**Faculty of Business and Management Sciences**

**Ethics Informed Consent Form**

**CONSENT TO PARTICIPATE IN A RESEARCH STUDY**

**Category of Participants (tick as appropriate):**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Staff/Workers* | *X* | *Teachers* |  | *Parents* |  | *Lecturers* |  | *Students* |  |
| *Other (specify)* |  |  | | | | | | | |

You are kindly invited to participate in a research study being conducted by Zandiswa Nkandi from the Cape Peninsula University of Technology. The findings of this study will contribute towards the *Master’s thesis*.

The tittle of the research study being conducted is “***An awareness model for the use of information technology security policies in the petroleum retail sector in South Africa”*** andthe main objective of this study is to develop an awareness model for the use of IT security compliance policies in the petroleum retail sector. This research is important to assist the petroleum retail sector protect its information from cybersecurity threats and realise its full potential in terms of IT security policy compliance.

Your participation in this research study is voluntary and no compensation will be provided for your involvement. Participants' names and organisation names will not be disclosed or published as part of this study; anonymity and confidentiality will be maintained.

The method of data collection will consist of a questionnaire, which will take approximately 10 to 15 minutes to complete.

Kindly complete the table below before participating in the research.

|  |  |  |
| --- | --- | --- |
| Tick the appropriate column with an X | | |
| Statement | Yes | No |
| 1. I understand the purpose of the research. |  |  |
| 1. I understand what the research requires of me. |  |  |
| 1. I volunteer to take part in the research. |  |  |
| 1. I know that I can withdraw at any time. |  |  |
| 1. I understand that there will not be any form of discrimination against me as a result of my participation or non-participation. |  |  |

Please only provide signature on the block provided below and return the signed document at your earliest convenience. You will be given a copy of this form on request.

|  |  |
| --- | --- |
|  |  |
| Signature of participant: | Date: |

Please complete the questionnaire below by placing a CROSS (X) in the appropriate box.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **INTERVIEW QUESTIONNAIRE** | | | | |  |
| 1. The password policy is available and easily accessible to me. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. Utilizing strong and not easy to guess passwords is essential to protect me from cyber-attacks. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. I frequently utilize a Virtual Private Network (VPN) in my day-to-day activities. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. VPN is easy to use, in my opinion. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. My work computer provides the capability to connect and utilize a personal USB storage device. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. I utilize social media platforms, including WhatsApp, Telegram, Facebook, and Instagram, as channels for sharing organizational data. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. Within the past six months, I have participated in online or in-person training sessions that focused on cybersecurity. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. Within my organization, I have access to a training platform that offers cybersecurity-related training topics. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. I have the capability to use my personal computer to gain access to organizational data and applications. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. I have the capability to use my work computer to access personal data and applications. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. I use my personal device to access organizational sensitive or personal information (POPIA / confidential). | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. Occasionally, I use public **spaces** (airplane/airport, hotel, restaurant) to access confidential data or information while traveling or working remotely. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. Occasionally, I connect to public **Wi-Fi** (airport, hotel, restaurant) to access confidential data or information while traveling or working remotely. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. I regularly share organisational information or data with partners, contractors, customers, suppliers, or vendors. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. I understand what is expected of me from the cybersecurity perspective. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. I know where to find information about cybersecurity. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. I know where to report cybersecurity related questions. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. I understand security capabilities around my home network / Wi-Fi. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. I understand my responsibility / obligation to log all security related incidents. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. Cybercriminals or scammers have previously attempted to carry out a cyberattack against my work computer. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. My work computer has been successfully hacked or exploited in the past. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. The computer provided by my organization grants me access to various social media platforms. | Strongly Agree | Agree | Disagree | Strongly Disagree | I don’t know |
| 1. What is the frequency at which your organization provides cybersecurity training? | Yearly | Quarterly | Monthly | Never | I don’t know |
| 1. What do you do if you suspect an email has been phished or if you spot any non-compliance concerns? | Report to line manager | Report via Phish alert | Report to Service Desk | I do nothing | I don’t know |
| 1. Which MFA or two-factor authentication method do you find best to use usage? | Authenticator App | SMS code | Phone call | I don’t know | I don’t know |
| 1. In terms of cybersecurity policies and awareness, what is your level of understanding? | I understand fully | I understand | Neutral | I don’t understand | I don’t know |
| 1. Is there anything in particular that you think contributes to employees falling victim of cyber-attack within an organization?   Please provide details in the space provided below: | | | | | |
|  | | | | | |