Pseudonymisation and Encryption

Policy Version 9

REZOLVE.ai

Document Information

Name of the document	Pseudonymisation and EncryptionPolicy
Release date	04-March-2019
Owned by	Mayank Baghel
Governed by	Mr.Udaya Bhaskar Reddy

RevisionHistory

Version No	Version Date	Details of Change
1	28-Feb-2019	Initially Drafted
2	04-Mar-2019	Final
3	15-Dec-2020	Reviewed and no change
4	03-Dec-2021	Reviewed and no change
5	04-Mar-2022	Updated Document Information
6	03-Mar-2023	Reviewed and no change
7	24-Nov-2024	Reviewed and No change
8	23-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
9	29-May-2026	Reviewed and No change

Reviewer and Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	04-June-2026

Table of Contents

16 Purpose 5

Scope and Purpose

The purpose of this document is to provide guidance to the Company (hereafter referred to as "Organization") for establishing and maintaining pseudonymisation and encryption of personal data.
The users of this document are the **Data Protection Officer**, **IT Security Officer**, and the **representatives of business units responsible for processing personal data**.

Responsibilities

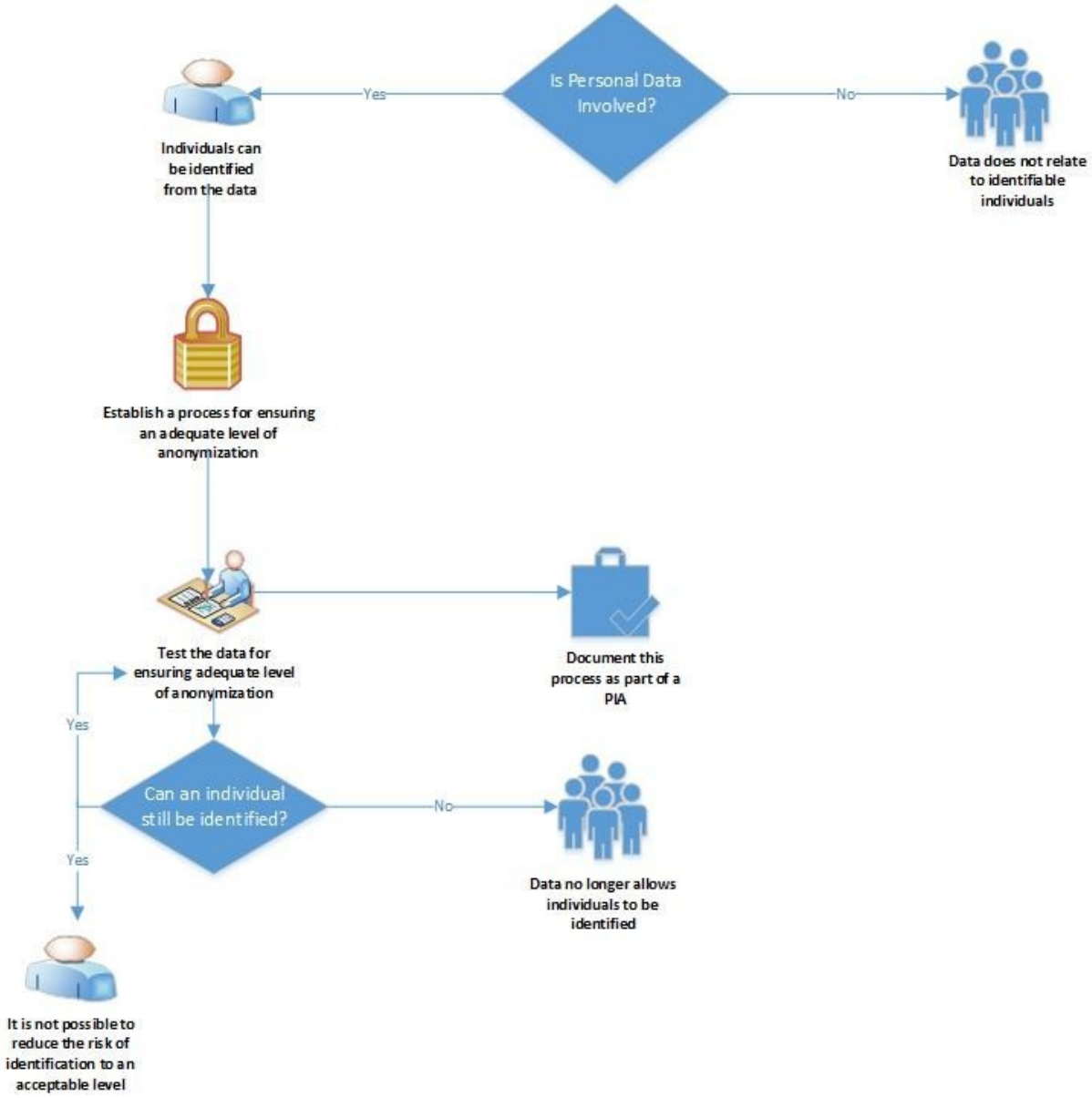
- Organization's Data Privacy Officer should be responsible for ensuring that the designated training in areas of Data Protection and Information Security covers Anonymization and Pseudonymization.
- All employees and contractors (full-time and part-time) should be responsible for compliance with the policies, procedures and guidelines.

What is Anonymization?

- Anonymization is the process of removing, obscuring or altering any identifiers in a dataset pertaining to a specific data subject.
- Anonymized data should be considered to be personal data for the original data controller whereas it is considered non-personal data for any other users of the data.
- Anonymization process allows data to be shared or distributed ethically and legally, thereby realizing their huge social, environmental and economic value, while preserving confidentiality.
- Anonymization of personal data can help facilitate the organization's data needs in a privacy-friendly manner.
- Anonymization also aids compliance with the data protection obligations whilst enabling proactive publication and sharing of data.
- Employees should only have access to the data that is necessary for the completion of the business activity which they are involved in.
- Data access to data subjects should be on a **need-to-know basis** principle. This principle applies to the use of personal data. By de-identification, users are able to make use of employees' data without having to access the identifiable data items.

When to Anonymize Data

- Organization should consider anonymization as a possibility at all times when handling personal data, where its disclosure in a non-anonymized form should be likely to reveal personal data resulting in a breach.
- Organization, while sharing the personal data, should have legal reasons to justify the sharing and disclosure of personal data. The requirement and necessity of every disclosure should be considered and documented.
- Organization, before sharing or providing data, should ensure that only data that is required to meet the purpose is shared/provided.
- The below table highlights the process when and how to anonymize data.


Is Personal Data Involved?
Yes
No
Individuals can be identified from the data
Data does not relate to identifiable individuals
Establish a process for ensuring an adequate level of anonymization
Test the data for ensuring adequate level of anonymization
Document this process as part of a PIA
Yes
Can an individual still be identified?
No
Data no longer allows individuals to be identified
Yes
It is not possible to reduce the risk of identification to an acceptable level

If it's not clear whether personal data is involved, the organization should consider:

- Is it reasonably likely that a data subject can be identified from those data and from other data? What other data are available, either to the public or to researchers or other organizations?
- How and why could your data be linked to other datasets?

Factors to take into account while establishing a process to ensure an adequate level of anonymization should include:

- The likelihood of re-identification being attempted;
- The likelihood that re-identification would be successful;
- The anonymization techniques which are available to use; and
- The quality of the data after anonymization has taken place and whether this will meet the needs of the organization using the anonymized data.

If it is not possible to reduce the risk of identification to an acceptable level (in cases where certain attributes of the personal data are required for processing operations, such as bank account number for payroll processing and thus cannot be anonymized), the organization should not publish unless the processing complies with the applicable laws.

Anonymization Techniques

- Data anonymization techniques should help in removing the identifiers from the data.
- These techniques can be statistical, algorithmic, or custom-built and should ensure that the data type of the field remains unchanged. That is, the masked value and the original values should belong to the same data type.
  For example, a field containing names of the data subjects should contain characters and not numbers after anonymization.
- The technique should be considered high-risk if organizations are unable to completely anonymize the data (i.e., certain attributes of the personal data can be used to identify the data subject).
- The costs of implementation, nature, scope, context, and purposes for processing, and the risk of re-identification should be considered while determining the anonymization technique to be utilized for a particular process.

Aggregation

- This involves publishing/providing the data as a summary, therefore ensuring that data relating to or identifying any data subject is not disclosed.
- Aggregation is a relatively low-risk technique as it will be difficult to find data about a specific data subject by using aggregated data.
- The resulting data cannot support data subject-level research but can be sufficient to analyze trends.

Data Masking

- Data Masking involves stripping out personal identifiers such as names from a piece of data, to create a dataset in which personal identifiers are not present.
  This is a relatively high-risk technique because the anonymized data still exists in a data subject-level form.

Nulling Out

- Nulling out consists of simply removing special categories of personal data by deleting it from the shared dataset. While this is a simple technique, it may not be suitable if an evaluation needs to be performed on the data or the fictitious form of the data.

Pseudonymisation

Definition of Pseudonymisation

- Pseudonymization enhances privacy by replacing most identifying fields within a data record by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field.
- As per GDPR, pseudonymization is "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information."
  To pseudonymize a data set, the "additional information" must be "kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person."

How Pseudonymisation Helps to Protect Privacy

- Pseudonymization or anonymization is highly recommended by the GDPR regulation. Such techniques reduce risk and assist "data processors" in fulfilling their data compliance regulations.
- Organizations should use the pseudonymization process for the following reasons:
  - **Permits processing of personal data** for a purpose other than originally intended, in the "existence of appropriate safeguards, which may include encryption or pseudonymization."
    Other purposes should include profiling, business analysis, outsourcing data processing to non-EU/EEA countries, and using for scientific, historical, and statistical purposes.
  - **Exempts the organization** from complying with data subject's rights to access, rectification, erasure, and data portability of his or her personal data, if the personal data can no longer be linked to the identified data subject.
  - **Makes pseudonymization a central feature** of the requirement for data protection by design and by default.
  - **Makes pseudonymization an appropriate technical measure** for ensuring the security of processing personal data.
  - **Requires that, in the event of a security breach, the organization notify identified data subjects impacted by the breach.**
    Since pseudonymized data is not linked to an identified data subject, notification is not required unless the data subject is identifiable due to:
    - The pseudonymization key is disclosed in a security breach.
    - The data subject is identified by linking pseudonymized and additional, non-pseudonymized data (e.g., birth date, gender, zip code).
    - The use of Codes of Conduct that include pseudonymization.
  - **Enables processing of personal data for scientific, historical, and statistical purposes** if the data is safeguarded by pseudonymization.

Current Pseudonymisation Policy

- As a policy, the company has decided not to use any pseudonymization technique.

Encryption Policy

Purpose

- Encryption is the conversion of data into a form, called cipher text, that cannot be easily understood by unauthorized people.
  Decryption is the process of converting encrypted data back into its original form, so it can be understood.
- The process of encryption ensures that only authorized people have access to confidential information. As information travels from one system/network to another system/network, there is an additional layer of security to protect the data.

Opportunity of Eavesdropping (Man-in-the-Middle (MITM) Attack)

- Encryption assures that the confidentiality, integrity, and non-repudiation of the data are maintained. It helps to mitigate risks associated with eavesdropping, also known as "man-in-the-middle" (MITM) attacks.

Policy Objective

- This policy aims to improve the security and confidentiality of information and reduce the risk of unauthorized access, loss, or damage to information.

Scope

- This policy is applicable to all the information stored at the Company in an electronic form.

Policy Standards

- **Encryption Algorithms:**
  Proven, standard algorithms such as SHA2, AES, and RSA must be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application.
- **Security Steering Committee:**
  The Security Steering Committee must approve any use of encryption algorithms.
- **Encryption Applicability:**
  Encryption shall be applied wherever possible to the information stored or transmitted, as appropriate for the information classification and business requirements.
- **Communication Security:**
  All communication established between public networks (such as the internet) and office networks should be encrypted.
- **Media Encryption:**
  All media containing office information shall be encrypted. This includes media, laptops, and USB devices (if allowed).
- **Standard Algorithms:**
  Only proven, standard algorithms and encryption technologies shall be used.
- **Key Management:**
  Encryption keys for sensitive data shall be changed at least half-yearly.
- **Proprietary Encryption:**
  The use of proprietary encryption algorithms is not allowed for any purpose unless reviewed by qualified experts.
- **Wireless Network Encryption:**
  For wireless networks transmitting cardholder data, encrypt the transmissions using Wi-Fi Protected Access (WPA or WPA2) technology, IPsec VPN, or SSL/TLS.
- **Decision Criteria:**
  The decision on the requirements of information encryption must be made considering the following criteria:
  - All applicable legal requirements for storing and transmitting information.
  - Risks in transmitting information internally and externally.
  - Risks in storing the information and access control.

What to Encrypt

- **Wireless Networks:**
  Encryption for all wireless networks.
- **Data in Transit:**
  Encryption for all data in transit.
- **Sensitive/Confidential Data:**
  Encryption for all sensitive/confidential data in storage and under transmission.

Exception to Encryption

- In certain circumstances, the company may choose not to encrypt critical data, databases, etc. In such situations, the Security Steering Committee needs to provide approval for a waiver to encrypt upon receiving a business case for not encrypting the data.
- Such a waiver for encryption shall be valid for one year, and approval needs to be obtained annually.

Encryption Key Management

- **Key Management:**
  Encryption key management shall be in place to support the organization's use of cryptographic techniques.
- **Tools for Key Generation:**
  Appropriate tools shall be used to generate strong cryptographic keys.
- **Key Length and Algorithm Selection:**
  Key length and encryption algorithms must be decided based on applicable legal requirements and risks identified in the risk assessment procedure.
- **Key Storage:**
  Encryption keys shall be stored securely in an encrypted manner.

Transferring Data

- **Data Sharing Agreements:**
  The organization's data-sharing agreements should be in place whenever data needs to be transferred to another organization.
- **Anonymized or Pseudonymized Data:**
  If the transfer of data requires secondary use, a form of anonymized or pseudonymized data should be sent.
- **Safeguards for Data Transfer:**
  Data transfers should be permitted where appropriate safeguards are provided by the data controller or processor. These safeguards should ensure enforceable data subject rights and effective legal remedies are available.
- **Types of Safeguards:**
  Appropriate safeguards include, among other things, binding corporate rules under standard contractual clauses.
- **Approved Mechanisms for Safeguards:**
  Data controllers or processors should rely on an approved code of conduct or an approved certification mechanism, along with binding and enforceable commitments in the third country to apply these safeguards. This includes ensuring data subjects' rights are protected.

Derogations for Data Transfers

The following are the list of derogations permitting transfers where:

1. **Explicit Informed Consent:**
   Explicit informed consent should be obtained from the data subject.
2. **Necessary for Contract Performance:**
   The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures.
3. **Contractual Necessity for Data Subject's Interest:**
   The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person.
4. **Public Interest:**
   The transfer is necessary for important reasons of public interest.
5. **Legal Claims:**
   The transfer is necessary for the establishment, exercise, or defense of legal claims.
6. **Vital Interests of the Data Subject:**
   The transfer is necessary to protect the vital interests of the data subject, where consent cannot be obtained.

- **Limited Derogations for Compelling Legitimate Interests:**
  A very limited derogation to transfer is available if the transfer is necessary for the purposes of compelling legitimate interests of the data controller. Notification to the supervisory authority is required if relying on this derogation.

Training

- **Employee Awareness:**
  The organization's employees should be made aware of their responsibilities relating to this policy through both generic and specific training programs and guidance.

Data Controller Security Measures

Overview:
Security measures create a comprehensive defense-in-depth strategy for protecting sensitive data within SaaS applications. By combining Data Loss Prevention (DLP), encryption at rest and in transit, HTTPS protocol, and VPN access, the organization effectively mitigates various risks associated with data breaches and unauthorized access.

Data Controller Decisions:
The data controller has the authority to decide which data needs to be anonymized and which can remain in its original form. This granular control ensures that only necessary data is exposed, reducing the risk of sensitive data leakage. There is no other processing of sensitive data managed by the customer.

Data Loss Prevention (DLP)

Data Loss Prevention (DLP) tools help prevent unauthorized access and transmission of sensitive data. These tools monitor, detect, and block sensitive data from being shared or transmitted without proper authorization.

Encryption

Encryption ensures that data is protected both when stored (at rest) and when transmitted (in transit):

- **Data at Rest:**
  Your application data is stored in an encrypted format in the database. Azure SQL Database provides built-in encryption mechanisms, ensuring that data remains secure even if the physical storage is compromised.
- **Data in Transit:**
  All data transmitted over the network uses TLS 1.2, a protocol that ensures data integrity and privacy between communicating applications. This prevents eavesdropping and man-in-the-middle attacks.

HTTPS Protocol

Using HTTPS for all internal applications ensures that data transmitted within your network is encrypted. HTTPS combines HTTP with TLS/SSL to encrypt the communication channel, protecting data from being intercepted by unauthorized parties.

VPN Access

Restricting access to data stores through a VPN adds another layer of security:

- **Encryption:**
  VPNs encrypt the data traffic between the user's device and the server, ensuring that any data transmitted is secure.
- **Access Control:**
  VPNs also enforce strict access controls, ensuring that only authorized users can access the data stores.

Anonymisation Techniques

Data anonymisation techniques should help in removing identifiers from the data:

- **General Considerations:**
  These techniques can be statistical, algorithmic, or custom-built. They should ensure that the data type of the field remains unchanged; for example, a field containing names of the data subjects should contain characters and not numbers after anonymisation.
- **Risk of Incomplete Anonymisation:**
  The technique should be considered high-risk if the organization is unable to completely anonymise the data, meaning certain attributes of personal data could still be used to identify the data subject.
- **Cost and Risk Considerations:**
  The costs of implementation, nature, scope, context, and the purposes for processing, as well as the risk of re-identification, should be considered while determining the anonymisation technique to be used for a particular process.

Anonymisation Techniques Overview

1. **Aggregation:**
   This involves publishing or providing the data as a summary, ensuring that data related to or identifying any data subject is not disclosed. Aggregation is a relatively low-risk technique, as it will be difficult to identify data about a specific data subject by using aggregated data. However, the resulting data cannot support data subject-level research but can be sufficient to analyze trends.
2. **Data Masking:**
   Data masking involves stripping out personal identifiers, such as names, from a piece of data to create a dataset in which personal identifiers are not present. This is a relatively high-risk technique because the anonymised data still exists in a data subject-level form.
3. **Nulling Out:**
   Nulling out consists of simply removing special categories of personal data by deleting it from the shared dataset. While this is a simple technique, it may not be suitable if an evaluation needs to be performed on the data or if the data is fictitious.
4. **Pseudonymisation:**
   - **Definition:**
     Pseudonymisation enhances privacy by replacing most identifying fields within a data record with one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field.
   - **GDPR Definition:**
     As per GDPR, pseudonymisation is "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." To pseudonymize a data set, the "additional information" must be kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person.

Pseudonymisation

To pseudonymize a data set, the "additional information" must be "kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person."

How Pseudonymisation Helps to Protect Privacy

Pseudonymisation (or anonymization) is highly recommended by the GDPR regulation. These techniques reduce risk and assist "data processors" in fulfilling their data compliance regulations. Organizations should use pseudonymisation for the following reasons:

1. **Purpose Beyond Original Intent:**
   It permits the processing of personal data for purposes other than originally intended, in "the existence of appropriate safeguards," which may include encryption or pseudonymisation. Other purposes may include profiling, business analysis, outsourcing data processing to non-EU/EEA countries, and using the data for scientific, historical, and statistical purposes.
2. **Exemption from Certain Rights:**
   It exempts the organization from complying with data subject's rights to access, rectification, erasure, and data portability of personal data, if the personal data can no longer be linked to the identified data subject.
3. **Data Protection by Design and Default:**
   Pseudonymisation makes it a central feature of the requirement for data protection by design and by default.
4. **Security of Personal Data:**
   Pseudonymisation serves as an appropriate technical measure to ensure the security of personal data processing.
5. **Security Breach Notification:**
   In the event of a security breach, the organization must notify identified data subjects impacted by the breach. However, since pseudonymised data is not linked to an identified data subject, notification is not required unless:
   - The pseudonymisation key is disclosed in a security breach.
   - The data subject can be identified by linking pseudonymised and additional, non-pseudonymised data (e.g., birth date, gender, zip code).
6. **Use of Codes of Conduct:**
   The use of codes of conduct that include pseudonymisation can help ensure compliance with GDPR.
7. **Scientific, Historical, and Statistical Purposes:**
   Pseudonymisation enables the processing of personal data for scientific, historical, and statistical purposes, provided the data is safeguarded by pseudonymisation.

Encryption Policy

Purpose:
Encryption is the conversion of data into a form (ciphertext) that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form so that it can be understood.

The process of encryption ensures that only authorized people have access to confidential information. As information travels from one system/network to another system/network, there is an opportunity for eavesdropping (also known as a "man-in-the-middle" (MITM) attack). Encryption ensures the confidentiality, integrity, and non-repudiation of the data.

Pseudonymisation

To pseudonymize a data set, the "additional information" must be "kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person."

How Pseudonymisation Helps to Protect Privacy

Pseudonymization or anonymization is highly recommended by the GDPR regulation. Such techniques reduce risk and assist "data processors" in fulfilling their data compliance regulations.

Organizations should use Pseudonymization process for the following reasons:

- **Permits processing of personal data for a purpose other than originally intended**, in "the existence of appropriate safeguards, which may include encryption or Pseudonymization." Other purposes should include profiling, business analysis, outsourcing data processing to non-EU/EEA countries, and using for scientific, historical, and statistical purposes.
- **Exempts the organization from complying with data subject's rights** to access, rectification, erasure, and data portability of his or her personal data, if the personal data can no longer be linked to the identified data subject.
- **Makes Pseudonymization a central feature of the requirement for data protection by design and by default.**
- **Makes pseudonymization an appropriate technical measure for ensuring the security of processing personal data.**
- **Requires that, in the event of a security breach, the organization notify identified data subjects impacted by the breach.** Since pseudonymization data is not linked to an identified data subject, notification is not required unless the data subject is identifiable due to:
    - The pseudonymisation key is disclosed in a security breach.
    - The data subject should be identified by linking pseudonymized and additional, non-pseudonymized data (e.g., birth date, gender, zip code).
- **The use of Codes of Conduct that include pseudonymization.**
- **Enables processing personal data for scientific, historical, and statistical purposes if the data is safeguarded by pseudonymization.**

Current Pseudonymisation Policy

As a policy, the company has decided not to use any pseudonymisation technique.

Encryption Policy

Purpose
Encryption is the conversion of data into a form, called a cipher text, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.
The process of encryption ensures that only authorized people have access to confidential information. As information travels from one system/network to another system/network, there is an opportunity for eavesdropping, also known as ‘man-in-the-middle’ (MITM) attack. Encryption assures that the confidentiality, integrity, and non-repudiation of the data.

Policy Aim

This policy aims to improve the security and confidentiality of information and reduce the risk of unauthorized access, loss of, and damage to information.

Scope

This policy is applicable to all the information stored at the Company in an electronic form.

Policy Standards

- Proven, standard algorithms such as SHA2, AES, and RSA must be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application.
- The Security Steering Committee must approve any use of encryption algorithms.

- Encryption shall be applied wherever possible to the information stored or transmitted as appropriate for the information classification and business requirements.
- All communication established between public network(s) (such as in internet) and office network should be encrypted.
- All media containing office information shall be encrypted. This includes media, laptop, USB (if allowed).
- Only proven, standard algorithms and encryption technologies shall be used. Encryption keys for sensitive data shall be changed at least half yearly.
- The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts.
- For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSec VPN, or SSL/TLS.
- Decisions on requirements of information encryption must be made considering the following criteria:
    - All applicable legal requirements for storing and transmission of information.
    - Risks in transmitting information internally and externally.
    - Risk in storing the information and access control.

What to Encrypt

- Encryption for all wireless networks
- Encryption for all data in transit
- Encryption for all sensitive/confidential data in storage and under transmission

Exceptions to Encryption

- In certain circumstances, the company may choose not to encrypt critical data, databases, etc. In such situations, the Security Steering Committee needs to provide an approval for a waiver to encrypt on receiving a business case for not encrypting the data.
- Such waiver for encryption shall be valid for one year and approval needs to be obtained annually.

Encryption Key Management

- Encryption key management shall be in place to support the organization's use of cryptographic techniques.
- Appropriate tools shall be used to generate strong cryptographic keys.
- Key length and encryption algorithms must be decided considering applicable legal requirements and risks identified in the Risk assessment procedure.
- Encryption keys shall be stored securely, in an encrypted manner.

Transferring Data

- Organization's data sharing agreements should be in place when data should be transferred to another organization.
- If the transfer of data should require secondary use, then a form of anonymised or pseudonymized data should be sent.
- Organization's data transfers should also be permitted where appropriate safeguards should be provided by the data controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available.
- Appropriate safeguards include amongst other things binding corporate rules under standard contractual clauses.
- Data controllers or processors should also rely on an approved code of conduct or an approved certification mechanism together in each case with binding and enforceable commitments in the third country to apply these safeguards including as regards data subjects' rights.
- Following below are the list of derogations similar to those included in the directive permitting transfers where:
    - Explicit informed consent should be obtained.
    - The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures.

    - The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person.
    - The transfer is necessary for important reasons of public interest.
    - The transfer is necessary for the establishment, exercise or defense of a legal claim.
    - The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained.
- There should be a very limited derogation to transfer is available and the transfer is necessary for the purposes of compelling legitimate interests of the data controller and notification to the supervisory authority should be required if relying on this derogation.

Training

Organization's employees should be made aware of their responsibilities relating to this policy through generic and specific training programs and guidance.

Data Controller Security Measures

- Security measures create a comprehensive defense-in-depth strategy for protecting sensitive data within SaaS applications. By combining DLP, encryption at rest and in transit, HTTPS protocol, and VPN access, which effectively mitigate various risks associated with data breaches and unauthorized access.
- **Data Controller Decisions:** The data controller has the authority to decide which data needs to be anonymised and which can remain in its original form. This granular control ensures that only necessary data is exposed, reducing the risk of sensitive data leakage. There is no other processing of sensitive data managed by the Customer.

Data Loss Prevention (DLP)

- Data Loss Prevention (DLP) tools help prevent unauthorized access and transmission of sensitive data.

Encryption

- **Encryption ensures that data is protected both when it is stored (at rest) and when it is being transmitted (in transit):**
    - **Data at Rest:** Your application data is stored in an encrypted format in the database. Azure SQL Database provides built-in encryption mechanisms, ensuring that data remains secure even if the physical storage is compromised.
    - **Data in Transit:** All data transmitted over the network uses TLS 1.2, a protocol that ensures data integrity and privacy between communicating applications. This prevents eavesdropping and man-in-the-middle attacks.

HTTPS Protocol

- Using HTTPS for all internal applications ensures that data transmitted within your network is encrypted. HTTPS combines HTTP with TLS/SSL to encrypt the communication channel, protecting data from being intercepted by unauthorized parties.

VPN Access

- Restricting access to data stores through a VPN adds another layer of security:
    - **Encryption:** VPNs encrypt the data traffic between the user's device and the server, ensuring that any data transmitted is secure.

- **Access Control:** VPNs can also enforce strict access controls, ensuring that only authorized users can access the data stores.

Note

- Next review cycle for this policy is March-2027. Management can review the policy any time and can make changes depending on the situation.
- All documents related to policies and procedures any reference to Actionable Science is as good as Rezolve.