HERITAGE FOODS LIMITED

Cyber Security Policy

HERITAGE FOODS LIMITED
CIN: L15209TG1992PLC014332
AN ISO: 22000 CERITIFIED COMPANY
Regd Off: H.No.8-2-293/82/A/1286,
Plot No: 1286, Road No. 1 & 65, Jubilee Hills,
Hyderabad, Telangana, 500033
Tel: +91-4023391221/222, Fax: 30685458
Email: hfl@heritagefoods.in
Website: www.heritagefoods.in

CYBER SECURITY POLICY

1. INTRODUCTION

Cyberspace is a complex environment consisting of interactions between people, software, and services, supported by worldwide distribution of Information and Communication Technology (ICT) devices and networks. In the light of the growth of Information technology (herein after called IT) in the sphere of business, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities. The protection of information infrastructure and preservation of confidentiality, integrity and availability of information in cyberspace is the need of the hour.

This Policy shall be called "**Cyber Security Policy**" of Heritage Foods Limited (herein after called 'the Company'). The intent of this policy is to ensure proper access to and usage of IT resources and prevent their misuse by the users.

The purpose of the policy is to protect information and information infrastructure from cyber incidents through a combination of processes, guidelines, technology and cooperation. This policy governs the usage of IT Resources from an end user's perspective.

This Policy defines what we want to protect and what we expect of our system users. It describes user responsibilities, such as protecting confidential information and creating nontrivial passwords and describes how we will monitor the effectiveness of our security measures.

2. SCOPE AND APPLICABILITY:

This policy applies to the Company including its Subsidiaries, Associate and Joint Venture Companies. The company also expects independent contractors, and all involved in the value chain to uphold the principles of this Policy and urges them to adopt similar policies within their own businesses. It is mandatory for all users to adhere to the provisions of this policy.

3. OBJECTIVE

- The Company will protect all its stakeholders' interests by ensuring confidentiality, Integrity and continuous availability of information and information systems under its control which includes, but is not limited to electronic, print information etc., on servers, workstations, laptops, networking and communication devices and information printed or written on paper or transmitted by any medium.
- The Company is committed to comply with all legal, regulatory, and contractual security obligations as may be applicable in cyberspace.

- The Company shall protect all Information from unauthorized access, use, disclosure, modification, disposal, or impairment whether intentional or unintentional, through appropriate technical and organizational security measures.

- The Company is committed to provide a virus free network and all Information processing systems will be auto updated with latest security patches from the manufacturer and loaded with an approved antivirus system.

- Only authorized and licensed software will be allowed to be installed on corporate systems.

- Company network will be always protected from the Internet through a firewall.

- All third-party partners dealing with the Company who use IT information assets will be asked to sign a non-Disclosure agreement (NDA).

- All changes in the information processing system will be managed through the change control process.

4. GUIDELINES

i. Confidentiality:
The assurance that sensitive information remains private and is not visible to an eavesdropper. Confidentiality is critical to total data security. Encrypting data by using digital certificates and Secure Socket Layer (SSL) or virtual private network (VPN) connection helps ensure confidentiality when transmitting data across untrusted networks.

ii. Authentication of Access:
All devices on the network of the Company should not be accessible without proper authentication. Authentication for access to the Company's computer networks shall be obtained after following the due process and procedure as prescribed by the IT team.

iii. Authorization:
Authorization implies assurance that the person/computer at the other end of the session has permission to carry out the access authentication request.

iv. Integrity:
Integrity would imply the assurance that the arriving information is the same as what was sent out. Understanding integrity requires to understand the concepts of data integrity and system integrity.

- Data integrity: Data is protected from unauthorized changes or tampering. Data integrity defends against the security risk of manipulation, in which someone intercepts and changes information to which he or she is not authorized. In addition to protecting data that is stored within our network, we might need additional security to ensure data integrity when data enters our system from untrusted sources. When data that enters our system comes from a public network, we need security methods so that we can perform the following tasks: –

- Ensure that the transmission has not been altered (data integrity).
- Prove that the transmission occurred (nonrepudiation). In the future, you might need the electronic equivalent of registered or certified mail.

- System integrity: Our system provides consistent and expected results with expected performance. For the OS operating system, system integrity is the most commonly overlooked component of security because it is a fundamental part of OS architecture.

- IT Department reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of the system.

v. Use of IT Devices:

IT devices (Desktops, Laptops, Printers, Scanners, Standalone PCs and other electronic devices connected to our network) issued by the Company to a user should be primarily used for official purposes and in a lawful and ethical manner.

vi. E-mail Access from the Company's Network:

- E-mail service authorized by the Company should only be used for official correspondence.
- All incoming e-mails are scanned for spam and virus infection.

vii. Filtering and blocking of sites:

- IT Department may block content over the Internet which is in contravention of this policy and other applicable laws of the land in force which may pose a security threat to the network.

- IT Department may also block content which, in the opinion of the organization concerned, is inappropriate or may adversely affect the network security and productivity of the users/organization.

viii. Password Policy:

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

ix. Backup Policy for Servers:

The purpose of this policy is to provide consistent rules for backup management to ensure backups are available when needed.

5. COMPLIANCE & RESPONSIBILITY

- It is the responsibility of all employees to adhere to the policy and the management has all rights to take disciplinary action in case of its violation.
- All employees of the Company are necessarily to be aware of the Information Security Policy of the organization.
- Employees while operating from remote/outside Company network should strictly connect via VPN for accessing Applications and Corporate Network.
- All employees should implement appropriate controls to ensure compliance with this policy by their users.
- IT Department will ensure resolution of all incidents related to the security aspects of this policy by their users.
- The IT Department should ensure that training and awareness programs on use of IT resources are organized at regular intervals.
- IT Department may use newsletters, banners, bulletin boards, corporate websites and Intranet etc. to increase awareness about this policy amongst their users.

6. Monitoring and Review:

The Company shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy. The Company, for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on devices under intimation to the user. This includes items such as files, e-mails, and Internet history etc. Monitoring and reviewing this policy is governed by IT department.

Any security incidents, security weaknesses and infringement of the policy actual or suspected, are reported, investigated by the designated team and appropriate corrective and preventive action shall be initiated.

The Executive Director, in consultation with the IT- Head is authorized to make modifications to this policy as and when deemed necessary and appropriate to ensure the effective use of the Policy.

The Company assures through this policy that any Cyber Security Matters resulting from or caused by the Company’s business activities shall be appropriately and adequately remedied in a time-bound manner.

--0--