AUTOMATIC SYSTEMS LTD.

ASL Data Disposal Policy

IT
AUTOMATIC SYSTEMS LTD
Champ de Mars

Table Of Contents

1. Objective

This policy outlines the procedures for securely disposing of sensitive data, including client records, employee records and financial documents, whether stored in hard copy or soft copy, in compliance with the **Data Protection Act (DPA) 2017**.

2. Scope

This policy applies to all employees, contractors and third-party service providers handling sensitive information, including:

- **Client Records**: Personal identification, betting history, payment details.
- **Employee Records**: Personal details, payroll information, employment contracts.
- **Financial Documents**: Company financial statements, transactional records.

3. Retention Periods

All sensitive information must be retained for the required legal, regulatory and business needs, after which it must be securely disposed of. The retention periods are as follows:

- **Client records**: Retained for 7 years after the client's last interaction.
- **Employee records**: Retained for 7 years after the termination of employment.
- **Financial documents**: Retained for 7 years after the end of the fiscal year.

Once the retention period lapses, records must be securely disposed of.

4. Roles and Responsibilities

Management will establish clear roles and responsibilities for secure record disposal:

- **Management**: Responsible for developing and overseeing the disposal procedures and finalizing the Record and Retention Schedule.
- **Data Protection Officer (DPO)**: Monitors compliance with the disposal process and ensures that records are disposed of according to the defined timelines.
- **Heads of Department**: Regularly review records within their department, supported by the DPO, to identify and handle records whose retention period has expired.
- **IT Team**: Responsible for disposal of soft copy records on servers or other media.
- **Employees**: Must comply with the disposal process outlined in this policy.

5. Disposal of Hard Copy Records

Sensitive information stored in hard copy (e.g., in filing cabinets) must be disposed of securely to prevent unauthorized access.

- **Shredding**: Hard copies containing sensitive information must be shredded.
- **Third-Party Disposal**: If using external disposal services, providers must be approved and provide certificates of destruction in accordance with the **DPA 2017**.

6. Disposal of Soft Copy Records

Sensitive data stored electronically on servers or other media must be securely deleted or destroyed.

- **Permanent Deletion**: Data must be irreversibly deleted from servers, ensuring no recovery. The method used by the IT Team is **Data Wiping with Overwriting** where the storage is overwritten multiple times with random data and then deleted.
- **Physical Media Destruction**: Physical media (e.g., including but not limited to hard drives) used to store sensitive data must be demagnetized or shredded.
- **Third-Party Services**: Providers must comply the **DPA 2017**, with destruction certificates provided.

7. Record and Retention Schedule

The **Record and Retention Schedule** outlines retention periods for all categories of sensitive information, in compliance with legal and business requirements. This schedule will guide the systematic disposal of data after the retention period lapses.

8. Walkthroughs and Regular Audits

To ensure ongoing compliance:

- **Walkthroughs**: Heads of Department, supported by the DPO, will conduct regular walkthroughs to identify instances where data retention has lapsed. This will involve:
    - Reviewing physical and electronic records.
    - Ensuring expired data is securely disposed of or put beyond use.
- **Regular Audits**: Management will conduct periodic audits to assess compliance with the disposal policy and retention schedule.

9. Data Breach Mitigation

Any breach or suspected breach of data during the disposal process must be immediately reported to the DPO. The DPO will initiate corrective actions, including notifying authorities as per the **DPA 2017**.

10. Training

All employees will receive regular training on:

- Secure disposal methods.
- Adhering to the Record and Retention Schedule.
- Compliance with the DPA 2017.

11. Penalties for Non-Compliance

Failure to comply with this policy may result in disciplinary actions, including termination of employment, or contractual penalties for third-party providers.