

PILANI INVESTMENT AND INDUSTRIES CORPORATION LIMITED

Information Technology Policy



1. Intent:

Increased protection of information and Information Technology Resources to assure the usability and availability of those resources to all users of Pilani Investment and Industries Corporation Limited is the primary intent of this Policy. The Policy also addresses privacy and usage guidelines for those who access Pilani Investment and Industries Corporation Limited Information Technology Resources.

2. Purpose:

Pilani Investment and Industries Corporation Limited recognizes the vital role information technology plays in effecting Company business as well as the importance of protecting information in all forms. As more information is being used and shared in digital format by Pilani Investment and Industries Corporation Limited authorized users, the need for an increased effort to protect the information and the technology resources that support it, is felt by Pilani Investment and Industries Corporation Limited and hence this policy.

Since a limited amount of personal use of these facilities is permitted by Pilani Investment and Industries Corporation Limited to its users, including computers, printers, e-mail and Internet access, therefore, it is essential that these Facilities are used responsibly by users, as any abuse has the potential to disrupt company business and interfere with the work and/or rights of other users. It is therefore expected of all users to exercise responsible and ethical behavior while using Pilani Investment and Industries Corporation Limited Information Technology facilities.

3. Reference:

In this Policy, a reference to the following word(s) shall have the following meanings assigned to it.

3.1 Information Technology Resources :

Information Technology Resources for purposes of this Policy include, but are not limited to the Company owned or those used under license or contract or those devices not owned by the Company but intentionally connected to Pilani Investment and Industries Corporation Limited - owned Information Technology Resources such as Computer hardware, printers, fax machines, voice-mail, software, e-mail and internet access.

3.2 User:

Anyone who has access to Pilani Investment and Industries Corporation Limited Information Technology Resources, including but not Limited to, all employees, temporary employees and probationers.

3.3 Policy:

This Policy includes within its purview the following referred Policies

→ The General Information Technology Usage Policy

1

- The Internet and Intranet Usage Policy
- The E-mail Usage Policy
- The Helpdesk Process
- The Business Continuity Planning and Disaster Recovery

4 Policy:

The use of the Pilani Investment and Industries Corporation limited information technology resources in connection with Pilani Investment and Industries Corporation Limited business use and limited personal use is a privilege but not a right, extended to various users. The privilege carries with it the responsibility of using the users of Pilani Investment and Industries Corporation Limited Information Technology resources efficiently and responsibly.

By accessing Pilani Investment and Industries Corporation Limited Information Technology Resources, the user *agrees* to comply with this Policy.

Users also agree to comply with the applicable laws and all governing contracts and licenses and to refrain from engaging in any activity that would subject Pilani Investment and Industries Corporation Limited to any liability. The Company reserves the right to amend these policies and practices at any time without prior notice.

Any action that may expose the Company to risks of unauthorized access to data, disclosure of information legal liability, or other potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

5. Scope

This policy applies to everyone who is in India has access to Pilani Investment and Industries Corporation Limited Information Technology Resources and it shall be the responsibility of all employees to ensure that this policy is clearly communicated understood and followed by the users.

This Policy also applies to all contracted staff and vendors /suppliers, if any, providing services to Pilani Investment and Industries Corporation Limited that bring them into contract with Pilani Investment and Industries Corporation Limited Information Technology resources.

The employees who contracts for these services shall be Responsible to provide the contractor /vendor /supplier with a copy of this Policy before any access is given to them.

These policies cover the usage of all of the Company's Information Technology and communication resources, whether they are owned or leased by the company or are under the company's possession, custody, or control, including but not limited to:

- All computer-related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, wireless computing devices, telecomm equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected.

- All electronic communications equipment, including telephones, radio communicators, voice mail, e-mail, fax machines, wired or wireless communications devices and services, Internet and other on-line services.
- All software including purchased or licensed business software applications, Pilani Investment and Industries Corporation Limited - written applications, employee or vendor/supplier-written applications, computer operating applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on Pilani Investment and Industries Corporation Limited - owned equipment.
- All intellectual property and other data stored on Pilani Investment and Industries Corporation Limited Information Technology equipment.
- These policies also apply to all users, whether on Company property or otherwise, connected from remote connections via any networked connection, or using Company equipment.

6. General standards for acceptable use of Pilani Investment and Industries Corporation Limited's Information Technology resources require:

- Responsible behavior with respect to the electronic information environment at all times.
- Compliance with all applicable laws, regulations and Pilani Investment and Industries Corporation Limited policies
- Respect for the rights and property of others including intellectual property rights
- Behavior consistent with the privacy and integrity of electronic networks, electronic data and information and electronic infrastructure and systems.

7. General Information Technology Usage Policy

7.1 Passwords

- Individual password security is the responsibility of each user.
- Passwords are an essential component of Pilani Investment and Industries Corporation Limited computer and network security systems. To ensure that these systems perform effectively, the users must choose passwords that are difficult to guess. This means that passwords must not be related to your job or personal life. This also means passwords should not be a single word found in the dictionary or some other part of speech.
- To make guessing more difficult, passwords should also be at least Seven characters long. To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change passwords every 30 days. Password history would be maintained for previous three passwords. This applies to the Systems Logon (windows password) and Cloud Mail passwords.
- Passwords must not be stored readable form in batch files, automatic log-in scripts, software macros, terminal function keys, m computers without access control systems, or other locations where unauthorized persons might discover them. Passwords must not be written down and left in a place where unauthorized persons might discover them.

Immediately upon assignment of the initial password and in all cases of password "reset" situations, the password must be immediately changed by the user to ensure confidentiality of all information.

- Under no circumstances, Users shall use another user's account or password without proper authorization.
- Under no circumstances, the user must share his/her password(s) with other user(s), unless the said user has obtained from the authorized official the necessary approval in this regard.
In cases where the password(s) is/are shared in accordance with the above, the user shall be responsible for changing the said password(s) immediately upon the completion of the task for which the password(s) was shared.
- In cases where no prior approval had been obtained for sharing of password(s) with other user(s), such user shall be completely responsible for all consequences that shall follow in respect of breach of this Policy and the Company shall initiate appropriate disciplinary proceedings against the said user.

7.2 Access Control

- All the Company computers that are either permanently or temporarily connected to the internal Computer networks must have a password-based control system. Regardless of the network connections, all computers handling confidential information must also employ appropriate password-based access control systems.
- All in-bound connections to the Company computers from external networks must be protected with an approved password.
Modems may only be used at the Company after receiving the written approval of the Management and must be turned off when not in use.
- All access control systems must utilize user-IDs, passwords and privilege restrictions unique to each user. Users are prohibited from logging into any Company's computer system anonymously. To prevent unauthorized access all default passwords, if any, must be changed before the Company use.
- Access to the server room, if any, is restricted and only recognized staff or someone with due authorization from the Management is permitted to enter the room.
- Users shall not make copies of system configuration files (e.g. Passwords, etc) for their own, unauthorized personal use or to provide to other users for unauthorized uses.

7.3. Managing System Privileges

- Requests for new user IDs and changes in privileges must be made to the designated authority in Mail. Users must clearly state why the changes in privileges are necessary.

The Company management reserves the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal and proper operation of the Company information Systems , which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others will not be permitted.

7.4 Changes to Systems

- No user must physically connect or disconnect any equipment, including the Company owned computers and printers, to or from any Company's network.
- With the exception of emergency situations, all changes to the Company information technology systems and networks must be documented, and approved in advance by the concerned Management..
- Only persons who have been authorized by the Management can make emergency changes to any Company's computer system or network.

7.5 Security (Access Control)

- There is maker-checker concept to reduce the risk of error and misuse and to ensure reliability of data/information.
- Users are forbidden from circumventing security measures.
- Users are strictly prohibited from establishing dial-up connections, using modems or other such apparatus, from within any Pilani Investment and Industries Corporation Limited premises.
- Users who have been given mobile/portable laptop / palmtop or any other device and duly authorized for such remote access, which connects to Pilani Investment and Industries Corporation Limited mail system on a real-time basis can do so through Internet.
- Unless the prior approval has been obtained, users shall not establish Internet or other network connections that could allow non-authorized users to gain access to the Company's Computer systems and Information. These connections include establishment of multi- computer file systems, Internet web pages & FTP servers.
- Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the Management. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, software copying, computer configuration changing or similar unauthorized attempts to compromise security measures will be considered serious violations of the Company policy. Likewise, short-cuts bypassing system security measures is absolutely prohibited.

8. Software Licensing Policy

- For all software including purchased or licensed business software applications, the Company - written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on the Company - owned equipment, all users must comply with the software licensing policy.

They must not use/install/download any software for their individual use or even for business Purpose without prior approval of the Management at Corporate office. In case any such software is found on any Company system which is not attached to the Individual user, it shall be the responsibility of the user to inform the same to the IT department, in case the same is not installed by the said user otherwise the Company shall initiate appropriate disciplinary proceedings against the said user.
- All necessary software's are pre-installed on all the Company systems for day to-day office needs . Request for any additional needs to be addressed to the Management for approval.
- Use of the Company network resource to illegally distribute or duplicate unauthorized copyrighted or licensed materials prohibited. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

9. Internet Usage Policy

- Internet software may only be installed / used by or with the approval of the the Management. Software patches or updates may only be downloaded, subject to approval and ensuring Strict adherence to the vendor's security and usage guidelines.
- Access to the internet and its resources is provided for the purposes of conducting business on behalf of the Company, filing of various returns to statutory authorities governing the Company such as MCA , RBI (COSMOS Returns), SEBI, Stock Exchange(s)etc .
Reasonable personal use of the Internet is permitted.
- The management reserves the right to block access to any Internet resource without any prior notice, *in* case anyone required access to restricted site, the same may be dealt as special *case* provided the same is identified as use strictly for official purpose and conducting the Company's business.
- Similarly, to protect Pilani Investment and Industries Corporation Limited IT systems from imported viruses, downloading or exchanging screensaver games ,entertainment software or other inappropriate files(for example video or audio materials for personal use),playing games against opponents or gambling over the internet is not permitted.
- Furthermore, users may not conduct any form of "hacking" or use malicious code to penetrate or attempt to penetrate other computers or to deliberately release viruses or other harmful programs within either the Company network or the internet or bypass security features.

10. Email Usage Policy

- All authorized users of the Company are provided with an E-mail account, which is either individual to the specific user or generic Email ID and the same is protected with a password which is provided to the individual user. The use of E-mail should be restricted only for the business purpose; however personal mail can also be exchanged to a limited quantum provided that such exchange does not amount to breach of this IT policy or otherwise materially affects Pilani Investment and Industries Corporation Limited operations. In case any individual is found using e- mail service, which is objectionable by any means, the access can be terminated by the management without any prior information however the same may be re- instated with the approval from the Director / Chief Executive Officer of the Company.
- Email users should be aware that exchange of information with external sites may not be Secured with high risks of spam, Trojans ,malicious codes etc. Hence exchange of information should be limited to reliable sites. Users are prohibited to use their names/e-mail ids/mail domain in public domain without prior authorization from the management.
- Information must not be transmitted internally or externally which is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory; pornographic or obscene, defamatory or any other material which is otherwise abusive or contains illegal content prohibited by law or regulation of the country or which brings the organization into disrepute. Information is understood to include text, images and is understood to include printing information and sending information via email.
- All material contained on the email system belongs to the Company and users should consider messages produced/received by them on the Company account to be secure. The confidentiality of email data should be maintained by the individual user.
- Security regarding access to the email system is of paramount importance. User identities and personal passwords must not be shared with others. Users should be cautious of providing their email addresses to external parties, especially mailing lists.
- Users transferring or receiving files or attachments from external sources should note that The Company system automatically checks downloaded material for viruses. However, in the event that a virus is suspected. the file or attachment must not be opened and the matter must be reported to the Management immediately for inspection and action.
- The Company email users are required to use this communication tool in a responsible fashion and to observe the related guidelines. The Company provides the email system for the purposes of conducting official business and it may not be used for personal gain or business activities unrelated to Pilani Investment and Industries Corporation Limited operations. Users must not use the system to promote an external cause without prior permission from the management.

- Where it is considered that there has been a breach in the use of the email system, the service of the user will be terminated without any prior information.

11. Information System Audit

The Audit Committee ensures that an Information System Audit of the Internal System and processes is conducted at least once in two years to assess operational risk faced by Pilani Investment and Industries Corporation Limited.

12. Helpdesk Process

All the queries, support pertaining to the system/user/network/back-end shall be made to the Registered Office at Kolkata at email id - pilaniinvestment1@gmail.com

13. Data Backup

In order to prevent loss of information by destruction of the magnetic means in which it is stored, a periodic backup procedure is carried out. Company takes daily backup in Data Server, PC & a Removable Hard Disk.
