Information Technology Security Policy

Objectives

The objectives of Norex Flavours Pvt. Ltd. Information Security Policy are to preserve:

Confidentiality - Access to Data shall be confined to those with appropriate authority.

Integrity – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.

Availability - Information shall be available and delivered to the right person, at the time when it is needed.

Policy aims

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Norex Flavours Pvt. Ltd. by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day-to-day business.
- Protecting information assets under the control of the organisation.

Scope

This policy applies to all information, information systems, networks, applications, locations, and users of Norex Flavours Pvt. Ltd.

Responsibilities for Information Security

- Ultimate responsibility for information security rests with the Admins Head of Norex Flavours Pvt. Ltd., but on a day-to-day basis the IT Officer shall be responsible for managing and implementing the policy and related procedures.
- Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of: -

Information Technology Security Policy

- The information security policies applicable in their work areas.
- Their personal responsibilities for information security
- How to access advice on information security matters

  - ❖ All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.
  - ❖ The Information Security Policy shall be maintained, reviewed and updated by the IT Officer.
  - ❖ Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.
  - ❖ Each member of staff shall be responsible for the operational security of the information systems they use.
  - ❖ Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
  - ❖ Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

Policy Framework

Management of Security

- At board level, responsibility for Information Security shall reside with the MD.
- The Norex flavours 's IT officer shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

Information Technology Security Policy

Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

Security Control of Assets
Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

Access Controls Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

User Access Controls
Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

Computer Access Control
Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

Application Access Control
Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

Equipment Security
In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

Computer and Network Procedures
Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Head QA/MD.

Vaibhav Agrawal

Managing Director

Information Technology Security Policy

Work Instructions & Control Measures for Stakeholder's Data Confidentiality

Security Measure	Associated Security Mechanisms
Access Control	Biometrics, Certificates, Multilevel security, Passwords, Reference monitor, Registration of User, Periodic Password Changed, User Permission & VPN
Security Policy	Administrative privileges, Malware detection, Multilevel security, Secure channel, Security sessions, Single Access Point, User Permissions, VPN
Non-Repudiation	Administrative privileges, Logging and auditing.
Physical Protection	Access Card, Alarms, Equipment tagging, Locks, offsite storage, Secured rooms, Security personnel.
System Recovery	Backup & Restoration, Configuration management, Connection services agreement, Disaster recovery, Redundancy.
Attack Detection	Administrative Privileges, Incident response, Intrusion detection system, Logging, Malware Detection, Data Breaches Detection.
Boundary Protection	Firewalls, Proxies, Single Access Point, VPN.

Norex, shares the control measures for stakeholder's data confidentiality mechanism to the respective stakeholders for their awareness on the listed mechanism is adopted and implement to secrecy of secure data.