

Remote and Flexible Work Style Policy

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

Remote and Flexible Work Style Policy

Table of Contents

1. Definitions	4
2. Executive Summary	5
3. Purpose	5
4. Objectives	5
5. Remote and Flexible Work Style Policy Introduction	6
6. Definition	6
7. Risks	6
8. Application of the Policy	6
9. User Responsibility	7
10. Remote and Mobile Working Arrangements	7
11. Access Controls	8
12. Anti-Virus Protection and Workstation Health Management	8
13. Policy Compliance	8
14. Policy Statement	8
15. Maintenance	8
16. Scope	9
17. Acknowledgement of Understanding	9

Remote and Flexible Work Style 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".

Remote and Flexible Work Style 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

Remote and Flexible Work Style Policy

	caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. 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 Remote and Flexible Style Policy is to provide the respective Social Path personnel, subcontractors, partners and associates, guidance in terms of remote and flexible work styles. Social Path provides users with the facilities, capabilities and opportunities to work remotely, or follow flexible work style, output based principles as appropriate. Social Path hereby ensures that all users who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities, as well as the individual's responsibility and accountability on terms of output based, working styles.

4. Objectives

This policy aims to provide adequate guidance in order to govern remote and flexible work styles, this guidance aims to prevent any harm to individuals or the organisation and reduce the risk associated with remote and flexible work styles, 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.

Remote and Flexible Work Style Policy

5. Remote and Flexible Work Style Policy Introduction

Our Employee remote work policy outlines our guidelines for employees who work from locations other than the Social Path offices. Social Path wants to ensure that both employees and our organisation will benefit from this type of arrangement as this provides a clear, output based, mature, working arrangement.

Portable computing devices are provided to assist users to conduct official Social Path business efficiently and effectively, and from any location that the user is either based at, if more productive from, or that aligns to providing a better environment with flexibility to allow the respective users to deliver their best work.

The Social Path corporate assets and associated equipment, and any information stored on these computing devices, should be recognised as valuable organisational information assets and should therefore be safeguarded appropriately.

6. Definition

This policy is applicable to any User that makes use of portable computing devices. This policy applies to all users' use of Social Path IT equipment and personal IT equipment, which is used to conduct official Social Path business, away from Social Path premises (i.e. working remotely, working from home).

Portable computing devices include, but are not limited to, the following:

- Laptop computers.
- Tablet PCs.
- Mobile phones.
- Any internet connected technology that can access any Social Path services, systems or productivity applications.

7. Risks

Social Path recognises that there are risks associated with users accessing and handling information in order to conduct official Social Path business. Mobile technology and connectivity services make portable computing devices productive to employees regardless of their location, as long as they are internet connected. This implies that employees, contractors and partners of Social Path are equipped to work from any location; these locations however may be public spaces, the employees home, or hotel accommodation. These locations provide limited security in terms of protecting these physical devices from theft. These "out of office" locations therefore mandate extra precautions be taken by all respective Users in order to maintain the required level of control across these devices.

This policy aims to mitigate the following risks:

- Increased risk of equipment damage, loss or theft.
- Accidental or deliberate overlooking by unauthorised individuals.
- Unauthorised introduction of malicious software and viruses.
- Potential legal action against Social Path or individuals 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.

8. Application of the Policy

- All IT equipment (including portable computer devices) provided to users is the property of Social Path.
- These Social Path assets must be returned upon the request of Social Path.
- Access for IT Services staff of Social Path shall be provided under strict control in order to allow essential maintenance security work or maintenance of the defined Social Path Systems and Services.
- All IT equipment is supplied and deployed for the respective Social Path Users by Social Path ICT Service staff.
- Only Hardware and software provided by Social Path is permitted to be utilised on these devices and licence compliance is mandated.
- Antimalware, Antivirus software may never be tampered with or removed

Remote and Flexible Work Style Policy

- Users are mandated to utilise secure remote working technology, Social Path provides adequate capabilities for either secure web access, or virtual private network connections and the related, secured technology to equip the Social Path workforce.

9. User Responsibility

It is the user's responsibility to ensure that the following points are adhered to at all times:

- Users must take due care and attention of portable computer devices when moving between home and another business site.
- Users are not permitted to install or update any software on a Social Path owned portable computer device.
- Users are not permitted to change the configuration of any Social Path owned portable computer device.
- Users will not install any hardware on any Social Path owned portable computer device, unless authorised by Social Path IT department.
- Users are not permitted to prevent the immediate installation and maintenance of Social Path installed Anti-Virus updates.
- Users must inform the IT department if any Social Path owned portable computer device depicts a message relating to configuration changes.
- Business critical data should be stored on suitable Social Path secured document or data storage services.
- Any and All faults must be reported to the IT Department/Management.
- Users must not remove or deface any asset registration number.
- User requests for upgrades of hardware or software must be approved before any procurement may commence.
- The IT equipment is supplied for the staff members' sole use.
- The user must ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, Social Path may recover the costs of repair.
- The user should seek advice from Social Path before taking any Social Path supplied IT equipment outside South Africa. The equipment may not be covered by Social Path's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel.
- Social Path may at any time, and without notice, request a software and hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.
- Any user who chooses to undertake work at home or remotely in relation to their official duties using their own IT equipment must understand that they are not permitted to hold any database or carry out any processing of information relating to Social Path, its employees, or customers.
- Under no circumstances should Personal or information be emailed to a private non-Social Path email address. For further information, please refer to the Email Policy.

10. Remote and Mobile Working Arrangements

- Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.
- Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. For home working it is recommended that the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use.
- Users must ensure that access / authentication tokens and personal identification numbers are kept in a separate location to the portable computer device at all times.
- All removable media devices and paper documentation must also not be stored with the portable computer device.
- Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use.

Remote and Flexible Work Style Policy

- Documents should be collected from printers as soon as they are produced and not left where they can be casually read.

11. Access Controls

It is essential that access to all Social Path information is controlled. Access is controlled through a multi-faceted approach that starts with the physical security of the devices. Physical controls, such as locking the home office or locking the computer's keyboard. Credential and complex passwords with multi factor or two factor authentication is applied to ensure that the users access credentials are secured and monitored. Additional controls including secure connectivity mediums, disk encryption and data encryption should be applied where applicable,

- All computer devices should be switched off, logged off, or locked when left unattended, even if only for a few minutes. All Mobile devices should be protected by a pin, passphrase and where equipped, with biometrics.
- All Social Path data on portable computer devices should, where possible, be encrypted.
- An SSL/TLS or IPsec VPN must be configured to allow remote users access to Social Path systems if connecting over Public Networks.
- Dual-factor authentication must be used when accessing the Social Path network and information systems (including Outlook Web Access) remotely via both Social Path owned, and non-Social Path owned equipment
- Access to the Internet from Social Path owned IT equipment, should only be allowed via onward connection to Social Path staff provided perimeter security firewalls and not directly to the Internet.

12. Anti-Virus Protection and Workstation Health Management

Social Path IT deploys remote management agents to each Social Path workstation, these agents manage and monitor the health of the computing device, provide proactive alerting back to the IT staff, and ensures that the Antivirus Software is fully managed and updated at all times, this capability also manages Windows and 3rd party patches and updates to maintain these assets without user intervention.

13. Policy Compliance

If any user breaches this policy, they may be subject to Social Path 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).

14. 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.

15. 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.

Remote and Flexible Work Style Policy

16. 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 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.

17. Acknowledgement of Understanding

I have read and agree to comply with the terms of this policy governing the use of The Company's Remote and Flexible Work Styles. 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: