©(ORGANISATION NAME)

DATA PROTECTION AND ENCRYPTION POLICY

Subject: Data Protection and Encryption Management Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 13	Authorised by:
Effective Date: June, 2024	Version 1.0	Next Review:

Author	Signature	Date
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this

document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

CONTENTS

1.0 INTRODUCTION

The purpose of this policy is to ensure data protection and privacy for internally classified data/documents as well as contractual clauses with clients, customers, vendors and other third parties. It establishes standards of compliance with global and domestic data privacy laws. This policy applies to all personal data being processed regardless of its storage location (e.g., on an employee's own device) and regardless of the data subject.

Reference	Description of Risk
SAFETag	Encryption Protection of BYOD & Office Devices
SAFETag	Password Management & Security of BYOD & Office Devices
SAFETag	Protection of Sensitive Data

1.1 OBJECTIVE

The objective of the policy is to

- Provide guidance on handling classified data and documents.

- Comply with the data protection law and ensure best practice.
- Protect the Organisation from risks of personal data breaches and other breaches of data protection law.

1.2 DATA AND APPLICATION CLASSIFICATION

The level/degree of protection accorded to data and application should be proportionate to the classification accorded to the data/application.

1.2.1 DATA CLASSIFICATION

SN	Classification	Description
1	Public Data	This type of data is freely accessible to all employees and the public. It can be freely used, reused, and redistributed without repercussions. Examples are marketing materials, flyers, posters, press releases etc.
2	Internal Data	This type of data is strictly accessible to internal company personnel or internal employees who are granted access. This might include internal memos or other communications, business plans, etc.
3	Confidential Data	Access to confidential data requires specific authorisation and/or clearance. Types of confidential data might include Personally Identifiable Information, Social Security numbers, cardholder data, M&A (Mergers & Acquisitions) documents, and more. Usually, confidential data is protected by laws like HIPAA and the PCI DSS.
4	Restricted Data	Restricted data includes data that, if compromised or accessed without authorisation, could lead to criminal charges and massive legal fines or cause irreparable damage to the company. Examples of restricted data might include proprietary information or research and data protected by state and federal regulations.

1.2.2 APPLICATION CLASSIFICATION

SN	Classification	Description
1	Mission Critical	These are important applications where failure will cause a severe impact to Organisation operations.
2	Business Critical	These are necessary applications where failure will cause significant impact to business operations. These applications usually give competitive advantage and adds to the value of the Organisation.

SN	Classification	Description
3	Business Important	These are applications that are enhancing in nature – "Could have". These applications drive operational efficiency; enhance the way we work and provides automation of processes.
4	Productivity Applications	These are applications that are enticing in nature – "Nice to have". These applications are nice to have and make work easy.

2.0 POLICY STATEMENTS ON DATA PROTECTION

2.1 The Organisation shall define a user access matrix for all its applications, and data access shall be on the principle of least privilege and on a need to know/need to have basis (see appendix 1 for sample).

2.2 The Organisation shall exercise legal ownership of the contents of all files stored on its computer and network systems, as well as all messages transmitted via these systems.

2.3 The Organisation reserves the right to access information stored on any computer system connected to its corporate network without prior notice.

2.4 All user/organisation files on their workstations should be backed-up at periodic intervals (see Disaster Recovery and Backup Policy for the defined frequencies).

2.4 The Organisation shall ensure all applications, systems, and infrastructure used in storing and processing data are adequately secured and protected (see Network Security Policy, Hardening/Baseline standards)

2.5 Data must be classified in different levels of sensitivity classifications with appropriate handling requirements in line with the section 1.2 of this policy.

2.6 The Organisation's entire Internal, Confidential, and Restricted data/information must be protected from disclosure to third parties.

2.7 In order to facilitate the above, the Human Resources department must ensure that the Confidentiality Agreements are signed by all employees, which should be including in the employment contracts or Organization Handbook.

2.8 Prior to sending information to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party must be seen to assure the confidentiality and integrity of the information.

2.9 Staff in custody of the Organisation's sensitive information must take appropriate steps to ensure that these materials are restricted to unauthorised persons.

2.10 Personal data must not be retained longer than required. A defined period should be set for retaining personal data e.g. 6 months, 1 year, 3 years.

3.0 PURPOSE

This policy sets out principles and expectations about when and how encryption of digital information should be stored or transferred.

3.1 SCOPE

This policy applies to all employees, non-permanent workers, consultants, vendors, and partners who directly or indirectly support or use the Organisation's digital information.

3.2 INTRODUCTION TO ENCRYPTION

Encryption, which is a subset of cryptography, is the use of coding to secure computer networks, online systems, and digital data. It is a concept that keeps vital information which is subject to potential data breaches, safe and confidential.

3.3 DATA ENCRYPTION FOR SECURE NETWORK TRANSIT

It is permitted for all the Organisation's employees to use computer systems which would normally and by default use encryption mechanism, to secure data in transit on a communication network. Whenever possible and appropriate, encryption shall be used to support security of remote access connections to the Organisation's network and computing resources.

3.4 REQUIRED USE OF ENCRYPTION

Loss, theft, or unauthorised disclosure of certain information could be detrimental to the Organisation. Such information includes all data that is classified as Confidential and Restricted data.

Data as described above must be encrypted:

3.4.1 Where it is stored on a computing device or any computer storage media which may be exposed to a significant risk of being lost or stolen (Computers used to access remotely stored data or to process locally stored data may create cache files. Depending on the technology in use, persistent and unencrypted cache files may be created.) Any such device when outside the Organisation's network or premises is at significant risk, this includes home computers.

3.4.2 Where data is to be transmitted via a computer network using a mechanism that does not itself incorporate encryption. Depending on the specific technology being used, this could refer to: sending data by email either within or outside the Organisation's network, transferring files offsite, remotely accessing files or web pages. The risk is that unencrypted data in transit may be intercepted.

3.4.2 Where data being processed by the Organisation is subject to an agreement with an external Organisation requiring use of encryption, the agreed handling procedures, encryption technologies and standards must be used.

3.5 MANAGEMENT OF ENCRYPTION KEYS

The following procedures for managing encryption keys must be in place:

3.5.1 Manage encryption keys such that an encrypted stored data will neither become unrecoverable nor accessible by an unauthorised person.

3.5.2 Facilitate authorised officers of the Organisation to obtain prompt access to the encrypted information in the case of an emergency or investigation.

3.5.3 Ensure that encryption keys are stored and always communicated securely.

3.5.4 Keep UpToDate records of custodian(s) of all encryption keys relating to important information.

3.5.5 Revoke encryption keys when the custodian(s) leave the Organisation.

3.5.6 Where practical, an unencrypted backup copy of critical Organisation's data should be securely maintained. Critical backup data should be stored where there are appropriate physical security measures in place (e.g. stored on resilient servers in an alarm enabled server room or on backup tapes stored in a fire safe preferably in a different building)

3.5.7 Significant Organisation's business information being communicated electronically should be authenticated using digital signatures; information received without a digital signature should not be relied upon.

4.0 RECOMMENDATIONS/ADVISORY ON ENCRYPTION

Organisations with 1 – 5 Staff	**Organisations with 6 – 20 Staff**	**Organisations with more than 20 Staff**
• The website, Intranet, and all web-based applications being used should be secured. Website protection with cloudflare Web application protection with Fortinet	• The website, Intranet, and all web-based applications being used should be secured. Website protection with cloudflare Web application protection with Fortinet	• The website, Intranet, and all web-based applications being used should be secured. Website protection with cloudflare Web application protection with Fortinet

Organisations with 1 – 5 Staff	Organisations with 6 – 20 Staff	Organisations with more than 20 Staff
• Make use of Microsoft Personal Data Encryption (PDE) on windows Personal Data Encryption (PDE) • Make use of Microsoft bit locker for disc volume encryption and encryption of USB removable storage devices Microsoft BitLocker • Encrypt your personal mobile devices Encrypt Android Devices Encrypt Apple (iOS and iPadOS) Devices	• Make use of Microsoft Personal Data Encryption (PDE) on windows Personal Data Encryption (PDE) • Make use of Microsoft bit locker for disc volume encryption and encryption of USB removable storage devices Microsoft BitLocker • Make use of open source encryption solutions 7-Zip gnupg • Make use of Windows VPN Connectivity for remote Access to Server Microsoft Windows VPN • Encrypt your personal mobile devices Encrypt Android Devices Encrypt Apple (iOS and iPadOS) Devices	• Make use of Microsoft Personal Data Encryption (PDE) on windows Personal Data Encryption (PDE) • Make use of Microsoft bit locker for disc volume encryption and encryption of USB removable storage devices Microsoft BitLocker • Make use of open source encryption solutions 7-Zip gnupg • Make use of enterprise encryption solution Nord Locker Trend Micro • Make use of enterprise email protection software Cisco Secure Email Encryption Service Paubox Email suite • Make use of Windows VPN Connectivity for remote Access to Server Microsoft Windows VPN

Organisations with 1 – 5 Staff	Organisations with 6 – 20 Staff	Organisations with more than 20 Staff
		• Make use of enterprise VPN Connectivity for remote Access to your Organisation Cisco VPN Sonic wall VPN • Encrypt your personal mobile devices Encrypt Android Devices Encrypt Apple (iOS and iPadOS) Devices • Make use of enterprise mobile device management Microsoft Intune

APPENDIX 1

User Access Matrix

- Root Admin
- Administrator
- Accountant
- Inputter
- Reviewer
- Authoriser
- Read Only

PS: Role AA, Role BB, Role CC, Role DD, Role EE are place holders and can be replaced with actual roles

Roles and Permissions Matrix	Root Admin	Administrator	Accountant	Inputter	Reviewer	Authoriser	ReadOnly	RoleAA	RoleBB	RoleCC	RoleDD	RoleEE
Information Technology												
Create/Delete User		X										
Assign Roles		X										
Reset Password		X										
Field Journalist												
Upload Media Content				X	X	X						
Update Media Content				X	X							
Delete Media Content				X								
Supervisory Journalist												
Upload Media Content												
Update Media Content					X	X						
Delete Media Content					X	X						