social development

Department:
Social Development
PROVINCE OF KWAZULU-NATAL

STANDARD OPERATING PROCEDURE ON INFORMATION SECURITY

TABLE OF CONTENT

1. INTRODUCTION

The Standard Operating Procedure (SOP) on Information Security seeks to provide steps and standardized procedure in the management of Information Security landscape within the Department.

2. PURPOSE

The purpose of this SOP is to manage and maintain confidential information and its integrity.

3. SCOPE OF APPLICABILITY

These procedures are applicable to all employees, visitors and contractors in the Department.

4. OPERATIONS MANAGEMENT

Operating Procedures

The following sets out the operating procedures to ensure the protection of information and secure operations of networks.

4.1.1 Computer user account control

4.1.1 Business Unit Manager:

4.1.1.1 segregates duties and areas of responsibility in the system to reduce opportunities for unauthorized access.

4.1.1.2 Prevents unintentional modification or misuse of departmental information assets.

4.1.1.3 Grants users access to only designated processing environment.

4.1.1.4 Provides information of users to ICT for implementation.

4.1.1.5 New request for access to the network must follow new user account creation procedures, refer to ANNEXURE "A"

4.1.2 The System Administrator:

4.1.2.1 Provides access rights to the user.

4.1.2.2 Review user access rights on quarterly bases

4.1.2.3 Invokes access rights when the environment changes.

4.1.3 The user performs access to only designated processing environment

4.2.1 Access to network

4.2.1.1 System Administrator:

4.2.1.1.1 Manages and monitor access to the network in accordance with Departmental policy. records and review authorization levels for all systems within the Business Unit at least every six months.

4.2.1.1.2 Addresses irregularities as a matter of priority

4.3.1 User Account registration and de-registration

4.3.1.1 System Administrator:

4.3.1.1.1 registers and de-registers user accounts

4.3.1.1.2 revoking access to all information systems and services.

4.3.1.1.3 perform quarterly review of information on user account in liaison with responsibility Managers to identify and disable redundant user accounts

4.3.2.1 Business Unit Managers

furnish records to Information and Communication Technology (ICT) Directorate regarding all officials who are exiting the department to terminate access on the respective system(s).

4.4.1 Privileged access

4.4.1.1 Business Unit

4.4.1.2 Request temporary access to ICT for third party access.

4.4.1.3 Keep a record of all roles and individuals with Privilege User Access.

4.5.1. Password security

End-user:

4.5.1.1 Keeps password secret and exclusive.

4.5.1.2 Changes password at first log on.

4.5.1.3 Changes password every 28 days, after which he/she will be prompted by the system to change the password.

4.5.1.4 Creates strong password consisting of at least alphanumeric characters. For example, strong password is a combination of:

- Special characters = # @ $ % & *
- Capital letters = A B C
- Numeric = 1 2 3 4
- Small letters = a b c d

4.5.1.5 Changes password that is believed to be compromised immediately and report the matter to a supervisor and ICT Helpdesk

System must be configured to:

4.5.1.6 Only allow password with a minimum length of eight (8) characters.

4.5.1.7 Lock out users after 3 incorrect attempts.

4.5.1.8 Prevent users from using the passwords they have used for the past 12 months.

4.6.1. Mobile device security

4.6.1.1 IT Operations Manager requests authority from Head of Department to configure Mobile devices for remote disabling, erasure and lockout.

4.7.1. Disposal of media

ICT Directorate:

4.7.1.1 Erase data on the equipment.

4.7.1.2 Sanitize the devices containing sensitive information before being destroyed

4.8.1. Cryptographic control

4.8.1.1 IT Operations Manager encrypts all data classified as sensitive using professional cryptographic tool and network compatible methodologies.

4.9.1. Physical and environmental security

IT Personnel

4.9.1.1 Controls IT Server rooms and only authorized personnel are allowed access.

4.9.1.2 Records date, time of entry and departure of visitors.

4.9.1.3 Supervise the entry of visitors in the server rooms unless their access has been previously approved.

4.10.1 Operations security

The IT Operations Manager responsible for:

4.10.1.1 ensuring security features, service levels, management requirements of all network services are identified and included in any network services agreement, whether these services are provided in-house or outsourced.

4.10.1.2 Protecting the integrity of software and information assets. ICT equipment must be maintained with the most recent anti-virus signature updates via a centrally managed console.

4.10.1.3 ensuring anti-virus updates are automatically distributed, with no manual intervention required by the end user or IT staff.

4.10.1.4 ensuring IT Specialists monitor the anti-virus console daily and fix the exceptions promptly.

4.10.1.5 Reviewing the anti-virus console reports quarterly.

4.10.1.6 Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures must be implemented.

The IT Operations Manager responsible for the development and review of the following security-oriented configuration items:

4.10.1.7 IT security charter.

4.10.1.8 IT security Plan.

4.10.1.9 IT security Tactical plans.

4.10.1.10 IT infrastructure plan.

4.10.1.11 Configuration Item Security baselines.

4.10.1.12 Data classification model.

4.10.1.13 Technical standards.

4.11.1. Incident management

The IT Operations Manager:

4.11.1.1 takes necessary steps on a temporary basis, such as removing systems from operation revoking system accesses

4.11.1.2 removing involved personnel from the network or systems

4.11.1.3 manages and stop security breach.

IT Operations Manager administer established plans and processes that are communicated within the department. Processes should include: -

4.11.1.4 Procedures for monitoring, detecting, analyzing and reporting of information security incidents

4.11.1.5 Procedures for logging incident management activities. Incident Report.

4.11.1.6 Procedures for handling forensic evidence.

4.11.1.7 Procedures for assessment of and decisions on information security vulnerabilities.

4.11.1.8 Authorization of delegated roles for handling of information security incidents. E.g. contact with authorities.

4.12.1. Information security awareness and training

ICT Directorate:

4.12.1.1 Conduct information security awareness workshops once every year.

4.12.1.2 Deliver workshops in two (2) sessions per district and head office, targeting all computer users within the Department.

14.12.1.3 Request an information security awareness slot presentation in the Induction workshop for newly appointed officials in the Department.

5. MONITORING, EVALUATION AND REVIEW

5.1 The Information and Communication Technology Directorate is responsible for communicating the provisions of this Standard Operating Procedure.

5.2 This Standard Operating Procedure will be monitored, evaluated and reviewed every three years or when the need arises on annual basis.

6. EFFECTIVE DATE

This Standard Operating Procedure will be effective on the date of approval.

7. TITLE OF THE STANDARD OPERATING PROCEDURE

This Standard Operating Procedure shall be called Standard Operating Procedure on Information Security.

8. STANDARD OPERATING PROCEDURE APPROVAL

This Standard Operating Procedure is approved on the 05th day of November in the year 2018.

MS NG KHANYILE
HEAD OF DEPARTMENT
DEPARTMENT OF SOCIAL DEVELOPMENT

social development

Department:
Social Development
PROVINCE OF KWAZULU-NATAL

ANNEXURE "A"

INFORMATION TECHNOLOGY USER ACCOUNT MANAGEMENT FORM

Please "tick"on the relevant box

New User Account / Re-registration		Termination		Change of Access / Move Account		Email Access		Internet Access		Password Reset	

FULL NAME/S		**SURNAME**		
PERSAL NO.		**TITLE**		
LOCATION / OFFICE		**SECTION / BUSINESS UNIT**		
TEL NO.		**JOB TITLE**		
FAX NO.		**FUNCTION ALLOCATION**	Access to Shared Folder	
			Administrator Rights	

REQUESTING USER NAME/S		**SURNAME**	
SIGNATURE		**DATE**	

APPROVED / NOT APPROVED

SUPERVISOR NAME/S		**SURNAME**	
SIGNATURE		**DATE**	

FOR OFFICIAL USE ONLY

REQUEST ATTENDED BY		**DATE**	
SIGNATURE			

social development

Department:
Social Development
PROVINCE OF KWAZULU-NATAL

ANNEXURE "B"

KWAZULU-NATAL DEPARTMENT OF SOCIAL DEVELOPMENT

COMPUTER USER DECLARATION FORM

Access to information technology resources and services has been granted to me, as a tool, for perfoming job duties and responsibilities for my Directorate. I have read and agree to abide by the Information Technology Policy and procedures which govern my use of this service.

Usage Statement

I will refrain from monopolising systems, overloading networks with excessive data, or wasting computer time, connect time, disk soace, printer paper, or other information technology resource.

I will report to management any observations of attempted security violations or illegal activities.

I will report to management if I receive or obtain information to which I am not entilted.

By signing this agreement, I certify that I understand and accept responsibility for adhering to the policies, procedures, and additional Departmental terms and conditions listed above. I also acknowledge my understanding that any misuse on my part may result in disciplinary action including, but not limited to termination of my access privileges.

THE EMPLOYEE

Name_____Signature_____Date:_____

Persal No:_____

ACCESS TO DEPARTMENTAL I.T. FACILITIES AUTHORISED

Head of Directorate:_____**Signature**_____**Date:**_____