Policy on Information Security

Status:	Approved
Custodian:	Directorate: Information Technology
Date approved:	2013-10-02
Implementation date:	2013-10-03
Decision number:	SAQA 09101/13
Due for review:	2016-10-02
File Number:	

Table of contents

This policy, its rules and procedures replace all previous policies and Guidelines on Information Security

1. Preamble

Information is an asset that, like other important business assets, has value to an organisation and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

The purpose of information security is to protect the South African Qualifications Authority (SAQA) from, or minimise the impact of, security incidents. Information Security has four basic components:

1.1 confidentiality/privacy – protecting assets from unauthorised disclosure, access, use or intelligible interception

1.2 integrity/safety – retaining the completeness and correctness of assets during use, in transit or while stored, and maintaining the health and safety of employees and visitors at work

1.3 availability – ensuring that assets are available to authorised individuals when required

1.4 verifiability – ensuring that logs and other records are kept so that the integrity of information can be tested and breaches of policy traced

The successful implementation of the Policy on Information Security (hereafter "the Policy") cannot be achieved without the cooperation of all employees. It is crucial, therefore, that all are aware of, and fully comply with, the general security requirements outlined in the Policy and also those specific to their office and function. This includes existing policies such as the Policy on Electronic Communications.

2. PURPOSE

The purpose of this policy is to clearly state SAQA's approach to Information Security, the relevant rules that apply to Information Security and the responsibilities of various role-players at SAQA that could impact on Information Security.

3. OWNERSHIP

The Directorate: Information Technology is the custodian of this policy.

4 SCOPE OF PRACTISE

4.1 The Policy applies to all the information assets of SAQA. All employees of SAQA shall be bound by the Policy. Contractors and employees who are or may be in a position to affect the security of SAQA assets shall be required to acknowledge their acceptance of all or relevant passages of the Policy.

4.2 The Policy sets out the responsibilities of SAQA employees. It does not create any basis for one employee to become legally liable to another.

4.3 This policy should be read in conjunction with the Policy on Electronic Communications.

5 RELATED PROCEDURES

5.1 The procedures contained in section 10 of this policy.

5.2 This policy should be read in conjunction with the Policy on Electronic Communications.

6. TYPE OF POLICY

This policy and its related procedures are of a strategic nature.

7 Policy on Information Security

It is the policy of SAQA that information owned by the organisation shall be managed:

7.1 to ensure that the business can survive threats to its information management and technology environment

7.2 to prevent loss or damage to SAQA, any particular individual or external organisation

7.3 to minimise the extent of loss or damage arising from a security breach or exposure

7.4 to ensure that adequate resources are applied to implement an effective security programme

7.5 to ensure all employees are informed of their responsibilities and obligations with respect to security

8. Definitions

8.1 **Assets:** this term should be interpreted in its widest context and includes (but is not limited to) the following assets of SAQA:

- employees (including SAQA Board members, all permanent and part-time employees of SAQA)
- manager (including any person responsible for a particular line function)
- software (including application software, operating system software, development tools, utilities)
- information (including data, printed documentation)
- services (including air-conditioning, communications)
- premises, equipment and fixed assets

8.2 **System:** any set of equipment or procedures, the activation of which causes work to be done or an output to be delivered. This includes, but is not limited to, computer equipment and manual procedures.

8.3 **Hard media:** any physical material on which information is recorded including, but not limited to, paper, magnetic media and plastic

8.4 **Security incident:** a breach of security or non-compliance with the Policy or its associated procedures, or where the confidentiality, integrity or availability of a SAQA asset has been compromised

8.5 **Serious security incident:** one whereby, in the opinion of the Chief Executive Officer, SAQA could be exposed to:

- loss of reputation
- loss of client confidence
- loss of significant amounts of money or other assets
- significant damage to facilities or employees
- loss from legal action
- loss of business continuity

9. RESPONSIBILITIES

9.1 Executive Office

The Deputy Chief Executive Officer is responsible for managing the Policy and granting sanction for specific and necessary deviation from the Policy.

9.2 Directorate: Information Technology

The responsibilities of the IT Directorate include:

- advising the I&IT Committee on the sufficiency and effectiveness of its Policy on Information Security and drafting any necessary amendments for the I&IT Committee
- ensuring the implementation of the Policy and its consequential procedures, including its associated administrative and monitoring procedures
- monitoring the sufficiency and effectiveness of those security procedures

9.3 Managers

- Managers of sections are responsible for implementing the Policy within the operational procedures of their areas.
- Access rights for users are to be requested by the director by completing the SAQA User Account Management Form (See Annexure A this policy)
- Directors have responsibility for initiating any disciplinary measures against employees who fail to comply with the Policy.

9.4 Staff

- Each employee must understand and comply with the Policy.
- Each employee is responsible for reporting security incidents of which he or she is aware.

9.5 Incident reporting

- All serious security incidents must be reported to the Director: InformationTechnology or his or her representative, who is responsible for investigating the incident and following appropriate procedures.
- Serious security-related incidents must be thoroughly investigated in order to assess the risk associated with the breach, enable remedial action to be taken and evaluate the effectiveness of the current security policies and procedures**.**

9.6 Disciplinary procedure

- Any breach of the Policy or associated policies may result in SAQA taking disciplinary action against an employee.
- Details of the disciplinary process are in line with the general policy and can be obtained from the Directorate: Human Resources**.**

10. Procedures

10.1 Confidentiality

There must be adequate controls to ensure that information and the information derived from it are only disclosed to authorised users.

10.2 Integrity

10.2.1 There must be adequate controls to ensure completeness and accuracy during the capture, storage, processing and presentation of electronic information.

10.2.2 There must be adequate measures to ensure that the computer system is able to resist compromise of its controls and that electronic information can only be accessed through established routes.

10.2.3 Workstations, personal computers and other terminal equipment must not be left unattended while logged into any application giving access to information not in the public domain.

10.2.4 All computers, whether connected to the network or not, must have installed and activated the appropriate anti-virus software as provided by the IT Directorate and this shall at all times be kept at the latest release level.

10.2.5 All computer software systems shall be upgraded to the latest patch levels as these become available. It is the responsibility of the IT Directorate to make these available. The only exception shall be application packages where the IT Directorate technical staff may, for operational reasons, have to test such patches and schedule suitable downtime.

10.3 Availability

10.3.1 There must be adequate measures to ensure the recovery or replacement of electronic information and resumption of business activities within an acceptable timeframe after any damage or disruption to service.

10.3.2 An IT Disaster Recovery Plan shall be maintained to ensure that the IT Directorate is able to resume operation in a timely manner following serious disruption to the availability of systems.

10.3.3 The IT Disaster Recovery Plan must be reviewed and updated as new systems or business processes are developed.

10.3.4 The IT Disaster Recovery Plan must also be tested on a regular basis.

10.4 Authentication

10.4.1 All users of computer systems shall be uniquely identified to the system being accessed.

10.4.2 All users shall possess private tokens, such as user identification (IDs) and passwords, which are used by the computer system to authenticate their identity.

10.4.3 Adequate measures must be in place to ensure users are forced to change their passwords every 40 days.

10.4.4 Users must not share their private tokens with others.

10.4.5 Users must not use one of their seven previously used passwords.

10.4.6 Users must select passwords that are robust as users shall be accountable for all actions performed under their identifiers.

10.5 Access Control

10.5.1 Access to electronic information, hard media and other assets shall be granted only to authenticated users.

10.5.2 Authority to access electronic information, hard media and other assets must be granted and revoked by the responsible manager.

10.6 Awareness

10.6.1 It is the responsibility of all managers to ensure that regular communication relating to security issues is distributed.

10.6.2 It is the responsibility of the IT Directorate to monitor developments in security and to disseminate relevant information throughout SAQA.

10.7 Information Security Officer

The IT Director will appoint an Information Security Officer, whose responsibilities will include (but not be limited to):

- Advising Management and the I&IT Committee on Information Security issues
- Information Security Risk Assessments
- Developing Information Security Procedures
- Managing Information Security Policies
- Information Security Planning
- Handling Information Security Incidents

- Reviewing Information Security Problems
- Ensuring that security logs and audit trials are produced and reviewed regularly.
- The Information Security Officer will work closely with the IT Director to perform his or her tasks
- SAQA has outsourced the Database Administration of its Oracle Database (used by the NLRD) and its MS SQL Databases, used by a variety of applications. The Service Level Agreement with the company that performs these duties includes regular reports with regard to logons to the databases and these reports must be reviewed by the Information Security Officer.
- To ensure proper segregation of duties, the information security officer may appoint another IT Staff member to review the user access on servers that the Information Security Officer needs to access by virtue of his/her role other than that of the Information Security Officer. Such an appointed staff member will submit reports on the user access directly to the IT Director.

10.8 Testing

The Policy shall be tested for overall compliance at least once annually. This annual review shall be coordinated by the Director: Information Technology and shall utilise internal and external expertise where appropriate.

10.9 Electronic Hard media

Information recorded on hard media shall at all times be stored in a secure environment with appropriate access control, access logging and fire protection.

10.10 Physical security

All information-processing areas used to house information resources supporting mission-critical applications must be protected by physical controls. All SAQA's servers are housed in the server room, which is appropriately controlled for the size and complexity of the operations. Storage and processing capacity should be negotiated with the Director: IT.

Physical access to the server room is restricted to authorised personnel. Authorised visitors are supervised and their entry and exit recorded in a log.

Designated employees shall wear a key-card/ID badge, which allows physical access to appropriate areas, as designated by the Director: IT.

10.11 End-user workstations (general and physical)

All computer users are responsible for their own workstations and should ensure that the workstations are physically secure by

- locking the office before leaving the premises

- ensuring Notebook computers are fastened down
- ensuring the safety of loan notebook computers

End-user workstations used in sensitive or critical tasks must have adequate physical (locked offices) controls.

All microcomputer end-user workstations must have updated virus protection software installed and enabled.

Users must execute the "Lock Workstation" function whenever they leave their immediate work area, unless the workstation is running a password-protected screensaver or is in a "locked-down" environment.

All other end-user workstations shall employ similar security procedures.

10.12 Logon IDs and passwords

Logon IDs and passwords must control access to all information resources except for those with public access, such as the SAQA's website and searchable databases.

Passwords should be at least eight characters in length and be a mixture of alpha, numeric and special characters.

Passwords should be changed, at a minimum, every 40 days. System administrators shall check user password histories to ensure none of the last seven passwords are repeated.

Users should be encouraged to change their password if they suspect it has been compromised.

User accounts will be locked after 5 unsuccessful attempts to log on.

10.13 Password selection

Computer crackers are extremely sophisticated. Instead of typing each password by hand, crackers use personal computers to make phone calls to try the passwords, automatically redialling when they become disconnected. Instead of trying every combination of letters, crackers use hit lists of common passwords such as *wizard* or *demo*. Even a modest home computer with a good password-guessing program can try thousands of passwords in less than a day. Some hit lists used by crackers contain several hundred thousand words. Therefore, any password that anybody might guess is a bad choice.

What are popular passwords? Your name, your spouse's name, your parents' name, your pet’s name. Other bad passwords are these names spelled backwards or followed by a single digit. Short passwords are also bad; because there are fewer of them, they are more easily guessed. Especially bad are "magic words" from computer games. Other bad choices include phone numbers, characters from favourite movies or books, local landmark names, favourite drinks or famous people.

Some rules for choosing a good password are:

- Use both uppercase and lowercase letters if the computer system considers an uppercase letter to be different from a lowercase letter when the password is entered.
- Include digits and punctuation characters as well as letters.
- Choose something easily remembered so it doesn't have to be written down.
- Use at least eight characters with a combination of numeric, alpha and special characters.
- It should be easy to type quickly so someone watching the keyboard cannot follow what is typed.
- Use two short words and combine them with a special character or a number, like robot4me or eye-con2.
- Put together an acronym that has special meaning to you.
- End of one word is the beginning of another word.

A standard admonishment is "never write down a password." You should not write your password on your desk calendar, on a Post-It label attached to your computer terminal, or on the pull-out drawer of your desk.

A password you memorise is more secure than the same password written down, simply because there is less opportunity for other people to learn it. But a password that must be written down (in order to be remembered) is quite likely a password that is not going to be guessed easily. If you write a password in your wallet, the chances of somebody who steals your wallet using the password to break into your computer account are remote. If you must write down a password, follow a few precautions:

- Do not identify the password as being a password.
- Do not include the name of the account or the phone number of the computer on the same piece of paper.
- Do not attach the password to a terminal, keyboard or any part of a computer.
- Mix in some "noise" characters or scramble the written version of the password in a way that you remember, but make the written version different from the real password.

- Never record a password on-line and never send a password to another person via electronic mail.

10.14 Internet usage

- Be familiar with your system's vulnerabilities.
- Security solutions should effectively balance risk exposure, expense, functionality and usability.
- Users and processes should only be granted the minimum access sufficient to perform their tasks.
- All services, protocols and ports that are not required should not be enabled.
- All entry points should be hardened..
- Users may not use software such as PC Anywhere to dial straight into their SAQA workstation. Users must use the network validation process.
- Users must assume all trading partners' networks are insecure and take preventative action.
- The IT directorate shall perform periodic integrity checks on SAQA's information technology resources to detect intrusions.
- Users should use the secure shell protocol instead of telnet for inbound external access to resources.
- Upon instruction from the HR directorate, the IT directorate should revoke the password/access and identifications of former users. The IT directorate should also review access permissions for employees who change roles.
- The IT directorate shall educate all personnel on the nature, purpose and importance of security measures.
- The IT directorate shall ensure the security of the connection and the data stream, using virtual private networking (VPN) protocols for users coming into and accessing resources from outside the firewall.
- The IT Directorate shall provide filters for viruses, spam and worms to ensure the protection of SAQA's information and infrastructure.
- Warning banners shall be placed on all access points. The banner shall warn authorised and unauthorised users:
    - about the proper use of the system
    - that the system may be monitored to detect improper use and other illicit activity
    - that there is no expectation of privacy while using the system
    - of the penalties for non-compliance

10.15 Backup guidelines

National Learners' Record Database (NLRD)

- An incremental daily backup of the database shall be performed. This includes a daily export of the database.
- A full off-line backup of the database and system files shall be performed every Saturday,
- Weekly backup of the database export shall be copied to DVD and stored off-site for 12 months.

All SQL Databases

- An incremental daily backup of the database shall be performed. This includes a daily export of the database.
- A full off-line backup of the database and system files shall be performed every Saturday

Mailboxes

- A full backup of the mailbox shall be performed every Saturday.
- An incremental backup of the mailboxes shall be performed Monday to Thursday.
- Archiving shall take place in line with SAQA's Policy on Records Management.

Electronic filing system

- A full backup of the Electronic Filing System shall be performed every Saturday.
- An incremental backup of the system shall be performed Monday to Thursday.
- Archiving shall take place in line with SAQA's Policy on Records Management.

User files stored on File Servers

- A full backup of the user files shall be performed every Saturday.
- An incremental backup of user files shall be performed Monday to Thursday.
- It is the responsibility of the user to save on the fileserver the files he or she wishes to have backed up.
- Only the user shall have the right to read and alter the documents in the folder allocated to the user.
- Each user shall keep one copy only of the same document on the server (i.e. e-mail, file attachments and other important documentation).

10.16 Termination of employment

- The HR Directorate must inform the IT Directorate of any resignations and the date on which these become effective.

- On termination the IT directorate shall save all the user's documents in the directorate subfolder. Designated people within the user's directorate shall have access to the subfolders.
- The documents shall be archived in line with SAQA's Policy on Records Management.
- The mailbox of the employee who has resigned shall be made available to a designated employee for a period of 90 days.

10.17 Loading of private software

- Only in exceptional cases shall private software be allowed on any business machine.
- Loading of private software must be approved by the line manager and IT director.
- If the private software interferes in any way with existing business software, the private software shall be removed immediately.

11. Documents

11.1 Policy on Electronic Communications

ANNEXURE A

USER ACCOUNT MANAGEMENT FORM

CREATION		**REVIEW**		**DATE: ……/……/20….**

Name:	
Surname:	
Directorate:	
Applications:	Accpac | NLRD | DFQEAS | Other:……
List Access Rights:	
Access Rights granted by:	
List Shared Folder Access:	
Folder Access granted by:	
Workstation:	Desktop ☐ Note Book ☐
If not a director:	Approval for Note book (DCEO):
TELEPHONE:	SAQA ☐ LOCAL ☐ NATIONAL ☐ INTERNATIONAL ☐
	Approval for International (DCEO):

LINE MANAGER	**DIRECTOR**	**IT DIRECTOR**
NAME:	**NAME:**	**NAME:**
TITLE:	**TITLE:**	**TITLE:**
DATE:	**DATE:**	**DATE:**
SIGNATURE:	**SIGNATURE:**	**SIGNATURE:**