Security and Privacy Awareness Training 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	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”.

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

3. Purpose

The goal of the Security and Privacy Awareness and Training Policy is to provide the respective Social Path personnel, subcontractors, partners and associates, guidance in terms compliance with the Social Path Information Security mandates and Controls. This policy aims to provide the baseline for ongoing cyber and information technology awareness training and the related controls.

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. Security and Privacy Awareness and Training Policy Introduction

Security and privacy awareness and training is an important aspect in protecting the Confidentiality, Integrity, and Availability (CIA) of sensitive information. Employees are the first line of defence and must be made aware of the security risks associated with the work performed at Social Path.

6. Purpose

Social Path understands that people are often the biggest threat (intentionally or inadvertently) to the security of sensitive information. As such, all users of information systems must be made aware of the security risks associated with their activities and of the applicable federal and agency requirements related to the security of Social Path information systems performing work on behalf of, or for Social Path's Clients.

Those with significant security responsibilities must be adequately trained to carry out their assigned information security-related duties and responsibilities.

7. Scope

This policy applies to all Social Path employees and contractors and anyone else needing access to Social Path information and its systems.

8. Policy

All employees, contractors, and anyone accessing Social Path information systems must understand how to protect the CIA of information and information systems.

Social Path will ensure that all employees and contractors are given security and privacy awareness training during the new hire process and before accessing any Social Path systems. This training reflects common security and privacy awareness specific to Social Path environment including, but not limited to, physical access, restricted areas, potential incidents, how to report incidents, laptop best practices, and how to spot a phishing scam.

In addition to the initial security training provided in the new hire orientation, all employees must take a security and privacy awareness course and pass the test within 30 days of hire.

This course and test are provided and tracked by the management of Social Path.

Social Path will provide ongoing training through the Security and Privacy Awareness and Training Team activities or SPAT. The SPAT provides information on a monthly basis on selected topics. An initial SPAT Chat presentation is conducted at the beginning of the month to give information, demonstrations, and general Q&A for all attendees. The SPAT also provides information via posters in designated areas throughout the facility and weekly articles posted on the internal intranet page.

Social Path will also conduct annual refresher training for all employees and anytime there are significant changes to the environment. This will be administered via the LMS and tracked for completeness and passing grade to show adequate understanding of the material.

This policy will be reviewed on an annual basis or whenever there are significant changes to the environment.

9. Management Commitment

Social Path Senior Management will commit to the development of a security and privacy awareness program allocating staff and resources. The Information Security Manager will have access to both the compliance and training departments for completion and update of training materials and tracking results.

10. Roles and Responsibilities

All employees and contractors are responsible for understanding and following all security related policies and procedures, and asking their manager or Security Officer for clarification if needed. Managers are responsible for ensuring all employees complete required security training. The management is responsible for enrolling all employees in first time and annual security training and tracking results.

The Security Manager is responsible for:

- Maintaining ongoing SPAT team activities
- Updating annual security training materials
- Conducting new hire training
- Ensuring all employees understand and following security related policies and procedures

11. Coordination among Organisational Entities

Security is everybody's business. As security tends to cross departmental and organizational boundaries, Social Path employees and contractors will work together to ensure that required security controls are in place, are maintained, and comply with the policy described in this document. Security concerns, security incidents, or suspected/confirmed vulnerabilities will be shared with appropriate personnel in the organization so that the vulnerability can be remediated (or mitigated with compensating security controls) and we can ensure that similar vulnerabilities in other systems or processes can be addressed.

12. Compliance

Compliance with the policy defined in this document is mandatory. Failure to comply with Social Path Information Security Policies may result in disciplinary actions up to and including termination of employment. Employees may also be held personally liable for any violations of this policy. Failure to comply with Social Path Information Security Policies may result in termination of contracts for contractors, partners, consultants, and other entities. Legal actions may also be taken for violations of applicable regulations and laws. Systems that do not satisfy Social Path Information Security Policy requirements may be prevented from being allowed to operate as a production system.

13. References

This policy establishes mandatory requirements and assigns roles and responsibilities to facilitate the implementation of the Social Path Security Awareness and Training Policy. The policy contains formal, documented policy statements and language designed to facilitate and guide the implementation of the policy, procedures, and controls. Formal, documented security procedures exist as separate documents titled AT-1 through AT-3.

This policy is consistent with the following guidance:

- C.F.R. Part 5 Subpart C (5 C.F.R 930.301)
- NIST SP 800-12 Introduction to Computer Security: The NIST Handbook
- NIST SP 800-16 Information Security Training Requirements: A Role- and Performance-Based Model
- NIST SP 800-37 Rev. 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-50 Building an Information Technology Security Awareness and Training Program
- NIST SP 800-100 Information Security Handbook: A Guide for Managers

14. Security Awareness (AT-1)

Social Path requires that all users complete a security awareness and training course (or courses as applicable) prior to being granted access to Social Path corporate or client systems.

Users are provided basic security awareness training as part of initial training for new users, as well as when required by system changes. All users must take refresher training at least annually.

Employees or contractors shall acknowledge having received the security awareness training either in writing or electronically as part of the training course completion (the current process involves sending copies of course completion certificates to the Social Path CISO).

The Social Path CISO maintains, and stores completed security awareness and training evidence artefacts (certificates) for users. Security awareness and training course completion artefacts (certificates) will be provided to the Agency ISSO or Security Steward upon request.

15. Security Training (AT-2)

Social Path must provide role-based, security-related training before authorizing access to the system or performing assigned duties, as well as when required by a system change or changes in personnel roles.

Social Path must provide security training materials that address the procedures and activities necessary to fulfil the defined roles and responsibilities for information system security.

Social Path must provide role-based security-related training to all appropriate personnel at least once every three years. Appropriate personnel includes but is not limited to System Administrators, Database Administrators, Network Engineers, Security Analysts, and the CISO.

The employee or consultant shall acknowledge having received the role-based training either in writing or electronically as part of the training course completion.

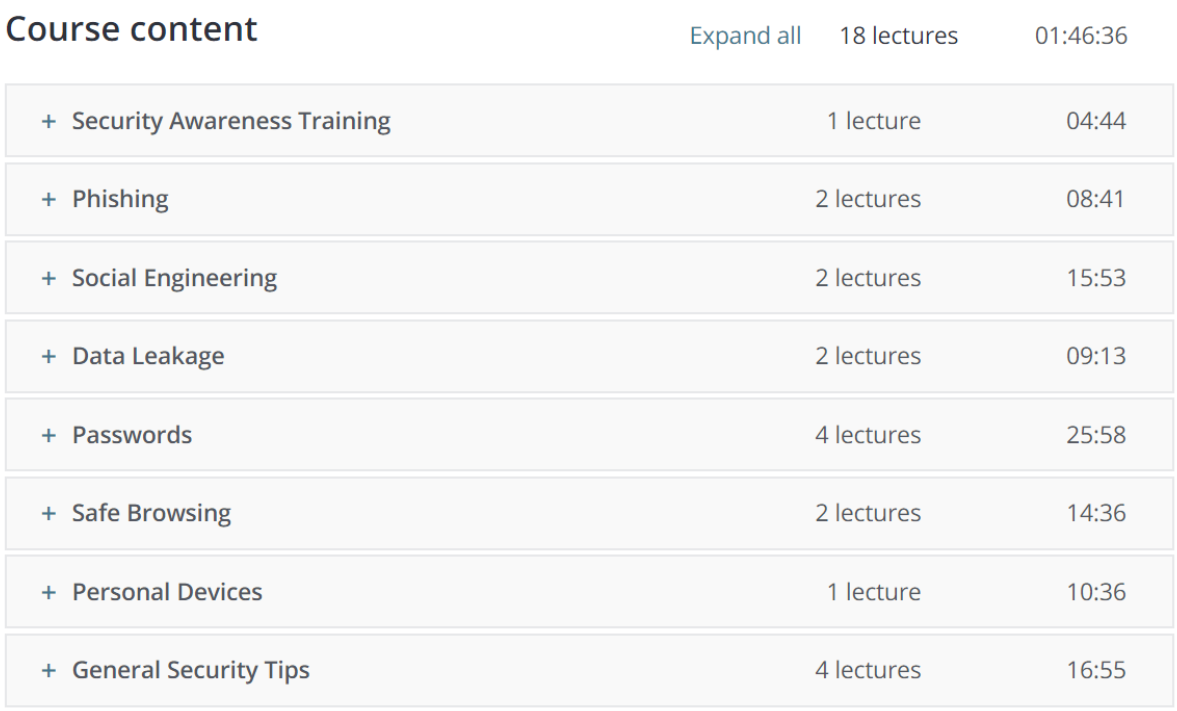
16. Security Training Records (AT-3)

Social Path must create and disseminate to users the security training documents.

The Social Path CISO must ensure activities for monitoring and documenting basic security awareness training, as well as role-based training, are conducted.

Employees and contractors must provide evidence of successful course completion (certificates) to the Social Path CISO. All security training records must be stored for at least 5 years.

17. FY20 Awareness Training: UDEMY Curriculum



Course content

Expand all 18 lectures 01:46:36

+ Security Awareness Training	1 lecture	04:44
+ Phishing	2 lectures	08:41
+ Social Engineering	2 lectures	15:53
+ Data Leakage	2 lectures	09:13
+ Passwords	4 lectures	25:58
+ Safe Browsing	2 lectures	14:36
+ Personal Devices	1 lecture	10:36
+ General Security Tips	4 lectures	16:55

https://www.udemy.com/security-awareness-training/?utm_source=adwords-learn&utm_medium=udemyads&utm_campaign=NEW-AW-PROS-PROF-ROW-DSA-1-EN-EURO_._ci__._sl_ENG_._vi_PROF_._sd_All_._la_EN_._&utm_content=deal4584&utm_term=_._ag_60674389651_._ad_311050879105_._de_c_._dm__._pl__._ti_aud-299743148827:dsa-304639795863_._li_1028645_._pd__._&gclid=Cj0KCQjwxMjnBRCtARIsAGwWnBNAKjsLG3xC-B4t6el65gUK07zjcklBmpzCM59sH9XezXwqF6IqbO4aAoBwEALw_wcB

18. 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.

19. 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.

20. 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 associated, 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.

21. 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: _____