Data Masking Policy

HT-ISMS-PL-23

Document Control

Document Title	Data Masking Policy		
Document ID	HT-ISMS-PL-23		
Document Type	Policy	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

Table of Contents

1. Introduction

HackTech makes use of a variety of data about identifiable individuals (personally identifiable information, PII), including data about:

- Current, past, and prospective employees

2. Purpose

The purpose of this policy is to set out the approach that HackTech requires when data masking techniques are used, so that the effectiveness of privacy safeguards can be maximized and compliance with relevant legislation can be ensured.

3. Scope

This policy 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. It covers all personally identifiable information (PII) held within the organization.

4. Data Masking Policy

4.1 General Policy

The use of data masking techniques must always take account of HackTech compliance obligations under relevant privacy legislation.

4.2 Application of Data Masking Techniques

This policy applies in two main sets of circumstances:

1. Where PII that is held internally requires the application of data masking techniques to reduce risk.

4.3 Exclusion

This policy does not apply to the preparation of PII for release to the general public. In such cases, specific guidance from top management must be sought as the requirements for effective data masking (such as anonymization) are typically more stringent, with a higher risk of re-identification.

4.4 Data Masking Techniques

Techniques that may be used include:

- Suppression of attributes that are not needed for the purpose of the processing, such as the removal of specific columns in spreadsheets

4.5 Risk-Based Approach

A risk-based approach will be used with regard to possible re-identification of PII, considering the sensitivity of the data and potential harm to the PII principal.

4.6 Subject Matter Expert Involvement

The involvement of a subject matter expert will be required in most cases to assess the risk of re-identification, for example by inferring someone's identity from other available data.

4.7 Supporting Technical Controls

Data masking techniques must be used in combination with supporting technical controls where possible. These may include restricting online access, allowing only query access to the data, and limiting the number of recipients of the data.

4.8 Documentation and Security

The process used for data masking must be documented in each instance and kept securely for audit purposes and to avoid its use in later re-identification. Where techniques for pseudonymization are used, the associated mapping tables (which show the real data against the pseudonym) must be secured effectively as they provide the key to re-identification.

4.9 Records and Agreements

Records must be kept of PII that has been provided to third parties, with written agreements covering how the data may be used and the controls that are expected to be applied to it.

5. Conclusion

By adhering to this data masking policy, 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.