This document has been produced by DataTech Solutions, www.datatechsolutions.co.za, a website offering market research and analytics for small and medium businesses.

Directors: K. HARIPERSAD; S. NAIDOO
Reg No: 2016/356449/07
Web: www.datatechsolutions.co.za
Email: sagaran@datatechsolutions.co.za

Data Destruction Policy

1 Purpose

The purpose of this policy is to provide a framework for destruction of records and information created, maintained, used and held by DataTech Solutions in the course of business and service delivery.

The policy:

1.1 Provides a framework for the effective, efficient and secure disposal of records and information created, maintained, used and held by DataTech Solutions.

1.2 Ensures records containing personal or sensitive data are timely and securely disposed, as required by the Data Protection Act 1998, Principles 5 and 7.

1.3 Ensures records are destroyed in accordance with legislative, regulatory and statutory compliance and business requirements, as stipulated in the Generic Retention Schedule, service specific retention schedules, business classification schemes and records systems.

1.4 Ensures records are authorized for disposal, by senior officers with designated responsibility.

1.5 Ensures all records scheduled for disposal are recorded for audit and accountability purposes.

2 Scope

2.1 The policy applies to all Employees, Elected Members, Committees, Directorates, Services, Partners and contractual third parties and agents of the DataTech Solutions. It stipulates their duties and responsibilities for the effective management of disposal of records, in order to comply with the policy and legislative, regulatory, financial and best practice requirements.

2.2 The policy applies to the disposal of all records, in all mediums, for all security classifications, whether retention is governed by legislation, statute, best practice or business need.

3 Definition

This document defines the framework for policy, practice and procedure to ensure the effective disposal and security of all information held by DataTech Solutions.

3.1 Destruction

Destruction can be defined as:

"[The] process of eliminating or deleting records, beyond any possible reconstruction"[1]

ISO 15489-1 states:[2]

- Destruction should always be authorised
- Records subject to pending or actual litigation or investigation should not be destroyed, even if the retention period has expired
- All backup copies, security copies, preservation copies and duplicate copies of all records authorised for destruction should be destroyed at the same point time or as soon as practical afterwards

Effective destruction at the end of the retention period ensures that office and server space are not used and that costs associated with the storage and maintenance of records are no longer incurred.

Principles governing disposal decisions:

- Expiry of applicable retention rationale
- Conclusion of business use
- Whether there is pending or actual litigation or investigation
- Whether the information is subject to a Data Protection or Freedom of Information request
- Corporate, historical or research value
- Access requirements
- Confidentiality and security requirements

Due to public accountability, transparency and the public right of access to certain Council and personal information, it is vital that disposal of records is a managed process and is adequately documented.

3.2 Disposition

Disposition can be defined as:

"[The] range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments"

Disposition may include:

- Physical destruction, overwriting and deletion
- Retention for a further period of time, based on business need
- Transfer to the Records Management Service for off-site storage and management
- Transfer to an alternative storage format e.g. scanning
- Transfer to the Archives and Local Studies Service for permanent preservation

4 Risks

DataTech Solutions recognises that there are risks associated with the destruction of information and records. This policy aims to mitigate the risks.

Examples of the common risks associated with data destruction are:

- Data breach
- Loss
- Theft
- Poor decision making, based on inaccurate or incomplete information
- Inconsistent or poor levels of service
- Insufficient administrative and technical controls
- Malware
- Inappropriate destruction method compromising confidentiality and security
- Lack of accountability and transparency
- Lack of business continuity
- Loss of public reputation
- Loss of corporate memory
- Non-compliance with legislative, regulatory, financial or best practice obligations
- Premature destruction
- Excessive retention
- Inappropriate storage

Non-compliance with this policy could have a significant effect on the efficient operation of the DataTech Solutions and may result in financial loss and an inability to provide necessary services to our customers.

5 Policy Compliance

If any user is found to have breached this policy, they may be subject to DataTech Solutions' disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

6 Revision History

Date of Change	Responsible	Summary of Change
November 2016	Yasteel Singh	Document created