Data Privacy Policy

Effective Date: April 7, 2025

Last Revised: April 7, 2025

Policy Owner: Information Security Department

Purpose

The purpose of this policy is to establish guidelines for the proper handling and protection of sensitive data within [Company Name] to ensure compliance with applicable data protection laws and regulations.

Scope

This policy applies to all employees, contractors, consultants, temporary workers, and third parties who have access to company data and information systems.

Definitions

- **Personal Data:** Any information relating to an identified or identifiable individual.
- **Sensitive Data:** Information that requires special handling, including Personal Data, financial information, health information, intellectual property, and confidential business information.
- **Data Subject:** An individual whose personal data is processed.
- **Processing:** Any operation performed on data, including collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, or deletion.

Policy Guidelines

Data Collection and Use

1. Only collect personal data for specified, explicit, and legitimate purposes
2. Process data lawfully, fairly, and in a transparent manner
3. Ensure data collected is adequate, relevant, and limited to what is necessary
4. Maintain accuracy of data and take reasonable steps to rectify inaccuracies
5. Retain data only as long as necessary for the purposes for which it was collected

Data Security

1. Implement appropriate technical and organizational measures to protect data against unauthorized access, disclosure, alteration, or destruction
2. Use encryption for sensitive data at rest and in transit
3. Restrict access to sensitive data on a need-to-know basis
4. Regularly back up data in accordance with the company's backup policy
5. Promptly report any suspected data breaches following the Incident Response procedure

Data Subject Rights

[Company Name] respects the rights of data subjects, including:

- Right to access their personal data
- Right to rectification of inaccurate data
- Right to erasure ("right to be forgotten")
- Right to restriction of processing
- Right to data portability
- Right to object to processing

Requests from data subjects should be directed to the Privacy Office at privacy@companyname.com.

Third-Party Data Sharing

1. Only share data with third parties when there is a legitimate business need
2. Ensure appropriate data processing agreements are in place with third parties
3. Conduct due diligence on third parties' data security practices
4. Maintain a record of all third parties with whom data is shared

Data Retention and Disposal

1. Retain data in accordance with the company's Data Retention Schedule
2. Securely dispose of data when it is no longer needed
3. Document the disposal of sensitive data

Training and Awareness

All employees must complete data privacy training:

- Upon hiring
- Annually thereafter

- When significant changes to privacy regulations or this policy occur

Non-Compliance

Failure to comply with this policy may result in:

- Disciplinary action, up to and including termination
- Legal penalties and fines
- Damage to company reputation

Related Documents

- Information Security Policy
- Data Classification Policy
- Incident Response Plan
- Data Retention Schedule
- Acceptable Use Policy

Policy Review

This policy will be reviewed annually or when significant changes in privacy regulations occur.

For questions about this policy, contact the Privacy Office at privacy@companyname.com or ext. 5555.