Information Security Policy

(Natures Basket Ltd)

Intent:

Increased protection of information and Information Technology Resources to assure the usability and availability of those resources to all users of Natures Basket Ltd. (NB) is the primary intent of this Policy. The Policy also addresses privacy and usage guidelines for those who access Natures Basket Ltd.'s Information Technology Resources.

Policy:

By accessing Natures Basket Ltd.'s 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 Natures Basket Ltd. to any liability. Natures Basket Ltd. reserves the right to amend these policies and practices at any time without prior notice.

Any action that may expose Natures Basket Ltd. 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.

Scope

This policy applies to everyone who, in India, has access to Natures Basket Ltd.'s Information Technology Resources and it shall be the responsibility of IT corporate office to ensure that this policy is clearly communicated, understood and followed by all users.

This Policy also applies to all contracted staff and vendors/suppliers providing services to Natures Basket Ltd. that bring them into contact with Natures Basket Ltd.'s Information Technology resources. The HR / Admin department and the respective Branch Managers 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:

1. All electronic communications equipment, including telephones, pagers, radio communicators, voice-mail, e-mail, fax machines, PDAs, wired or wireless communications devices and services, Internet and intranet and other on-line services.
2. All software including purchased or licensed business software applications, Natures Basket Ltd. -written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on Natures Basket Ltd. -owned equipment.
3. All intellectual property and other data stored on Natures Basket Ltd.'s Information Technology equipment.
4. 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.

General Information Technology Usage Policy

Passwords

Individual password security is the responsibility of each user.
Passwords are an essential component of Natures Basket's 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 90 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 in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control systems, or in 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.
1. Under no circumstances, Users shall use another user's account or password without proper authorization.
2. Under no circumstances, the user must share his/her password(s) with other user(s), unless the said user has obtained from the concerned IT Head 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.
3.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 Natures Basket Ltd. shall initiate appropriate disciplinary proceedings against the said user.

Access Control

1. All Natures Basket Ltd. computers that are either permanently or temporarily connected to the internal computer networks must have a password-based access control system. Regardless of the network connections, all computers handling confidential information must also employ appropriate password-based access control systems.
2. All in-bound connections to Natures Basket Ltd. computers from external networks must be protected with an approved password or ID access control system. Modems may only be used at Natures Basket Ltd. after receiving the written approval of the IT Head and must be turned off when not in use.
3. All access control systems must utilize user-IDs, passwords and privilege restrictions unique to each user. Users are prohibited from logging into any Natures Basket Ltd. system anonymously. To prevent unauthorized access all vendor-supplied default passwords must be changed before Natures Basket Ltd.'s use.
4. Access to the server room is restricted with RFID lock and only recognized IT staff or someone with due authorization from IT Head is permitted to enter the room.

5. 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.

Managing System Privileges

Requests for new user-IDs and changes in privileges must be made to the IT Department in Mail. Users must clearly state why the changes in privileges are necessary.
In response to feedback from the Human Resources Department, the IT department will revoke any privileges no longer needed by users. After receiving information from HR / Admin department all system access privileges will be terminated within 24 hours when a user leaves Natures Basket Ltd. Natures Basket Ltd. 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 Natures Basket Ltd. 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.

Changes to Systems

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

Security (Access Control)

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 Natures Basket Ltd.'s premises.
Users who have been given mobile/portable laptop / palmtop or any other device and duly authorized for such remote access, which connects to Natures Basket Ltd.'s mail system on a realtime
basis, can do so through the Internet.
Unless the prior approval of the IT Head has been obtained, users shall not establish Internet or other external network connections that could allow non-authorized users to gain access to Natures Basket Ltd. systems and information. These connections include the establishment of multicomputer 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 IT Head. 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 Natures Basket Ltd. policy. Likewise, short-cuts bypassing system security measures is absolutely prohibited.

Software Licensing Policy

For all software including purchased or licensed business software applications, Natures Basket Ltd. -written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on Natures Basket Ltd. -owned equipment, all users must comply with the software licensing policy and must not use/install/download any software for their individual use or even for business purpose without prior approval of the IT Head at corporate office. In case any such software is found on any Natures Basket Ltd. system which is

not allocated to the individual user, it shall be the responsibility of the user to inform the same to the IT department, in cases the same is not installed by the said user otherwise Natures Basket Ltd.

shall initiate appropriate disciplinary proceedings against the said user.
All necessary software's are pre-installed on all Natures Basket Ltd. systems for day-to-day office needs. Request for any additional needs to be addressed to the IT Head for approval.
Use of Natures Basket Ltd. network resources to illegally distribute or duplicate unauthorized copyrighted or licensed material is prohibited. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

Internet and Intranet Usage Policy

Internet software may only be installed / used by or with the approval of the IT Head. 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 Natures Basket Ltd. Reasonable personal use of the Internet is permitted, according to constraints and conditions set out by the Firewall. The IT department 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 Natures Basket Ltd. business. The approval for the same needs to be obtained by the Department Head / from the IT Head.
Similarly, to protect Natures Basket Ltd.'s IT systems from imported viruses, downloading or exchanging screensavers, 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 Natures Basket Ltd. network or the internet or bypass security features.

Email Usage Policy

All authorized users of Natures Basket Ltd. 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 Natures Basket Ltd.'s operations. In case any individual is found using e-mail service, which is objectionable by any means, the access can be terminated by IT department without any prior information, however the same may be re-instated with the approval from the Managing Director and IT Head at the corporate office.
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 IT Head.
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 Natures Basket Ltd. and users should consider messages produced/received by them on Natures Basket Ltd. 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 Natures Basket Ltd. 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 IT Department immediately for inspection and action.
Natures Basket Ltd. email users are required to use this communication tool in a responsible fashion and to observe the related guidelines. Natures Basket Ltd. 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 Natures Basket Ltd.'s operations. Users must not use the system to promote an external cause without prior permission from the IT Head.
Reasonable personal use of the email system is permitted. Personal use of the e-mail service must not interfere with Natures Basket Ltd.'s operations, involve cost implications for Natures Basket Ltd. or take precedence over the user's job accountabilities.
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.

Helpdesk Process

All locations where Natures Basket Ltd. operates whether by itself or through its sub-agencies all help and support pertaining to the system/user/network/back-end shall be provided by the IT executives (only for Mumbai) or where the local IT Executives are not available, by the service centre IT helpdesk.
In case any user finds any problem with the IT systems or need any help, they can send in their request to IT Executives at corporate office via e-mail to nbit.support@godrejnb.com In the event of emergencies IT Executive can be contacted via telephone 022 25195215 however all phone calls must be followed by an e-mail later.

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. The responsibility for backing up the information located in shared access servers is the network administrators. It must be borne in mind that not only are hard disks inclined to fail, but also magnetic tapes are quite prone to errors that destroy their contents, so we need to do the restoration testing time to time basis.
General Rule: As daily Full backup is happening for all critical business applications.
Data Backup in File Servers: The Systems Management backs up all the information in the file servers through an automated procedure.
Data Backup in Database Servers: The Systems Management backs up all the information in the databases through an automated procedure.
Data Backup in Desktop PC and Notebook: This task is the responsibility of the user to whom the computer has been assigned.