Neon Vinimay Private Limited

DATA LEAKAGE POLICY

Circular: - Ref. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

Policy created by	**Designated Officer**
Policy reviewed by	**Technology Commitee**
Policy reviewed on	**31/12/2023**
Policy Approved by	**Board of Directors**
Policy approved on	**04/01/2023**

Version – 1.0

Purpose

This policy is a guide in identifying and gaining an understanding of the components that make up the information security system to manage risk to systems, assets, data, and capabilities.

Scope

Data Leakage Policy (DLP) is a set of technologies and business policies to make sure end-users do not send sensitive or confidential data outside the organization without proper authorization. DLP enforces remediation with alerts, encryption, and other protective actions to prevent end users from accidentally or maliciously sharing data that could put the organization at risk. Sensitive information might include financial records, client data, credit card / debit card data, or other protected information. The most common method that this data is leaked is via email.

Policy

Data Leakage Policy (DLP) features and products enable your organization to locate, monitor and protect your sensitive content from loss or misuse. Through policy enforcement, the organization will be complying by minimizing risk and preventing unauthorized use of confidential information.

Data Leakage Policy (DLP) encompasses the processes and rules used to detect and prevent the unauthorized transmission or disclosure of confidential information. The purpose of this procedure is to establish a framework of controls for classifying and handling the organization's data based on the data's level of sensitivity, storage location, value, etc. Confidential data can reside on or in a variety of mediums (pictures, paper documents, shred bins, physical servers, virtual servers, databases, file servers, personal computers, point-of-sale devices, USB drives and mobile devices) and can move through a variety of methods (human, network, wireless, etc.). The organization relies on a variety of DLP strategies and solutions to prevent data loss. The organization's DLP strategies and solutions are reevaluated regularly to ensure their relevancy and effectiveness. This security procedure applies to all the employees and users of the organization. Individuals working for the organization internally or externally are subject to the same rules when they are using the organization's information technology resources or have any means of access to data that has been classified as confidential or private.

- **Best Practices**
  - The sender will receive an Outlook message when an email is sent that contains sensitive information. Faculty and staff can still manually encrypt any email.
  - Do not forward email you receive that contains sensitive information. If it is required to do so, redact the sensitive information before replying.
  - Seek alternate means of transmitting the sensitive data. (secure web applications, etc.)
- **Data classification**

In the context of information security, is the classification of data based on its level of sensitivity and the impact to the organization should that data be disclosed, altered or destroyed without authorization. Classification of data will aid in determining baseline security controls for the protection of the data. All organizational data is classified into one of three sensitivity levels (tiers), or classifications:

Tier 1-

Confidential Data i.e., when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the organization. Unauthorized access to or disclosure of confidential information could constitute an unwarranted invasion of privacy and cause financial loss and damage to the organization's reputation and the loss of community confidence. The highest level of security controls should be applied. Access to Confidential data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the organization who require such access in order to perform their job ("need-to-know"). Access to Confidential data must be requested for an individual and approved by the Technology Committee. Data access granted to individuals must be reviewed and authorized by the Data Owner who is responsible for the data.

Restricted Data is a particularly sensitive category of Tier 1-Confidential data. Restricted data is defined as 'any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transmission'.

Tier 2-

Internal/Private Data i.e., when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the organization. By default, all information assets that are not explicitly classified as Confidential or Public data should be treated as Internal/Private data. A reasonable level of security controls should be applied to internal data. Access to Internal/Private data must be requested for an individual and approved by the Technology Committee. Data access granted to individuals must be reviewed and authorized by the Data Owner who is responsible for the data. Access to Internal/Private data may also be authorized to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by one's department. Internal/Private Data is moderately sensitive in nature. Often, Tier 2 Internal/Private data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the organization should this information not be available when needed is typically moderate. Examples of Internal/Private data include such as financial reports, some research data.

Tier 3-

Public Data i.e., when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the organization. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data. Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity of Public data should be protected.

Violations –

Anyone who knows or has reason to believe that another person has violated this procedure shall report the matter promptly to his/her supervisor, department head or the Technology Committee. After a violation of this procedure has been reported or discovered, the issue will be handled as soon as possible to reduce harm to the organization. Violators of this procedure may be subject to disciplinary action, up to and including the termination of employment depending on the severity of the violation or data breach.

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.

Neon Vinimay Private Limited

For NEON VINIMAY PVT. LTD.

DIRECTOR

Jatesh Jain

Designated Officer

Date: -31/12/2023