Computer Network and Internet Access Policy

Document Classification	**Confidential**	☐
	Internal	☐
	Public	☒

Table of Contents

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	08/06/2021	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”.

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.

	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 the current and future Social Path owned, operated or supported environments.

3. Purpose

The goal of the Computer Network and Internet Access Policy is to provide the respective Social Path personnel, subcontractors, partners, and associates, guidance in terms of responsible access and usage of the Social Path networking and internet access facilities, and the respective Social Path ICT assets utilised to perform any ICT related function across these mediums.

4. Objectives

This policy aims to provide adequate guidance 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. Computer Network and Internet Access Policy Introduction

The Internet is a constantly growing worldwide network of computers and servers that contain millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material.

Users are further cautioned that it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Employees and users (herein referred to as “Users,” or “User”) accessing the Internet do so at their own risk and understand and agree that Social Path (herein referred to as "Company," or “The Company”) is not responsible for material viewed or downloaded by users from the Internet. To minimize these risks, your use of the Internet at The Company is governed by this Policy.

6. Permitted Use of Internet and Company computer network

The computer network is the property of The Company and is to be used for legitimate business purposes. Users are provided access to the computer network to assist them in the performance of their jobs. Additionally, certain Users may also be provided with access to the Internet through the computer network. All Users have a responsibility to use The Company's computer resources and the Internet in a professional, lawful, and ethical manner. Abuse of the computer network or the Internet, may result in disciplinary action, including possible termination, and civil and/or criminal liability.

7. Computer Network Use Limitations

7.1.1. Prohibited Activities.

Without prior written permission from The Company, The Company's computer network may not be used to disseminate, view, or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, Trojan horse programs, etc.) or any other unauthorized materials. Occasional limited appropriate personal use of the computer is permitted if such use does not a) interfere with the User's or any other employee's job performance; b) have an undue effect on the computer or company network's performance; c) or violate any other policies, provisions, guidelines, or standards of this agreement or any other of the Company. Further, at all times users are responsible for the professional, ethical and lawful use of the computer system. Personal use of the computer is a privilege that may be revoked at any time.

7.1.2. Illegal copying.

Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the company.

7.1.3. Communication of trade secrets.

Unless expressly authorized to do so, Users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to The Company. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties under State and Federal Economic Espionage laws with a duty not to Waste or Damage Computer Resources.

7.1.4. Accessing the internet.

To ensure security, avoid the spread of viruses & malware, and to maintain The Company’s Internet Usage Policies or Acceptable Use Policies, employees may only access the Internet through a computer attached to The Company's network and approved Internet firewall or other security device(s). Bypassing The Company's computer network security by accessing the Internet directly by personal connections such as (but not limited to) Cellular Networks, Wimax, modems, or proxy avoidance techniques or by any other means is strictly prohibited.

7.1.5. Frivolous use.

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, Users must not deliberately perform acts that

waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups or other social media, uploading, or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

7.1.6. Virus detection.

Files obtained from sources outside The Company, including disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage The Company's computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Company sources, without first scanning the material with Company-approved virus checking software. If you suspect that a virus has been introduced into The Company's network, notify The Company immediately.

7.1.7. No Expectation of Privacy

Employees are provided with computers and Internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, post, send or receive using the company's computer equipment. The computer network is the property of The Company and may be used only for Company purposes.

7.1.8. Waiver of privacy rights.

User expressly waives any right of privacy in anything they create, store, post, send or receive using the company's computer equipment or Internet access. User consents to allow company personnel access to and review of all materials created, stored, sent, or received by User through any Company network or Internet connection.

7.1.9. Monitoring of computer and Internet usage.

The Company has the right to monitor and log and archive any and all aspects of its computer system including, but not limited to, monitoring Internet sites visited by Users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users via Email, IM & Chat & Social Networking.

7.1.10. Blocking Sites with Inappropriate Content

The Company has the right to utilize hardware and software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

7.1.11. Blocking Sites with Non-productive Content.

The Company has the right to utilize hardware and software that makes it possible to identify and block access to Internet sites containing non-work-related content such as (but not limited to) Drug Abuse; Hacking; Illegal or Unethical; Discrimination; Violence; Proxy Avoidance; Plagiarism; Child Abuse; Alternative Beliefs; Adult Materials; Advocacy Organizations; Gambling; Extremist Groups; Nudity and Risqué; Pornography; Tasteless; Weapons; Sexual Content; Sex Education; Alcohol; Tobacco; Lingerie and Swimsuit; Sports; Hunting; War Games; Online Gaming; Freeware and Software Downloads; File Sharing and Offsite Storage; Streaming Media; Peer-to-peer File Sharing; Internet Radio or TV; Internet Telephony; Online Shopping; Malicious Websites; Phishing; SPAM; Advertising; Brokerage and Trading; Web-Based Personal Email; Entertainment; Arts and Culture; Education; Health and Wellness; Job Search; Medicine; News and Media; Social Networking; Political Organizations; Reference; Religion; Travel; Personal Vehicles; Dynamic Content; Folklore; Web Chat; Instant Messaging or IM; Newsgroups and Message Boards; Digital Postcards; Education; Real Estate; Restaurant or Dining; Personal Websites or Blogs; Content Servers; Domain Parking; Personal Privacy; Finance and Banking; Search Engines and Portals; Government and Legal Organizations; Web Hosting; Secure Sites; or Web-based Applications.

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 they use or manipulate. All users have a role to play and a contribution to make to ensure that 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 The Company's computer network. 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: _____