Data Masking Procedure

HT-ISMS-SOP-34

Document Control

Document Title	Data Masking Procedure		
Document ID	HT-ISMS-SOP-34		
Document Type	Procedure	Classification	Internal
Version	1.0	Release Date	
Author	Name		
	Designation		
Reviewer	Name		
	Designation		
Approver	Name		
	Designation		

Revision History		
Version	Revision Description	Release Date
1.0	Initial Release	

Document Distribution			
Name	Department	Designation	Company
	IT	System Admin	HackTech
	Operations	VP Projects	HackTech
	IT	Information Security	HackTech

Contents

1. Introduction

HackTech collects and processes a wide variety of personally identifiable information (PII) as part of its normal business operations. To reduce risk both in the long-term storage of this PII and in circumstances where it is shared with a third party, it may be appropriate to use data masking techniques to anonymize the information

2. Purpose

The purpose of this document is to set out a process for data masking which must be followed where the task is carried out, and to form the basis for more detailed procedures that may be created to cover specific, often regular, data masking exercises.

3. Scope

This control applies to all systems, people, and processes that constitute the organization's information systems, including board members, directors, employees, suppliers, and other third parties who have access to HackTech systems.

4. Data Collection and Types:

- **Types of PII Collected:**
  - Aadhaar Card Number
  - PAN Card Number

5. Application to Product and Employee Data:

While HackTech does not save clients' user data, but if it requires to store we ensure masking for product data and employees' data as well.

6. Data Masking Process:

a. Understanding Requirements:

- Identify the types of PII collected and the specific needs for masking and encryption.

b. Analyzing Data Attributes:

- Review the collected data attributes to identify sensitive information that requires masking.

c. Performing Anonymization:

I. Masking Aadhaar Card, PAN Card, and Other Numbers:

- Data Entry:
    - Only the last four digits of the Aadhaar card number, PAN card number or any PII are retained during data entry.

II. Storage and Encryption:

- PII Data Storage:
    - Only the last four digits of sensitive numbers are stored in the database.
    - These digits are encrypted using SHA-256 encryption to ensure data security.

III. Data Security Measures:

- Database Encryption:
    - All stored PII data, including the last four digits of sensitive numbers, are encrypted using SHA-256 to safeguard against database compromises.

d. Assessing Reidentification Risk:

- Evaluate the risk of reidentification of masked data.

e. Setting Controls:

Once sufficient anonymization has been carried out to meet the re-identification risk threshold, additional controls must be considered to accompany the dataset.

- Access control – limiting the people who have access to the PII within the organization, often using file permissions or an encryption key or password.

f. Documentation:

- Maintain detailed policy and procedure documents to outline the data masking and encryption processes.

g. Review and Audit:

- Conducts monthly audits to ensure compliance with data security policies.

9. Conclusion

By adhering to this data masking procedure, HackTech aims to ensure the secure and compliant handling of PII through effective data masking techniques. This approach not only helps mitigate the risks associated with data breaches but also ensures compliance with legal and regulatory requirements, thereby protecting the privacy of individuals and fostering trust with stakeholders.