

Removable Media and Portal Storage Policy

Document Classification	Confidential ☐ Internal ☐ Public ☒
--------------------------------	---

Removable Media and Portal Storage Policy

Table of Contents

1. Definitions	4	
2. Executive Summary	5	
3. Purpose	5	
4. Objectives	5	
5. Removable Media and Portable Storage Policy Introduction	6	
6. Risk Mitigation	6	
7. Application of the Policy	6	
7.1 Restricted Access to Removable Media	6	
7.1.1 Procurement of Removable Media		7
7.1.2 Security of Data		7
7.1 Incident Management	7	
7.2 Third Party Access to Social Path Information	7	
7.3 Disposing of Removable Media and Portable Storage Devices	8	
7.4 User Responsibility	8	
8. Policy Statement	8	
9. Maintenance	8	
10. Scope	8	
11. Acknowledgement of Understanding	9	

Removable Media and Portal Storage Policy

CHANGE CONTROL TABLE

No.	Revision	Status	Date	Author	Description of the change
1.	00.01	New	10/09/2018		Initial Document
2.	00.02	Reviewed	30/10/2018		Review
3.	00.03	Reviewed	09/11/2018		Updated
4.	00.04	Reviewed	15/11/2018		Review
5.	00.05	Reviewed	30/11/2018		Updated
6.	01.00	Released	16/01/2019		Released
7.	01.01	Reviewed	06/08/2021	JR McEndoo	Released
8.			Date		
9.			Date		
10.			Date		

DOCUMENT STATUS

No.	Status	Definition / Description
1.	New	New Document
2.	Reviewed	Document reviewed by Author and Management.
3.	Released	Document checked and released by Management. This document can only be modified if the version number is updated

VERSIONS

No.	Versions take place in two stages. Accepted documents receive the next higher integral version number.	
1.	00.01, 00.02 etc.	Not released versions, with the status "processed".
2.	01.00	First released version with the status "released".
3.	01.01, 01.02 etc.	Versions which supplement the version 01.00 and are "processed"
4.	02.00	Second released versions with the status "released".

Removable Media and Portal Storage Policy

DISTRIBUTION LIST

No.	Company	Name & Surname
1.	Social Path	Jessica Rose McEndoo
2.	Social Path	Charlotte Annie Wilhelm
3.	Social Path	Dorothy Constance Collett
4.	Social Path	Jana Elizabeth Doyle
5.	Social Path	Linda Monica Ceresa-Hall
6.	Connect Digital Mind	Olivia Dawn Bosman
7.	Social Path	Weronika Kinga Lukasiak
8.	Social Path	Lysandra Harding
9.	Qubi Solutions	Willie Cloete
10.	Emile Hay	Emile Hay

1. Definitions

Company:	Refers to Social Path (Pty) Ltd. (Social Path)
Confidential	Highly sensitive or valuable information, both proprietary and personal. Information, which is confidential by law or data if made public or even shared in an uncontrolled way around the Company, could seriously impede the Company's operations and therefore is considered critical to its on-going operations. Such information should not be copied or removed from the Company's operational control without specific authorisation from EXCO.
Employee:	Any person appointed on a company contract of employment, excluding independent contractors and persons employed by temporary employment services.
Internal	Information not approved for general circulation outside the Company where its loss would inconvenience the Company or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Disclosure of such data to anyone outside of the Company requires EXCO authorisation.
Public	Data or information that does not fall under any other classification levels and may be broadly distributed without causing damage to the Company, its employees and stakeholders.
Event	An event is an exception to the normal operation of IT infrastructure, systems, applications or services.
Incident	An incident is an event that violates the Social Path Computing Policy, Information Security Policy; or threatens the confidentiality, integrity, or availability of the Social Path Information Systems / Platforms or Services. "Information Security Incident" in the remainder of this policy and procedure document refers to an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel.

Removable Media and Portal Storage Policy

	Incident management is concerned with intrusion, compromise and misuse of information and information technology resources and mediums, and the availability and continuity of critical information systems and processes.
	An Information Security Incident include, but are not limited to, the following types of scenarios: • Data Loss, Data Corruption or Data Theft, • Unauthorised exposure or leakage of company confidential information or data, • Unauthorised Access Attempts (either failed or successful) to access data, systems, platforms or information storage. • Cyber Attacks including Denial Of Service (DoS), Distributed Denial of Service attacks (DDos), Man in the Middle Attacks, Malware, Spear Fishing, etc. • Changes to information or data or system hardware, firmware, or software characteristics without the Stakeholders' knowledge, instruction, or consent. • Any unauthorised Changes to access permissions or privileges. • Any unauthorised use of any System or Service for the processing, storage or manipulation of data. • Unplanned / Unscheduled System, Service, Platform or Connectivity Outages / Service Disruptions • Severe System Performance or Functional Degradation

2. Executive Summary

This policy forms an integral part of the Social Path Information Security management methodology that aims to enforce governance and accountability for information security management across all of the current and future Social Path owned, operated or supported environments.

3. Purpose

The goal of the Removable Media and Portable Storage Policy is to provide the respective Social Path personnel, subcontractors, partners and associates, guidance in terms of responsible access and usage of these technologies for storing or transporting Social Path data.

4. Objectives

This policy aims to provide adequate guidance in order to govern responsible usage, this guidance aims to prevent any harm to individuals or the organisation and reduce the risk associated with the use of these mediums, to this end, all users and managers of Social Path information and IT systems are expected to:

- Understand their roles in providing the respective clarity and guidance to their respective personnel,
- Report any abuse, or breach of policy immediately to ensure that adequate corrective action can be taken.

This policy and the related Social Path policies and procedures provide a clear and consistent methodology to help to ensure that usage of any ICT related services, solutions or technology is adequately and consistently governed.

5. Removable Media and Portable Storage Policy Introduction

This document states the Removable Media policy for Social Path. The policy establishes the principles and working practices that are to be adhered to by all users in order for Social Path data to be safely stored and transferred on removable media and portable storage devices.

This policy aims to ensure that the use of removable media devices is controlled in order to:

- Minimize the potential for data loss through theft or failure of these devices
- Protect data that is required to be transferred via these mediums by utilising encryption
- Ensuring the security of Social Path data and information.
- Prohibit the disclosure of information as may be necessary by law.
- Minimise inadvertent data loss through data corruption, device failure or device theft or loss.

6. Risk Mitigation

Social Path recognises that there are risks associated with users accessing and handling information in order to conduct official Social Path business.

Information is used throughout the organisation and may be occasionally, selectively, shared with external organisations and partners where required and approved by Social Path management, in aid of delivering a defined solution or service.

Securing this data is of paramount importance – particularly in relation to protecting data in line with the requirements of Social Path clients. Any loss of the ability to access information or interference with its integrity has a significant effect on the efficient operation of Social Path. It is therefore mandated, for the continued operation of Social Path, that the confidentiality, integrity, and availability of all information systems be maintained at the appropriate level.

This policy aims to mitigate the following risks:

- Disclosure of information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential legal action against Social Path as a result of information loss or misuse.
- Social Path reputational damage as a result of information loss or misuse.

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

7. Application of the Policy

7.1 Restricted Access to Removable Media

The Social Path policy prohibits the use of all removable media devices. The use of removable media devices is only to be considered for approval if a valid business case for its use is presented, including the required measures to protect this usage.

Requests for access to, and use of, removable media devices must be made to Jessica Rose McEndoo, Director of Social Path and reasons for their use must be provided, in writing.

Removable Media and Portal Storage Policy

Should access to, and use of, removable media devices be approved the following conditions apply and must be adhered to at all times.

7.1.1 Procurement of Removable Media

All removable media devices and any associated equipment and software must only be purchased and installed by IT Services. Non Social Path owned removable media devices may not be used to store or transport any Social Path information.

The only equipment and media that should be used to connect to Social Path equipment or the Social Path network is equipment and media that has been purchased by Social Path and approved for use by Jessica Rose McEndoo, Director of Social Path.

7.1.2 Security of Data

Data that is only stored in one location, or of which there is only one copy, in one format is at much higher risk of becoming inaccessible or corrupted through loss, destruction or malfunction of the respective IT equipment.

The principles for protecting data therefore consider that critical data is required to be stored in more than one location, geographically separate from each other at a distance that ensures that a disaster or destructive incident is less likely to impact both instances of the respective data. This principle applied to removable media implies that there be a primary copy, a backup copy, and then when mandated and approved, an additional copy for transportation

Based upon these principles, removable media may not be the only data storage location utilised for data storage that relate to Social Path purposes, primary copies, backup copies and cloud backups are required before data is copied to these mediums for the defined purpose.

From a data migration perspective, the principle implies that Copies of any data stored on removable media must also remain on the source system until the data is successfully transferred to another system and verified as correct.

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whilst in their care or under their control.

NOTE | All data stored on removable media devices must be encrypted.

7.1 Incident Management

- It is the duty of all users to immediately report any actual or suspected breaches in information security to Social Path management.
- It is the duty of all Social Path employees, contractors or partners to report any actual or suspected breaches in information security to Social Path Management
- Any misuse or irresponsible actions that affect business data, or any loss of data, must be immediately reported as a security incident to Social Path management.

7.2 Third Party Access to Social Path Information

No third party (external contractors, partners, agents, the public or non-employee parties) may receive data or extract information from the Social Path' s network, information stores or IT equipment without explicit approval. Should third

Removable Media and Portal Storage Policy

parties be allowed access to Social Path information then all the considerations of this policy apply to their storing and transferring of this data.

7.3 Disposing of Removable Media and Portable Storage Devices

All removable media devices that are no longer required, reached end of life or become damaged, must be returned to Social Path management for secure disposal.

7.4 User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), external hard disk drives and recordable CDs/DVDs:

- Any removable media device used in connection with Social Path equipment or the network or to hold information used to conduct official business must only be purchased and installed by Social Path IT.
- Any removable media device that has not been supplied by Social Path IT may not be used.
- All data stored on removable media devices must be encrypted where possible.
- Virus and malware checking software must be used when the removable media device is connected to a machine.
- Only data that is authorised and necessary to be transferred should be saved on to the removable media device.
- Data that has been deleted can still be retrieved.
- Removable media devices must not be used for archiving or storing records as an alternative to other storage equipment.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage.
- Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

8. Policy Statement

Social Path will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information technology and/or the associated digital assets (data) within the custody of Social Path.

9. Maintenance

- The Social Path Executive and Information Security Personnel are responsible for the maintenance and revision of this Policy.
- This policy, and all related appendices, are reviewed as deemed appropriate or required, but no less frequently than every 12 months.
- This Policy review is undertaken by the Social Path Executive and Senior Management team.

10. Scope

This policy and procedures apply to the Platforms, Information Systems, Data, Services and Networks leveraged or utilised by Social Path and their respective service delivery partners and associates, including any person or device who gains access to these systems or data. The policy therefore applies to all Partners and Employees of Social Path, contractual third parties and representatives of Social Path who use Social Path IT services and solutions, or have access to, or custody of, customer information or Social Path proprietary information.

All Partners and Employees of Social Path, contractual third parties and representatives must therefore understand and adopt this policy and are responsible for ensuring the safety and security of Social Path systems and the information that

Removable Media and Portal Storage Policy

they use or manipulate. All users have a role to play and a contribution to make in order to ensure safe and secure use of the defined Social Path systems, services, platforms and associated technology, and the information that these environments contain.

11. Acknowledgement of Understanding

I have read and agree to comply with the terms of this policy governing the use of Removable Media and Portable Storage. I understand that violation of this policy may result in disciplinary action, including possible termination and civil and criminal penalties.

Printed Name:

Role / Designation

Signature:

Date: