computer and communications systems.

2. Scope

This policy applies to all Company’s computer systems and facilities, with a target audience of Company’s Information Technology employees and partners.

3. Policy

Access Control System

Access Control System – User ID Creation Date - Access control systems must be configured to capture and maintain the creation date for every user ID.

Access Control System – Last Logon Date - Access control systems must be configured to capture and maintain the date and time of the last logon for every user ID.

Access Control System – Last Logoff Date - Access control systems must be configured to capture and maintain the date and time of the last logoff for every user ID.

Access Control System – Password Change Date - Access control systems must be configured to capture and maintain the date and time of the last password change for every user ID.

Access Control System – User ID Expiration Date - Access control systems must be configured to capture and maintain an expiration date or every user ID that represents the last date that the user ID is active for use.

Malfunctioning Access Control - If a computer or network access control system is not functioning properly, it must default to denial of privileges to end-users.

Special Privileged Users - All multi-user computer and network systems must support a special type of user ID, which has broadly-defined system privileges that will enable authorized individuals to change the security state of systems.

Operating System User Authentication - Developers must not construct or install other mechanisms to identify or authenticate the identity of users without the advance permission of Company's management.

Access Control System Modification - The functionality of all access control systems must not be altered, overridden or bypassed via the introduction of additional code or instructions.

Password Generation Algorithms - All software and files containing formulas, algorithms, and other specifics used in the process of generating passwords or Personal Identification Numbers must be controlled with the most stringent security measures supported by the involved computer system.

Password Retrieval - Computer and communication systems must be designed, tested, and controlled so as to prevent both the retrieval of, and unauthorized use of stored passwords, whether the passwords appear in encrypted or unencrypted form.

Access Control Information In Cookies - Company's information systems must never store any access control information in cookies deposited on, or stored on, end-user computers.

System Capabilities And Commands - End users must be presented with only the system capabilities and commands that they have privileges to perform.

Authorization

Sensitive Or Valuable Information Access - Access to Company's sensitive information mustbe provided only after express management authorization has been obtained.

Granting Access To Organization Information - Access to Company's information must always be authorized by a designated owner of such information, and must be limited on a need-to-know basis to a reasonably restricted number of people.

Information System Privilege Usage - Every information system privilege that has not been specifically permitted by the Company's management must not be employed for any Company's business purpose until approved in writing.

Granting System Privileges - Computer and communication system privileges must be granted only by a clear chain of authority delegation.

User ID And Privilege Approval - Whenever user IDs, business application system privileges, or system privileges involve capabilities that go beyond those routinely granted to general users, they must be approved in advance by the user's immediate supervisor and Company's management.

Owner Approval for Privileges - Prior to being granted to users, business application system privileges must be approved by the applicable information owner.

System Access Request Authorization - All requests for additional privileges on Company's multi-user systems or networks must be submitted on a completed system access requestform that is authorized by the user's immediate manager.

Default User Privileges - Without specific written approval from management, administratorsmust not grant any privileges, beyond electronic mail and word processing, to any user.

Computer Access Training - All Company's users must complete an approved information security training class before they are granted access to any Company's computer systems.

Access and Privilege Assignment

Production Programs And Information Access - Access controls to production programs and information must be configured such that production programs and information systems software support personnel are not granted access privileges except for problem resolution.

Operations Personnel Information Access - Access controls to production programs and information must be such that computer operations personnel are restricted from modifying systems software, application software, and production information.

Privilege Restriction — Need To Know - The computer and communications system privileges of all users, systems, and programs must be restricted based on the need to know.

User IDs Employed In Abusive Activity - All access privileges for a user ID shown to be engaged in abusive or criminal activity must be immediately revoked.

Developer Access To Production Business Information - Where access to production business information is required so that new or modified business application systems may be developed or tested, only "read" and "copy" access must be granted on production machines. This access is permitted only for the duration of the testing and related development efforts, and must be promptly revoked upon the successful completion of these efforts.

Secret Information Access - Access to sensitive information must be granted only to specific individuals, not groups of individuals.

II. PASSWORD POLICY

1. INTRODUCTION

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of Company's entire network. As such, all employees are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

2. PURPOSE

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3. POLICY

3.1 General

• All application-level passwords (e.g. Passwords used to logging into .net applications and web module) must be changed at least every 45 days and cannot be used the past 5 password.
• All user-level passwords (e.g., email, desktop computer, etc.) must be changed at least every 45 days and cannot be reused the past 10 passwords.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• All user-level and application-level passwords must conform to the guidelines described below.

3.2 Guidelines

The Password Construction Requirements
i. Be a minimum length of eight (8) characters on all systems and maximum of twelve (12) characters.
ii. Not be a dictionary word or proper name.
iii. Not be the same as the User ID.
iv. Expire within a maximum of 45 calendar days.
v. Password must have at least one alphabet and one numeric character and one special character.
vi. Not be identical to the previous five (5) passwords.
vii. Not be displayed when entered.
viii. Ensure passwords are only reset for authorized user.
ix. Not be transmitted in the clear or plaintext outside the secure location.

3.3 Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. When a user quits (retires, resigned, suspended, dismissed, etc.), Default passwords shall be changed immediately on all equipment or the user id must be disabled immediately.

3.4 Password Protection Standards

Do not use your User ID as your password. Do not share passwords with anyone. All passwords are to be treated as sensitive and confidential information.
Here is a list of "do not's"
• Don't reveal a password over the phone to anyone
• Don't reveal a password in an mail message
• Don't reveal a password to the boss
• Don' talk about a password in front of others
• Don't hint at the format of a password (e.g., "my family name")
• Don't reveal a password on questionnaires or security forms
• Don't share a password with family members
• Don't reveal a password to a co-worker while on vacation
• Don't use the "Remember Password" feature of applications
• Don't write passwords down and store them anywhere in your office.
• Don't store passwords in a file on ANY computer system unencrypted.
If someone demands a password, refer them to this document or have them call COMPANY help desk.
If an account or password is suspected to have been compromised, report the incident to

COMPANY Helpdesk and change all passwords.

3.5 Application Development Standards

Application developers must ensure their programs contain the following security precautions:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Copy paste of user id and password should be disabled in application
- System should compel the user to change his password when he logs in for the first time.
- System should disable the user id, if wrong password is entered on three consecutive occasions.

3.6 Remote Access Users

Access to the COMPANY networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required).

3.7 Penalties

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

111. USER ACCESS POLICY

INTRODUCTION

This Policy describes how user is added and deleted from the system and how to the access to various menus and forms is controlled in the system.

PURPOSE

The main objective of this policy is to control the access to the system. The following policies and procedures are necessary to ensure the security and restrict the unauthorized access to the various module in the system.

ROLE DEFINITIONS

HR team

HR team refers to the employees in the HR department who will have access to HR Related activities like enroll an employee, Add Increment to an employee etc.

Super User

A highly privileged system user who can assign or remove roles to a particular user id .

POLICIES

User Addition/Creation

User addition is done by HR team through the HR module. When the joining process of an employee is completed in the system by the HR team, an employee code will be generated. Automatically a user id is created in the system with employee code as his user id.

User Deletion

User deletion is also directly linked with the HR module. When an employee is Resigned /terminated his user id will be automatically deleted from the system.

User Access Control

HR team can assign respective roles to the user id based on the designation of the employee. Base on the roles assigned by HR, a user will be able to view/access particular menus and forms.

1V. INFORMATION SECURITY

1.1 Policy Description

This is the collection of policies that implement the overall spirit of the management system. Policies are broad but topical in nature.
The Information Security Management System is

- Aligned to global standards for Information Security Management – ISO/IEC 27001:2013
- Adopt best practices for Information Security Management

There is adequate focus on ensuring adequate protection of information assets by

- Following efficient and effective processes
- Protecting customers' and organization's information

a) An effective Management System is established for Information Security

b) All policies are approved will be communicated to all Customers, vendors and other interested parties

c) Periodic reviews of this policy will be carried out to ensure its continued suitability and applicability.

d) Periodic reviews of the policy implementation will be conducted by internal or external auditors

e) Company adheres to their customer's policies, processes and other guidelines, if any, as required by and agreed with the customer

f) There is an effective mechanism to ensure continual improvement of Processes practiced

g) Senior management is fully committed to IT service management and information security

h) Threats and risks to information system assets are properly identified using effectively managed and structured Risk Management framework on periodic basis

i) All identified Security risks in information systems have been reduced to an acceptable level

j) Specific security standards which are sub sets of this policy are established by the Chief Information Security Officer

k) Information is protected against unauthorized access and malicious activities with required security infrastructure in place

l) Measures are taken to assure confidentiality, Integrity and availability of information

m) Build, maintain and review a competent and professional security organization to manage the implementation of, and compliance with, Information Security Policy, Standards and Procedures

n) Give top priority to security awareness and education in order to ensure that all personnel are fully aware of the security requirements and all relevant security measures

o) Compliance with Government Regulations, legislative and contractual requirements are ensured

p) All breaches of information security, actual or suspected, are reported to, and investigated by the Incident Management Process.

V. COSMOS RETURNS POLICY

Purpose

This policy summarizes the system driven COSMOS Return reports for RBI to ensure continued regulatory compliance.

Scope

The policy applies to Cosmos regulatory/supervisory returns of the Company.

Policy

The input data for preparing COSMOS return shall be generated automatically by incorporating various checks and validations prescribed in the utility file provided by the RBI. Required modifications shall also be made in the report as per the periodic changes introduced by the RBI.

Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to termination of employment. Any employee will also be liable and responsible for the pecuniary losses incurred to the Company in relation to the same.

VI. DATA BACK UP POLICY

The Policy Statement

The availability of the information shall be ensured as per the business requirements. To ensure the availability, backups of the data shall be performed as per agreed frequency and stored securely.

Appropriate backup procedures in place to ensure that all critical information is backed up periodically. The backup and restore procedures for each system is documented separately or per group of systems and reviewed periodically.

Access to the backed-up shall be restricted to the authorized users only.

The latest versions of the software, application software, and application configuration shall be backed up initially after the implementation and immediately after any changes.

It is the responsibility of the user to backup important business data stored in the desktop computer.

The information in the backup media must be examined regularly for recoverability to ensure that the media can be relied upon during emergencies. To verify the accessibility of backup media, mock restoration tests shall be carried out. The periodicity of the restoration tests shall be included in the associated backup procedure.

The backup shall be stored in a remote location, significantly away from the primary data center and business location. The backup location should have the same level of physical security and environmental controls as the main site. The offsite location of the backed-up data shall be documented in the associated procedure. Daily Oracle DB backup copied into the external Hard disk and submitted to the Management TFS backup copied into external HDD on every fortnight and submitted to the Management. Open source backup is copied into external HDD from bit bucket submit to the Management All backup will kept at distant location

Appropriate restore procedures must be in place and the restore procedures for each critical system shall be documented and tested according to the defined periodicity.

The data shall be archived when not in use and to meet legal and regulatory requirements. The legal and regulatory requirements shall be documented in the associated procedure.

VII. BUSINESS CONTINUITY POLICY

Purpose

The purpose of this policy is to create and maintain a Business Continuity Plan (BCP) for the IT support of critical Company processes. An effective plan allows the Company to minimize the adverse effect of emergencies that arise. The Company has an ethical obligation to the organization's workforce, shareholders, and customer stakeholders to protect the continuing operations of the business.

Scope

This policy encompasses all IT processes and technology that supports critical business functions.

Policy

Since the entire IT system is outsourced, management should make sure that the service provider is having proper Disaster Recovery mechanism of IT system and Business Continuity Plan.

VII. E- MAIL POLICY

1. Purpose

This policy provides the rules and requirements for the secure use and management of electronic mail.

2. Scope

This policy applies to all users of Company information assets including but not limited to Company employees, contractors and partners. This policy applies whether electronic mail is accessed from Company networks or via any remote location.

3. Policy

Email Privileges

Authorized Usage - Company electronic communications systems generally must be used for business activities only. Incidental personal use is permissible as long as it does not consume more than a trivial amount of system resources, does not interfere with worker productivity, and does not preempt any business activity. Company electronic communication systems must not be used for charitable fund raising campaigns, political advocacy efforts, religious efforts, private business activities, or personal amusement and entertainment. News feeds, electronic mail mailing lists, push data updates, and other mechanisms for receiving information over the Internet must be restricted to material that is clearly related to both Company business and the duties of the receiving workers. Workers are reminded that the use of corporate information system resources must never create the appearance or the reality of inappropriate use.

Default Privileges - Electronic communication systems must be established and maintained such that only the privileges necessary to perform a job are granted to a worker. For example, when a worker's relationship with Company comes to an end, all of the worker's privileges on Company electronic communications systems also must cease.

User Separation - Where electronic communications systems provide the ability to separate the activities of different users, these facilities must be implemented. For example, electronic mail systems must employ personal user IDs and secret passwords to isolate the communications of different users. Company employees must not employ the user ID or the identifier of any other user.

Use At Your Own Risk - Workers access the Internet with Company X facilities at their own risk. Company is not responsible for material viewed, downloaded, or received by users through the Internet. Electronic mail systems may deliver unsolicited messages that contain offensive content.

Message Ownership

Company's Property - As a productivity enhancement tool, Company encourages the business use of electronic communications systems, notably the Internet, telephone, pager, voice mail, electronic mail, and fax. Unless third parties have clearly noted copyrights or some other rights on the messages handled by these electronic communications systems, all messages generated on or handled by Company electronic communications systems are considered to be the property of Company.

No Guaranteed Message Privacy - Company cannot guarantee that electronic communications will be private. Workers must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Electronic communications can be accessed by people other than the intended recipients in accordance with this policy. Because messages can be stored in backups, electronic communications actually may be retrievable when a traditional paper letter would have been discarded or destroyed. Workers must accordingly be careful about the topics covered in Company electronic communications.

Incidental Disclosure - It may be necessary for technical support personnel to review the content of an individual worker's communications during the course of problem resolution. These staff members must not review the content of an individual worker's communications out of personal curiosity or at the request of individuals who have not gone through proper approval channels. Advance approval by the Information Security Manager is required for all such monitoring.

Passwords

Sharing Passwords - Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. Information Technology Department staff must never ask users to reveal their passwords. If users need to share computer resident data, they should utilize message forwarding facilities, public directories on local area network servers, groupware databases, and other authorized information-sharing mechanisms.

Strong Passwords - To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess.