SHEQ SYSTEM

This document is the property of Necsa and shall not be used, reproduced, transmitted or disclosed without prior written permission

DOC NO.	SHEQ-INS-0320	REV.	1	PAGE	1	OF	3
TITLE	**INFORMATION SECURITY: REQUIREMENTS FOR THIRD PARTY ACCESS**						

1 PURPOSE AND SCOPE

This procedure governs the manner in which an application for Third Party access to Necsa's classified information or information systems is to be made, considered, granted or declined and the contractual requirements which must be concluded in writing prior to granting Third Party access.

The procedure applies to any person not full time employed and subjected to the Necsa conditions of employment that needs to access Necsa's information and information systems. The access must be specific applicable systems must be indicated on the form.

The Information Security Officer or persons designated by the Information Security Officer to grant and facilitate access to Necsa's information or information systems to a Third Party.

2 REFERENCE

2.1 This document complies with the guidelines established in:

- ISO/IEC 17799:2005 Security Policy

2.2 This document refers to the following:

- SHEQ-INS-0310 Information Security: Acceptable Use Requirements
- SHEQ-INS-0321 Information Security: Requirements for Remote Access
- SHEQ-INS-8921 Necsa's Requirements for the Security Clearance of Items (Deliveries and Removals)
- SHEQ-INS-8929 Classification of Information
- SHEQ-INS-8930 Security Requirements for the Control of Classified Information
- SHEQ-INS-8950 Requirements for Security Screening

	NAME	SIGNATURE	DATE
PREPARED	AJ Nel ISO		
CHECKED	MJ Mostert CSO		
CHECKED	L Russell SM: SIM		
ACCEPTED	F Mashilo SM: SS		
ACCEPTED	I E Steyn SM: SHEQD		
ACCEPTED	R Masango GE: NC		
APPROVED	RM Adam CEO		
DISTRIBUTION	This document is available on SHAREPOINT – SHEQ SYSTEM DOCUMENTS SHEQ Records		

2.3 This document prescribes the use and implementation of:

- SHEQ-FRM-0310 Third Party or Remote Access or Mobile Computing Application and Agreement (Exhibit 1 of SHEQ-INS-0310))

3 REVISION HISTORY

- Revision 0 – 2007/05/28 – First Issue - This document was established in close collaboration with the members of the ISC by M.W. Heyink, Necsa's consultant for Information Security
- Revision 1 – Minor language, changes, removal of duplicate policy statements, rectifying of abbreviations and changes in responsibilities to reflect best practice (A J Nel)

4 DEFINITIONS AND ABBREVIATIONS

4.1 Third Party, being a person not employed by Necsa or subject to Necsa's permanent employment conditions.

4.2 The following abbreviations are used in this document:

EMP Event Management Process
ISC Information Security Committee;
ISO Information Security Officer.

5 PRINCIPLES

This information security procedure is based on the following principles:

i) Access to classified information will only be approved if the applicant's security competency (vetting/screening) is at the same level as the information accessed.
ii) Access to classified information or information systems by a Third Party shall be granted strictly on a "need to know" and a "need to access" basis.
iii) Access shall only be available to persons authorised by Necsa to have access to the information;
iv) Information remains confidential to authorised persons only and not be disclosed to persons not authorised by the owner to have access to the information; and
v) Information shall be protected against a compromise of its integrity arising from unauthorised or accidental amendment.
vi) Access can only be recommended by full time Necsa line Management that is subjected to the Necsa conditions of employment.

6 APPLICATION AND AGREEMENT

6.1 The manager of the group requiring a Third Party be granted access to Necsa's information or information systems shall:

i) Ensure that security screening to the required level is performed on a third party prior to approval by Security Services as prescribed in SHEQ-INS-8930 and -8950;
ii) Ensure that an Access Application and Agreement form (SHEQ-FRM-0310) is properly and fully completed and signed by the Applicant (the Third Party) and line Manager before submission to the ISO;

6.2 Within a reasonable period of receipt of the application and subject to the urgency of the application the ISO shall consider the application and inform the manager of his decision to either accept or decline the application subject to conditions which the ISO may require.

7 REMOTE ACCESS

Any Third Party that requires remote access to Necsa's classified information or its information systems shall comply with the provisions of the Requirements for Remote Access (SHEQ-INS-0321), and agree to the provisions governing the granting of remote access.

8 ENFORCEMENT OF PROCEDURE

8.1 The requirements of this procedure shall have the force of a contractual agreement between Necsa and the third party users.

8.2 This procedure shall be enforced by the ISO in conjunction with the line Management.

8.3 If a Third Party breaches the terms of the Contractual Agreement or is suspected by the ISO of any activity which may compromise Necsa's information security in any manner, the ISO may immediately and without notice to the Third Party revoke the Third Party's access to Necsa's classified information and information systems and may require that the Third Party be removed from Necsa's premises.

8.4 Suspected or actual compromises of information shall be registered as events in the EMP – see part 21 of SHEQ-INS-8930.

8.5 The third party may not claim any compensation or loss of income that may arise as a result of the revoking of access of the third party.

9 RECORDS

The following records shall be kept:

DESCRIPTION	RETENTION PERIOD	BY WHOM
Completed Access Application and Agreement forms (Exhibit 1 of SHEQ-INS-0310)	5 years after end of contract	ISO/ SS record custodian
Records of any compromise or suspected compromise under the access granted to a Third Party (shall at least be recorded in the EMP)	Unlimited5 years after end of contract	ISO/ SS record custodian
Records of revocation/termination of Third Party's access (also to be recorded in classified information register)	Unlimited5 years after end of contract	ISO/ SS record custodian

Note: The recording of information accessed by the Third Party is prescribed in SHEQ-INS-8930 – parts 5 and 6).

1 PURPOSE AND SCOPE

Necsa is the owner and custodian of information (in all its forms) and information systems critical to its business. The purpose of this procedure is to regulate the proper use of Necsa's information and information systems in accordance with requirements and that appropriate safeguards be established, implemented and enforced. This document prescribes general requirements and shall be implemented in conjunction with the documents listed in 2.2.

This procedure applies to all users of information and information systems owned, or under the control of Necsa. It shall also apply to the use of information communication or storage devices (including cellular telephones) used to gain access to Necsa's information or information systems or to store information owned by Necsa.

2 REFERENCES

2.1 This document complies with the requirements of:

- ISO/IEC 17799:2005 – Security Policy
- Section 86 of the Electronic Communications and Transactions Act 2002 (Act 25 of 2002)

2.2 This document refers to the following:

SHEQ-INS-0306	Information Security: Glossary
SHEQ-INS-0315	Information Security: Requirements for Physical and Electronical Access
SHEQ-INS-0320	Information Security: Requirements for Third Party Access
SHEQ-INS-0321	Information Security: Requirements for Remote Access
SHEQ-INS-0322	Information Security: Requirements for Mobile Computing and Communication
SHEQ-INS-8921	Necsa's Requirements for the Security Clearance of Items (Deliveries and Removals)
SHEQ-INS-8929	Classification of Information
SHEQ-INS-8930	Security Requirements for the Control of Classified Information
SHEQ-INS-8950	Requirements for Security Screening

2.2 This document prescribes the use and implementation of:

- Third Party or Remote Access or Mobile Computing Application and Agreement (Exhibit 1)

	NAME	SIGNATURE	DATE
PREPARED	M W Heyink		
CHECKED	A C van der Bijl		
APPROVED	A C van der Bijl		
DISTRIBUTION	As per latest revision of distribution list SHEQ-LST-0001 SHEQ Records		

3 REVISION HISTORY

- Revision 0 – First issue – This document was established in close collaboration with the members of the Information Security Committee (ISC) by M W Heyink, Necsa's consultant for information security.

4 DEFINITIONS AND ABBREVIATIONS

4.1 Unless inconsistent with the context, the expressions set out in this procedure will have the meanings assigned to them in the glossary of terms. (See SHEQ-INS-0306.)

4.2 The following abbreviations are used in the document:

User ID	User identification
ISC	Information Security Committee
ISO	Information Security Officer
CEO	Chief Executive Officer

5 PRINCIPLES

This information security procedure is based on the following principles:

i) Information to be **available** to persons authorised by the owner to have access to the information;
ii) Information shall remain **confidential** to authorised persons and not be disclosed to persons not authorised by the owner and ISO to have access to the information; and
iii) Information shall be **protected** from unauthorised or accidental amendment.

6 RESPONSIBILITIES

6.1 Necsa has established an ISC charged with the responsibility of implementing, monitoring and enforcing generally accepted information security practices within Necsa and reporting on the information security status of Necsa.

6.2 The ISC shall determine the requirements necessary to ensure that appropriate safeguards and controls are established to protect the classified information and information systems owned by, or under the control of Necsa.

6.3 The appointed ISO shall be responsible for implementing the information security procedures and for establishing and implementing appropriate standards and guidelines necessary to support the procedures established by the ISC.

6.4 The ISC shall be responsible for directing efforts to ensure the continuous and ongoing education and awareness of users, owners of classified information and administrators of the information systems as to their information security responsibilities.

7 PHYSICAL ACCESS TO INFORMATION

7.1 The ISC shall direct that appropriate physical security access restrictions and protections of Necsa's classified information and information systems are established and maintained and in accordance with the requirements of SHEQ-INS-0315 and -0830. The ISO shall ensure that persons responsible for physical security of information are designated.

This document is the property of Necsa and shall not be used, reproduced, transmitted or disclosed without prior written permission

7.2 Physical access shall be restricted to persons properly authorised to have access to any classified information or components of the information system.

7.3 All visitors (including employees, agents or consultants employed by Necsa) requiring ad hoc or temporary access to classified information or areas containing such information or information systems shall be authorised by the ISO, in conjunction with the relevant manager.

7.4 All visitors who have received authorisation to gain physical access to Necsa classified information or its information systems shall be accompanied by a person responsible for such information, areas or systems, designated to receive and accompany the visitors.

7.5 The authorisation of visitors to areas that house information or information system components and the information or system accessed shall be recorded and these records maintained by the ISO.

7.6 The ISO, or persons designated by the ISO to do so, shall be responsible for implementing and maintaining the necessary physical barriers or protections and monitoring their continuous use.

8 OWNERSHIP AND CLASSIFICATION OF INFORMATION

8.1 All information owned or controlled by Necsa shall be assigned an owner, who shall determine who shall be entitled to gain access to the information. The author of a document shall be viewed as the "owner" unless otherwise determined.

8.2 All information shall be deemed to be not classified (i.e. open), but "for use internally within Necsa," unless it has been classified in accordance with SHEQ-INS-8929.

8.3 Any person who intentionally accesses, or interferes with, or attempts to access, information to which they are not authorised, may be subject to disciplinary action or any other legal remedies available to Necsa.

8.4 Unauthorised access to, interception of, or interference with information, constitutes a criminal offence as addressed in Section 86 of the Electronic Communications and Transactions Act (Act 25 of 2002). Where appropriate the ISC may, in addition to any disciplinary action which may be taken in terms of 8.3, recommend the institution of criminal proceedings, to protect the classified information and information systems under Necsa's control.

9 ACCESS TO INFORMATION

9.1 The ISO shall ensure that control of logical access to Necsa classified information and information systems are implemented. Access shall be recorded in accordance with the requirements of SHEQ-INS-0830.

9.2 Persons designed by the ISO shall, in accordance with the direction of the ISC and the information owner, grant and/or revoke access to Necsa's classified information or information systems.

9.3 Access to Necsa information systems shall be protected by the allocation of user identities to authorised users and the selection of authentication measures by the users. The authentication measures shall conform to the requirements of procedures and standards established by the ISO who shall communicate the requirements to users from time to time.

9.4 If directed by the ISC access to classified information may require additional or alternative security measures than user identification and password control. Users shall take whatever steps may be

directed in procedures or standards established by the ISO to achieve the levels of security directed by the ISC.

9.5 Authentication measures (e.g. passwords and/or challenge phrases) are confidential and users shall take all reasonable steps to safeguard their confidentiality.

9.6 Under no circumstances shall a user disclose his or her password, or challenge phrase, to another person or record the password in a manner that will allow it to be accessed and used by another person. Administrators of information systems can bypass authentication measures under certain circumstances.

9.7 No user shall request or use the password of another user. If a user is requested to disclose his or her password, regardless of the authority or the requestor, they shall immediately report this to the ISO. A request for another user's password shall be regarded as a serious breach of this procedure and may be subject to disciplinary action.

9.8 Any access to an information system under Necsa's control and all activity on the information system using the user identity assigned to, and the password selected by a user, shall be attributed to the user and the onus of proving the contrary shall be on the user.

9.9 Any user, who suspects that his or her password, or that of any other user, has become known to a person other than the authorised user or that the authentication of the persons identity has been compromised in any way, shall immediately report this suspicion to the ISO.

9.10 Failure by a user to employ all reasonable steps to safeguard the confidentiality of a password selected by the user, may lead to immediate suspension of access by the user to Necsa's information and/or information systems and disciplinary action as may be appropriate.

9.11 Users shall:

i) ensure, if information to which they are not authorised is accessed, that it is not distributed to any other person;
ii) report, to the ISO, the fact they have gained access to information which they are not authorised to have access to; and
iii) report, to the ISO, any unauthorised access by a third party to Necsa classified information or information systems that comes to their knowledge.

9.12 Any user, who has accessed Necsa classified information or information systems, shall ensure that before he or she leaves the location, or the computer or device used for the access, he or she use all reasonable means necessary, or as directed by the ISO, to prevent an unauthorised person from gaining access to it.

10 THIRD PARTY ACCESS

Save for persons employed by Necsa, no person shall be granted access to classified information or information systems under the control of Necsa, without the prior written authorisation of the ISO **and** such person having entered into a written agreement (see Exhibit 1) governing the conditions of such access as addressed in the Requirements for Third Party Access (SHEQ-INS-0320).

This document is the property of Necsa and shall not be used, reproduced, transmitted or disclosed without prior written permission

11 REMOTE ACCESS

No person shall be granted remote access to information and information systems under the control of Necsa using any computer or device not under the direct control of Necsa, without the prior written authorisation of the ISO **and** such person having entered into a written agreement (see Exhibit 1) governing the conditions of such access as addressed in the Requirements for Remote Access (SHEQ-INS-0321).

12 MOBILE COMPUTING AND COMMUNICATION

No person shall be granted permission to remove a computing device or information retained on a computer device or to gain access to classified information or information systems from a location outside the influence of the physical security protections implemented by Necsa without having entered into a written agreement (see Exhibit 1) governing the conditions of use of the device or access to the information or information systems as addressed in the Requirements for Mobile Computing and Communication (SHEQ-INS-0322).

13 USE

13.1 The use of any classified information or information system under the control of Necsa shall be lawful, professional, ethical and conform to the provisions of this procedure and any information security procedure, standard, or guidelines that may be directed from time to time by the ISC and implemented by the ISO. Users shall also comply with the security screening requirements prescribed in SHEQ-INS-8950.

13.2 Use of Necsa classified information and information systems is granted to users primarily to assist in the execution of tasks appropriate to their employment or any contractual obligations to which they may be subject. While limited personal use may be permitted, this shall be at the absolute discretion of the ISC, which may delegate its authority to persons designated by it to determine what personal use is appropriate in any given circumstances.

13.3 Personal use shall be limited to use which is incidental and occasional. Personal use shall not:

i) interfere with the users' assigned work or performance of their duties;
ii) interfere with any other users' work or the performance of their duties;
iii) interfere with the operation of the Necsa information system; or
iv) be contrary to the provisions of this, or any related, procedure or standard.

13.4 Personal use required to extend beyond the limits set out in 13.3 shall only be allowed with the prior written consent of the relevant manager of the division or department in which the user is employed, and duly authorised by the ISO. The consent shall be specific as to the personal use allowed and the time period for which the consent is granted.

14 E-MAIL AND VOICE COMMUNICATION

14.1 Users shall not use Necsa information or information systems for excessive personal e-mail or voice communication.

14.2 Users shall **not** use Necsa information systems to:

i) subscribe to or access any e-mail system which is not the standard e-mail system provided by Necsa;
ii) initiate or forward chain messages;
iii) initiate or forward unsolicited e-mail;

iv) send numerous e-mails with the intention of disrupting or inconveniencing the recipient;
v) access the e-mail accounts of other users;
vi) communicate any information that is confidential to Necsa;
vii) communicate any material that is sexually explicit, obscene, discriminatory, racially or religiously prejudicial, or defamatory;
viii) communicate, copy or store any material the communication, copying or storage of which may constitute an infringement of a third party's intellectual property rights;
ix) communicate any files in excess of the size designated from time to time by the ISO;
x) open e-mails received from an unknown source; or
xi) automatically forward any communications received from third parties to any forwarding address.

14.3 Users shall immediately report to the ISO e-mails received from an unknown source, chain messages, unsolicited mail, any suspicion of unauthorised access to e-mail accounts, or the receipt of any material, which is sexually explicit, obscene, discriminatory, racially or religiously prejudicial, defamatory, or may constitute an infringement of a third party's intellectual property rights.

14.4 No sensitive information which is to be protected from potential interception shall be transmitted from Necsa's information systems, without authorisation from the ISO.

14.5 The ISO shall, at the request of a user wishing to transmit sensitive information, with the authority of the owner of the information, ensure that the necessary security measures have been implemented to protect the confidentiality and integrity of the information. (The requirements of SHEQ-INS-8930 shall be complied with.)

14.6 The provisions of 14.4 and 14.5 above shall apply to all communications, whether by voice, e-mail, or through any other media using the Internet or telecommunications systems.

15 CELLULAR PHONES OR OTHER INFORMATION STORAGE AND COMPUTER DEVICES

15.1 No information confidential to Necsa shall be downloaded, displayed, communicated or removed from Necsa using computer devices (including cellular telephones) or storage media without the prior consent of the owner of the information or the ISO. (See SHEQ-INS-8930 for a pro-forma to be used to request such authorisation.)

15.2 The ISO shall have the right to check that information under the control of Necsa or accessed from its information system has not been downloaded onto any cellular phone, computer device or storage media without authorisation.

15.3 The ISO shall, from time to time, check any computer device, including cellular telephones, or storage media in the possession of the user to ensure compliance with the requirements of Necsa's information security measures.

16 INTERNET USE

16.1 Necsa encourages use of the Internet (through the established fire wall) for the purpose of research necessary within the course and scope of a user's employment. However, users shall exercise care to ensure that their use falls within the provisions of Necsa procedures generally, and in particular, the information security procedures.

16.2 No user shall enter into any commercial transaction using a Necsa information system, which may have the effect of binding Necsa contractually without the prior written consent of the ISC. No

This document is the property of Necsa and shall not be used, reproduced, transmitted or disclosed without prior written permission

commercial transaction, however entered into, shall be transacted by a user if the transaction falls outside of the user's authority.

16.3 If a user uses information systems provided by Necsa to enter into any commercial transaction which is personal or on behalf of a third party other than Necsa, Necsa shall not be liable for any loss or damages incurred, of whatever nature that may be suffered by any party, and the user indemnifies Necsa against any such liability.

16.4 Users shall not use the Necsa information system to:

i) display, download or communicate any material, which is sexually explicit, obscene, discriminatory, racially or religiously prejudicial, defamatory, or may constitute an infringement of a third party's intellectual property rights;
ii) communicate their own, or any third party's, photograph or personal information including but not limited to, telephone or mobile numbers, physical addresses or e-mail addresses;
iii) subscribe to or participate in Chat Groups, Bulletin Boards, Newsgroups or Discussion Groups, without the prior written authorisation of the ISO; or
iv) surf the World Wide Web without purpose.

17 MALICIOUS CODE (VIRUSES)

17.1 Viruses are a primary cause of disruption of information systems and, if not dealt with correctly and promptly, may cause both financial and indirect loss to Necsa. Care in use of e-mail and downloading of software are important protections in the avoidance of viruses. All Necsa computers and devices shall be loaded with corporate anti-virus programmes.

17.2 Only the ISO or persons designated by the ISO, in writing, shall be entitled to download any software onto Necsa information systems. No user shall download or install any software from any storage medium, the Internet or any other source, onto information systems under the control of Necsa.

17.3 Any software that may reasonably be required by a user shall be provided or referred to the ISO, who shall, in collaboration of Corporate Information Technology personnel, supervise the checking, scanning and secure installation of the software onto the appropriate information system.

18 PHYSICAL SECURITY

18.1 The ISC shall direct that appropriate physical security measures be taken to safeguard Necsa classified information and information systems (see SHEQ-INS-8930).

18.2 The ISO shall, in conjunction with Necsa's security group, implement the directions of the ISC.

18.3 Users shall comply with the physical security restrictions published from time to time by the ISO.

19 BACKUP

19.1 Users shall strictly adhere to the provisions of all information security procedures and standards, requiring the backup and retention of information.

19.2 If, for whatever reason, Necsa information resides on a computer or computer device which is not subject to backup in the normal course, the user shall ensure that such information is backed up and the media on which the backup is stored is securely retained separate from the computer or computer device on which the information resides.

This document is the property of Necsa and shall not be used, reproduced, transmitted or disclosed without prior written permission

20 PRIVACY OF PERSONAL INFORMATION

20.1 Necsa shall adhere to legislation protecting the privacy of personal information.

20.2 Necsa shall collect, process, store and communicate personal information of users and third parties necessarily required in conducting its business. Disclosure of personal information to third parties, unless required in terms of law, shall not be made without the prior consent of the owner of the information

20.3 Necsa shall use it's best endeavours to protect personal information from unauthorised disclosure to third parties but shall not be liable for any damages suffered by the user or third party resulting from any inadvertent disclosure of personal information.

20.4 A person shall be entitled to have sight of any personal information belonging to that person, that is collected or stored by Necsa and shall be entitled to require Necsa to correct any incorrect information.

20.5 Necsa shall destroy personal information no longer required and/or that Necsa is not obliged to retain by law.

20.6 Necsa shall be entitled to use personal information for the purpose of processing statistical data or profiling persons provided that the aggregated information cannot be linked to the identity of a particular person.

20.7 Necsa shall use personal information to facilitate communication with users and third parties.

20.8 With the approval of this procedure and the signing of the Application and Agreement (Exhibit 1) a user automatically consents to Necsa's use of their personal information for the purposes stated and in the manner described in the procedure.

21 CONSENT TO INTERCEPTION AND MONITORING OF COMMUNICATIONS

21.1 Users accept and shall ensure the following:

i) the information and information systems are provided primarily for conducting the business of Necsa;
ii) allowing limited, incidental and occasional personal use of the information systems is an indulgence granted by Necsa to users;
iii) the information created, communicated or stored by users in the fulfilment of employment or contractual obligations to Necsa, is owned by Necsa;
iv) users have no expectation of privacy in the information referred to in 21.1(iii); and
v) notwithstanding the indulgence granted to users to use the Necsa information and information systems for the creation, communication and storage of information for personal purposes, Necsa has the right to intercept and monitor all information created, communicated and stored using the information systems.

21.2 The interception, monitoring and retention of any records of information shall be carried out:

i) in order to establish the existence of facts;
ii) for the purpose of detecting and investigating the unauthorised use of information or the information system; and
iii) with the intent of ensuring the ongoing security and effective operation of the information systems in the normal course of their operation.

21.3 Accidental interception or retention of information in the normal course of business, which is personal to a user, shall immediately be reported to the ISO.

21.4 Information which is, to the knowledge of the ISO, personal, shall not be intercepted or monitored without the prior approval of the ISC.

21.5 If interception, monitoring or retention of information known to the ISO to be personal, is authorised by the ISC, the ISC shall direct who may view the information and that the information remain confidential to those authorised to view the information.

22 ENFORCEMENT OF PROCEDURE

22.1 The terms of this procedure shall have the force of a contractual agreement between Necsa and users of Necsa's information or information systems.

22.2 This procedure shall be enforced by those parties appointed by the ISO to do so.

22.3 If disciplinary proceedings are appropriate they will be conducted in terms of the disciplinary procedures in force at Necsa from time to time.

23 SHEQ RECORDS

The following records shall be kept:

DESCRIPTION	RETENTION PERIOD	BY WHOM
Authorisation documents including the complete Access Application and Agreement (Exhibit 1)	Unlimited	ISO

BBS
BEHAVIOURAL BASED SAFETY REDUCES AT-RISK BEHAVIOURS

INFORMATION SECURITY

THIRD PARTY OR REMOTE ACCESS OR MOBILE COMPUTING APPLICATION AND AGREEMENT

necsa
We're in your world

1 **PARTICULARS OF THIRD PARTY, REMOTE ACCESS OR MOBILE COMPUTING APPLICANT (i.e. the person or persons who wishes to gain mobile computing privileges or access to Necsa's classified information or information system)**

Full name:	
Identity number*:	
Company:	
Designation:	
eMail address:	
Contact number/s:	
Physical address:	
Scope of work for Necsa covered by this application:	The rewriting and implementation (phase 1) of the current Waste Tracking System (WTS) software and 2) adding of new modules to include new processes (phase 2 of project).

Application for:	Yes or No
Third Party Access	Yes
Remote Access	No
Mobile Computing Privileges	No

Duration of required access from 2022-07-15 .. to 2023-07-14 .

*To be accompanied by a copy of the Third Party's identity document

2 **AGREEMENT**

I, the abovenamed Applicant, by my signature hereto, confirm that:

2.1 The information contained in this application is to the best of my knowledge true and correct;

2.2 I have read and understand the provisions governing my access (see page 3 of this form) and use of Necsa's classified information and information systems contained in this Application and I agree to adhere to its provisions; and

2.3 I have read and signed the Declaration of Secrecy (SHEQ-FRM-8934).

Name [Print] .. **Signature:** . **Date:** . ..

ALL PAGES TO BE INITIALLED BY APPLICANT, MANAGER AND ISO

PROVISIONS GOVERNING THIRD PARTY AND REMOTE ACCESS TO AND MOBILE USE OF NECSA'S INFORMATION AND INFORMATION SYSTEMS AND COMPUTER DEVICES

1 The Applicant has been engaged by Necsa to do work on behalf of Necsa which requires the Applicant to be granted access to Necsa's classified information and information systems ("access") or mobile computing privileges. The Applicant has applied to the Information Security Officer (ISO) for access or mobile use privileges (as applicable) and in applying agreed to abide by the following provisions governing the Applicant's access or the use of mobile computing devices and has initialled all the pages of this application together with the Acceptable Use Procedure appended to this application.

2 The Applicant further agrees:

2.1 to be bound by, and abide by the provisions of all relevant Necsa Information Security Procedures (e.g. Necsa's Requirements for Acceptable Use and Mobile Computing and Communication);

2.2 familiarise himself/herself with all procedures and procedures which apply to the access or mobile use granted to the Applicant, specifically, but without derogating from the general application of this clause, Necsa's Requirements for Acceptable Use; and

2.3 follow all directives given to the Applicant by Necsa's ISO.

3 **CONFIDENTIALITY**

3.1 The Applicant recognises that in being granted access or mobile use privileges and in his or her dealings with Necsa, governed by the terms of this agreement, he or she may have access to proprietary or classified information belonging to Necsa or a third party, including, without limitation:
(i) information access which is restricted by statute;
(ii) information that is marked in a manner that conveys its classification;
(iii) information that is confidential or a trade secret;
(iv) information that contains confidential information relating to customers;
(v) financial information;
(vi) information relating to contractual arrangements or dealings;
(vii) confidential reports; and
(viii) source and object program codes and development plans.

3.2 The Applicant agrees to and shall take all reasonable steps to protect the classified information against any unauthorised or improper access. Further, to take all reasonable steps to appropriately safeguard the physical security of any mobile computer device as well as any Necsa information stored on a mobile computer device or any other storage media (including paper).

3.3 The User undertakes that he/she shall observe all confidentiality obligations assumed in any employment contract with Necsa or any other agreement under and in terms of which the User provides services to Necsa.

3.4 The obligations contained in this agreement are supplementary to any confidentiality agreement that may have been entered into between the Applicant and Necsa. The provisions of this agreement shall be of full force and effect and, if in conflict with any other agreement, shall prevail.

3.5 The User undertakes to take all steps reasonably necessary to establish and maintain information security in all instances that information may be remotely accessed by the User.

3.6 The Applicant's obligation of confidentially shall endure indefinitely after the termination or expiry of this agreement (i.e. the provisions of this clause shall survive the termination of this agreement).

4 **PRIVACY**

4.1 The Applicant acknowledges that in the course of the services undertaken by him or her in terms of this agreement, access to and sight of personal information gathered by Necsa may be gained.

4.2 The Applicant further acknowledges that it is aware that this information is regarded as strictly private to Necsa and the particular person to whom it relates, that the information is, or may become subject, to the protection of privacy or data control legislation within South Africa or any other competent jurisdiction and that the improper disclosure of such information may render Necsa liable to criminal or civil proceedings.

4.3 The Applicant agrees that in the event of a breech of the obligations established in this clause due to the wilful default or negligence, he or she shall indemnify Necsa against all direct damages suffered by Necsa as a result of such breach.

4.4 The provisions of this clause shall survive the termination of this agreement.

5 OWNERSHIP

The Applicant agrees that the approval of the application does not, unless expressly agreed to the contrary in writing, confer or transfer any rights of ownership of mobile computer devices, or any Necsa information or Necsa intellectual property rights to the Applicant.

6 MOBILE COMPUTING SAFEGUARDS

6.1 The Applicant shall, prior to removing any computer device or media containing Necsa classified information from Necsa's premises, ensure the appropriate application of access controls, including hard disk encryption and login protection using strong passwords (or such other safeguards as the ISO may direct).

6.2 The Applicant shall not share dynamic password tokens, smart cards, fixed passwords or any other authentication device with any other person.

6.3 The Applicant shall not permit access to any person, including family members, friends and others to the mobile computer device or any password or token used to safeguard access to the device.

6.4 The Applicant shall ensure that classified information, mobile computer devices and/or storage media on which classified information is stored, are, when not being used by the Applicant, securely stored and accessible only to the Applicant.

6.5 The Applicant shall comply with the requirements of SHEQ-INS-8921 for the security clearance of items to be removed from Necsa's sites.

7 BACKUPS

7.1 The Applicant shall ensure that only classified information, gathered using a portable computer device or any other form of storage media, where appropriate, be backed up on appropriate Necsa servers.

7.2 The Applicant shall ensure that the classified information is backed up in a timely fashion and where appropriate, is deleted from the portable computer device or storage media.

7.3 Any copies of classified information in text and hard copy shall immediately be destroyed by the Applicant once it has served its purpose. (The destruction of such a document shall be such that the document cannot be re-created and read by a third party.)

8 CHANGES AND COMPROMISES

8.1 The Applicant shall inform the ISO of any software downloaded onto the mobile computer device (whether inadvertently or intentionally) before connecting to Necsa's information system.

8.2 The Applicant shall further inform the ISO of any hardware configuration changes to the mobile computer device before connecting to Necsa's information system.

8.3 If the Applicant changes residence or if the security of the Applicant's residence is compromised in any manner, the Applicant shall immediately inform the ISO of such change or compromise.

9 TRAVEL CONSIDERATIONS

The Applicant shall ensure the following while travelling:

9.1 That no Necsa classified information or a mobile computer device or media containing Necsa classified information shall be used in such a way that information may be accessed or viewed by third parties.

9.2 The Applicant shall not check-in the mobile computer device or media containing classified Necsa information as luggage but shall retain the information, computer device or media in their personnel possession at all times. While travelling the Applicant shall take all reasonable measures to ensure that the mobile computer device, storage media or Necsa classified information cannot be lost or stolen during the course of the journey.

9.3 If the Applicant, for whatever reason will not have the mobile computer device, storage media or Necsa classified information under his or her immediate control, the Applicant shall ensure that it is locked away in an adequately secure place.

10 SAFEGUARD OF TWO FACTOR AUTHENTICATION MECHANISMS FOR REMOTE ACCESS

The Applicant shall ensure the following:

i) Any mechanism (including, but not limited to, identification tokens or smart cards, which shall be used to facilitate the two factor authentication required to establish remote access, at all reasonable times, be kept on the User's person or under the User's control.
ii) Any device contemplated in i) above shall, when not in use, be securely stored under lock and key, and the key retained by the Applicant.

11 THE REMOTE ACCESS ENVIRONMENT

The Applicant undertakes:

i) to only log onto the Necsa information system remotely if he or she is satisfied that the environment from which such log-on occurs, is conducive to the security of Necsa's information;
ii) that he or she shall not leave the computer or computer device, through which remote access to Necsa's information systems is obtained, unattended while logged in to Necsa's information system;
iii) when any information is downloaded onto the computer, computer device or any other information storage mechanism, that the information is adequately protected to avoid access by any third party to the information; and
iv) that if any printouts of Necsa information are made and retained outside of the physical protections provided by Necsa that these shall be securely stored under lock and key, the key of which shall be retained or under the control of the Applicant.

12 REVOCATION OF ACCESS RIGHTS

12.1 The Applicant acknowledges that the ISO shall, in his or her entire discretion, be entitled to revoke access to the Applicant without notice and require that the Applicant remove himself/herself from Necsa's premises, where applicable.

12.2 In the event of the Applicant becoming aware of any compromise or potential compromise of any classified information or information systems or of the mechanisms used to authenticate the Applicant, he or she shall immediately inform the ISO of the compromise or potential compromise. In this event the Applicant shall adhere to all instructions given to him or her by the ISO. These events shall be registered as events in the EMP – see part 21 of SHEQ-INS-8930.

12.3 If the ISO, in his or her entire discretion believes that the Applicant has breached any terms of this agreement, the ISO shall be entitled to immediately and without notice to the Applicant, revoke the privileges granted to the Applicant.

12.4 The ISO shall, without limitation, revoke access privileges granted in terms of this Application and Agreement in the following circumstances:

(i) The agreed date for the revocation of the privileges and access has been reached;
(ii) the user of Necsa's information or devices is in breach of any provision of the Access Application and Agreement which, in the discretion of the ISO, may compromise the security of Necsa's classified information or information systems;
(iii) The termination or change of the User's employment or engagement by Necsa including a contract in terms of which the User provides services to Necsa;
(iv) The compromise of any authentication mechanism required by Necsa to be used by the Applicant to gain access to its classified information or information systems; and
(v) Any other event, action or omission on the part of the Applicant which, in the discretion of the ISO, warrants the revocation of access to the Applicant.

12.5 The Applicant agrees that Necsa's ISO or another authorised official may access the Applicant's premises to ensure compliance with the requirements of this agreement.

.. . . ..

Applicant's name [Print] **Signature** **Date**

BBS
BEHAVIOURAL BASED SAFETY REDUCES AT-RISK BEHAVIOURS

DECLARATION OF SECRECY

necsa
We're in your world

I, (ID: .. .), herewith declare:

1 I have taken note of the provisions of the:

- Protection of Information Act (Act 84 of 1982) and in particular of the provisions of Section 4 of the Act;
- Nuclear Energy Act (Act 46 of 1999) Sections 28 and 31.

2 I understand that I shall be guilty of an offence if I reveal any information which I have at my disposal by virtue of my office and concerning which I know or should reasonably know that the security or other interests of Necsa require that it be kept secret from any person other than a person.

- to whom I may lawfully reveal it; or
- to whom it is my duty to reveal it in the interests of Necsa; or
- to whom I am authorised by Necsa's CEO or by an officer authorised by the CEO to reveal it.

3 I understand that the said provisions and instructions shall apply not only during my term of office but also after the termination of my services at Necsa.

4 I am fully aware of the serious consequences that may follow any breach or contravention of the said provisions and instructions.

I have read and understand the above requirements.

Signature:

Place:

Date: