Data Masking Policy

# Introduction

a. Purpose: The purpose of this policy is to protect sensitive data and preserve individual privacy by implementing data masking techniques.

b. Scope: This policy applies to all employees, contractors, and third-party entities that handle or have access to sensitive data within the organization.

# Definitions

a. Sensitive Data: Any information that, if compromised, could result in financial loss, reputational damage, or harm to individuals, including but not limited to personally identifiable information (PII), financial data, health information, and intellectual property.

b. Data Masking: The process of transforming sensitive data in such a way that it is rendered unreadable or irreversibly de-identified, while still maintaining its authenticity and usability for non-production purposes.

# Data Masking Guidelines

a. Data Classification: The organization shall classify data based on its sensitivity level and determine which data requires masking for non-production use.

b. Data Masking Techniques: The organization shall employ approved data masking techniques, such as:

* Tokenization: Replacing sensitive data with random tokens while preserving format and data type.
* Substitution: Replacing sensitive data with fictitious but realistic values.
* Shuffling: Randomly reordering the sensitive data within a dataset.
* Encryption: Using strong encryption to protect sensitive data during non-production use.

c. Retention of Original Data: The organization shall ensure that the original sensitive data is securely stored and accessible only to authorized personnel.

d. Data Masking for Development and Testing: Data masking shall be applied to sensitive data used in development, testing, and quality assurance environments.

e. Data Masking for Training and Analytics: Data masking shall be applied to sensitive data used in training and analytics to prevent unauthorized access to real data.

f. Preservation of Data Relationships: Data masking techniques should preserve the relationships and referential integrity of masked data to maintain the usefulness of the data.

# Access Controls and Monitoring

a. Access Control: Access to masked data shall be restricted based on the principle of least privilege. Only authorized personnel with a legitimate need should have access to masked data.

b. Monitoring: Regular audits and monitoring shall be conducted to ensure compliance with this policy and detect any unauthorized access or use of sensitive data.

# Incident Response and Reporting

a. Data Breach Incident: In the event of a data breach involving masked data, the organization shall follow the established incident response plan and notify affected individuals and regulatory authorities, as required by applicable laws and regulations.

b. Reporting: Any suspected or actual violations of this policy shall be reported to the designated privacy officer or the relevant department head for investigation.

# Training and Awareness

a. Privacy Training: All employees and relevant stakeholders shall receive training on this data masking policy and related privacy practices.

b. Privacy Awareness: The organization shall promote privacy awareness among employees to emphasize the importance of protecting sensitive data through data masking.

# Policy Review and Updates

a. Regular Review: This policy shall be reviewed periodically to ensure its effectiveness and alignment with changing organizational needs and regulatory requirements.

b. Updates: Any updates or revisions to this policy shall be communicated to all relevant stakeholders.

# Non-Compliance

a. Violations of this policy may result in disciplinary action, up to and including termination, in accordance with the organization's policies and procedures.

By implementing this Data Masking Policy, the organization can safeguard sensitive data and reduce the risk of data breaches while maintaining the utility of the data for non-production purposes.