INFORMATION SECURITY POLICY AND MANUAL IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 of 2013 ("POPI")

Approved by: Danie van Wyk (Chief Executive Officer)

Approval date: 1 July 2019

Effective date: 1 July 2019

Key Contacts

Designation	Contact name	Telephone	E-mail
Information Security Officer	Danie Joubert	079 962 6428	daniej@bh1.co.za
Chief Executive Officer	Danie van Wyk	083 252 2603	danie@ibls.co.za

Version history

Version	Date	Author	Description
V1.0	01.07.2019	Danie Joubert	1st Issue

1 INFORMATION SECURITY

1.1 Statement of purpose

The value of information as an asset to Onevap (Pty) Ltd (ONEVAP), and all its subsidiaries, cannot be underestimated. The ever-increasing dependence of ONEVAP on information systems creates a unique vulnerability for our organisation which requires the introduction of business rules to provide clear and definitive instructions to assist ONEVAP in securing its information.

The term "information security" refers to the integrity, availability and confidentiality of the lifeblood of our organisation, which includes business trade secrets, contractual relationships, intellectual property, financial and operational systems, client and transaction details and information published to the public.

A breach in information security may compromise ONEVAP' ability to provide goods or services, be the cause of losses in revenue through fraud or destruction of proprietary or confidential data, lead to breaches of business contracts, trade secrets and privacy or damage our reputation with our stakeholders. Information is accordingly considered to be a primary asset of ONEVAP and must be protected in a manner commensurate to its value.

Accordingly, the management of ONEVAP has resolved that information security must be regarded as a critical part of ONEVAP risk management programmes. This policy has accordingly been prepared with reference to international best practices to provide a benchmark for the minimum level of due care for information security efforts within ONEVAP, thereby providing a framework for the safeguarding of our organisational information, compliance with relevant legislation and to serve as reference documents for internal quality control processes.

The objectives defined in this document may in certain cases conflict with other business objectives (such as improved efficiency and the reduction of costs). Management has examined these conflicts and resolved that the controls set out in this policy are required to manage the risks to ONEVAP.

The responsibility to preserve ONEVAP' information security is not limited to the IT Department but requires the co-operation of every employee. This policy has accordingly been written with the following goals in mind:

- to establish business rules to ensure the integrity, availability and confidentiality of all ONEVAP information; and
- to educate employees about their obligations for the protection of all ONEVAP information.

1.2 Status and application of policy

This policy applies to the whole of ONEVAP as defined above.

All employees should read, understand and agree to be bound to this document as part of the ONEVAP standard terms and conditions of employment.

Where non-employees, such as contractors, are permitted access to ONEVAP' information systems, they shall likewise contractually be required to adhere to the terms of this policy.

1.3 Policy updates

Updates to this policy and related information shall from time to time be published on the ONEVAP intranet / be made available to employees.

1.4 Further information

Further information about this document can be obtained from the ONEVAP, as defined below.

2 DEFINITIONS

2.1 In this document:

2.1.1 "confidential information" shall include:

i. all information that ONEVAP has an interest or obligation to keep confidential by law, contract or otherwise; and

ii. secret knowledge, trade secrets, intellectual property, know-how, processes and techniques, technical detail, method of operating, cost and source of material, pricing and purchasing policies and other matters which relate to ONEVAP' business in respect of which information is not readily available in the ordinary course of business to a competitor of ONEVAP;

iii. personal information;

2.1.2 ''data subject'' means the person to whom personal information relates;

2.1.3 "electronic communication" means any communication of information by electronic means;

2.1.4 "electronic communications systems" means all systems used by ONEVAP that enable electronic communications, including (without limitation) the Internet, voice mail, electronic mail and facsimiles;

2.1.5 "employee" means a part- or fulltime employee of ONEVAP, including any contractor with access to ONEVAP' information systems;

2.1.6 "incident" means any problem, malfunction, breach or suspected breach of information or the compromise of an information system;

2.1.7 "information" means representations of information in any form generated, sent, received or stored and includes:

i. voice, where the voice is used in an automated transaction; and

ii. a stored record;

2.1.8 "information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes electronic communications systems;

2.1.9 "intellectual property" shall include all copyright, rights in business names, trade marks, trade names, service marks, patents, designs and/or inventions, as well as all rights to source codes, trade secrets, and all other rights of a similar character (regardless of whether such rights are registered and/or capable of registration) and all applications and rights to apply for protection of any of the same;

2.1.10 “interconnect” means to link two telecommunications systems so that users of either system may communicate with users of, or utilise services provided by means of, the other system or any other telecommunication system

2.1.11 “ISO” means the information security officer, nominated by board of directors as such from time to time, which for the time being shall be the person appointed as the ONEVAP IT Manager;

2.1.12 "legal representative" means the person nominated by board of directors as such from time to time, being the ONEVAP legal advisor;

2.1.13 ‘‘operator’’ means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

2.1.14 “owner” means, in respect of information, the person nominated as custodian of such information in terms of this policy, being the CEO;

2.1.15 “personal information” has the meaning given to it in POPI, being information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

i. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
ii. information relating to the education or the medical, financial, criminal or employment history of the person;
iii. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
iv. the biometric information of the person;
v. the personal opinions, views or preferences of the person;
vi. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
vii. the views or opinions of another individual about the person; and
viii. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

2.1.16 “policy” refers to this information security policy and manual in terms of POPI;

2.1.17 ‘‘processing’’ means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

i. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

ii. dissemination by means of transmission, distribution or making available in any other form; or

iii. merging, linking, as well as restriction, degradation, erasure or destruction of information;

2.1.18 "records coordinator" means the person nominated by board of directors as such from time to time, being the ISO; and

2.1.19 ‘‘responsible party’’ means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

2.1.20 “sensitive information” means information designated as “internal use only”, “confidential”, or “secret” in terms of this policy; and

2.1.21 “technical representative" means the person nominated by board of directors as such from time to time, for the time being the ISO.

3 ORGANISATIONAL SECURITY

Objective: To manage information security within ONEVAP and to establish a framework to initiate and control the implementation of information security within the organisation.

3.1 Information Security Management Forum

3.1.1 The ISO, owner and legal representative shall collectively act as custodian of this policy ("information security management forum") and shall be responsible to:

i. allocate information security responsibilities throughout ONEVAP to give effect to the provisions of this policy;

ii. regularly review, evaluate and update this policy when ONEVAP' security requirements change by:

a) assessing risks to ONEVAP, thereby establishing threats to information and other assets, vulnerabilities and evaluating the likelihood of an occurrence and the potential impact thereof;

b) monitoring the legal, statutory, regulatory and contractual requirements that ONEVAP has to satisfy; and

c) any specific principles, objectives and requirements for information processing that ONEVAP has developed to support its operations;

iii. monitor compliance with this policy though internal audit processes, as envisaged in clause 3.3 below;

iv. establish business continuity and disaster recovery procedures, as envisaged in clause 3.4 below; and

v. co-ordinate the resolution of incidents, as envisaged in clause 3.5 below; and

vi. co-ordinate user training in all policy topics.

3.2 Statutory appointments

3.2.1 The CEO of ONEVAP shall act as information officer for ONEVAP for purposes of the Promotion of Access to Information Act of 2000 and the Protection of Personal Information Act of 2013 and be responsible to discharge ONEVAP' responsibilities in terms thereof.

3.2.2 The information officer shall consult the ISO and legal representative prior to any information disclosure in terms of clause 3.2.1 above.

3.3 Audit process

3.3.1 Compliance with this policy shall be monitored though internal audit processes established by the information security management forum in consultation with the IT department.

3.3.2 External audits may in addition be periodically commissioned by the information security management forum.

3.4 Business continuity and disaster recovery

The information security management forum shall implement a business continuity management process for developing and maintaining business continuity throughout ONEVAP.

3.4.1 Business continuity plans shall be maintained with a view to:

i. formulating controls to identify and reduce risks to an acceptable level;
ii. ensuring quick, effective and orderly response to incidents; and
iii. timely resumption of essential operations and the limitation of consequences of damaging incidents.

3.4.2 The technical representative shall be responsible to implement and periodically test the business continuity and disaster recovery plans to ensure that they are up to date and effective.

3.5 Incident management

3.5.1 Employees are obliged to report any incident to the ISO.

3.5.2 Employees are prohibited from utilising ONEVAP' systems to forward such information, specifically hoaxes pertaining to system vulnerability information, to other employees, whether the other employees are internal or external to ONEVAP.

3.5.3 The ISO shall, with approval from the information security management forum, establish and document incident management procedures, which shall include mechanisms to enable the types, volumes and costs of incidents to be monitored.

3.6 Collection of evidence

In the event that an employee suspects that a breach of this policy may have occurred on an information system (whether relating to ONEVAP or client information), no further action is permitted in respect of such information system until such time as the ISO has authorised same.

4 COMMUNICATIONS AND OPERATIONS MANAGEMENT

4.1 Company property

ONEVAP encourages the use of electronic communications as a means of enhancing productivity. Electronic communication systems and all messages generated on or handled by same are however considered to be the property of ONEVAP.

4.2 Authorised usage

Subject to clause 4.3 below, electronic communication systems must be used only for business activities as may be specifically authorised. Employee privileges on electronic communication systems are assigned on the basis that only those capabilities necessary to perform a job are granted (the principle of "least privilege").

4.3 Private use

4.3.1 ONEVAP permits incidental personal use, provided that such use shall be subject to the provisions of 4.4 below and further does not:

i. interfere with job performance;
ii. deny other employees' access to the system resources; and
iii. incur significant costs.

4.3.2 Employees are forbidden from using electronic communication systems for private business activities.

4.3.3 Any private use within the meaning of this clause 4.3 is at the employee's own risk and the employee further indemnifies ONEVAP from any liability in respect thereof.

4.4 No expectation of privacy

4.4.1 It is the policy of ONEVAP not to regularly monitor the content of electronic communications. Employees who make use of the electronic communication systems should however have no expectation of privacy when using the electronic communication systems, as electronic communications may be monitored, intercepted, stored and accessed to support operational, maintenance, auditing, security and investigative activities in instances such as the following (which are not intended to be all-inclusive):

i. ensuring that ONEVAP' information systems are not being used in contravention of this policy;
ii. responding to legal proceedings that call for producing electronically stored evidence;
iii. locating, accessing, and retrieving information in an employee's absence; and
iv. investigating indications of impropriety or counteracting theft.

4.4.2 The IT department automatically monitors the use of the electronic communication systems and may be required to review the contents of stored or transmitted data in the course of their duties. Such actions shall at all times be within the ambit of this policy and the specific provisions authorised by the technical representative to system administrators appointed by the IT department in writing. For avoidance of doubt it is stated that system administrators may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels provided for in this policy.

4.5 Procedural requirements

4.5.1 All examinations in respect of breach of any laws, or of the ONEVAP' conditions of employment or disciplinary code, or of any of the provisions of this policy, shall:

i. require prior review and written approval by the legal representative, or in the event that a request to the legal representative is inappropriate, the chief executive officer of ONEVAP, of the scope of the investigation; and
ii. conducted under the direct control of the technical representative.

4.5.2 The results of any findings shall, until otherwise reclassified by the legal representative (or the chief executive officer, as the case may be), be labelled "secret" in accordance with ONEVAP' classification scheme (see clause 5.3).

4.6 Electronic contracting

4.6.1 Applicable law provides that:

i. information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message; and
ii. information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect but is merely referred to in such data message.

4.6.2 Employees are accordingly required to refrain from making unauthorised statements in electronic communications that could bind ONEVAP. All contracts formed through electronic offer and acceptance messages must be subject to being formalised and confirmed via paper documents.

4.6.3 Under no circumstances may employees employ the use of scanned versions of hand-rendered signatures to give the impression that any electronic communication has been signed.

4.7 Encryption of electronic communications and devices

4.7.1 Employees should note that most electronic communications are by default not secure.

4.7.2 In certain instances, this policy prescribes the use of encryption technologies. Electronic communications may only be encrypted utilising technologies approved by the ISO and further subject to any conditions imposed in respect thereof in terms of procedures.

4.7.3 All company owned external hard drives are to be encrypted by means of Bitlocker and current contents deleted before leaving the premises to collect client information. Passwords of these drives are strictly controlled and unique per client. Client information is confidential and is only to be accessed by ONEVAP and the respective client.

4.7.4 All company owned as well as contractor laptops are to be encrypted using Bitlocker before client data is copied onto it or before is to leave the premises. Each user is given his/her own unique decryption password. These passwords are strictly managed by the IT department. Under no circumstances can this password be given to anyone else either by the employee/contractor or the IT department.

4.7.5 All daily server backups are encrypted on each tape by means of unique 2048-bit SSL certificates with 256-bit encryption. These backups are stored offsite for safety and cannot be accessed by any external source or system without the certificates.

4.8 Acceptable and unacceptable use

4.8.1 4.8.1 Employees must comply with the Company's Acceptable Use Policy in place from time to time (forming part of the Company's Personnel Policy), which inter alia states that they may not use electronic communication systems for the purpose of:

i. receiving or transmitting any discriminatory, obscene, offensive, profanity, obscenities, derogatory remarks discussing employees, customers, competitors or others;
ii. any defamatory, discriminatory, or obscene material;
iii. infringing on another person's (whether natural or legal) intellectual property rights (e.g. copyright);
iv. carrying messages which may be seen to be insulting, disruptive, offensive to other employees or could lead to a breach of confidentiality;
v. any attempt to penetrate or to gain unauthorised access (or attempted access) to the electronic communication systems or network security of any ONEVAP or other third party system;
vi. the violation or attempted violation of any law; or
vii. placing an unusual burden on the electronic communication systems in the sole discretion of the technical representative.

4.9 Responsibilities of employees

4.9.1 Employees must respect the physical hardware and network configurations of the electronic communications systems.

4.9.2 Employees may not transmit sensitive parameters (such as access codes, account details, credit card numbers or passwords) over an electronic communication system unless same is properly protected, as provided for in this policy.

4.9.3 Employees may not misrepresent or hide their own or another employee's identity on the Internet or on any other ONEVAP information system.

4.9.4 Employees may not download files or software from the Internet unless authorised to do so by the ISO or technical representative.

4.10 Segregation of duties

Duties and areas of responsibility shall be segregated in accordance with management's instructions from time to time

4.11 Prior review and posting of information

4.11.1 Prior review by an employee's immediate manager shall be required in the event that any ONEVAP information is to be used for any speech, presentation, technical paper, book or other communication to be delivered to the public (including any advertisement, Internet web page, electronic bulletin board posting, electronic mail message, voice mail message).

4.11.2 Employees may not post information pertaining to ONEVAP or its business to public discussion groups, chat rooms, web pages, electronic bulletin boards, or other mechanism which provides public access to information on the Internet unless they have been preauthorized by senior management in writing.

4.12 Corporate Image

Employees must always observe the policies from time to time in place with regard to the format and appearance of communications and corporate documents.

4.13 Electronic communications notice

4.13.1 The following notice shall automatically be attached to all outgoing electronic messages (excluding facsimiles):

4.13.2 The technical representative shall procure that the aforesaid message is attached to all electronic mail. Employees must procure the inclusion of the aforementioned text on all other electronic communications.

4.13.3 The hyperlinked terms applicable to electronic communications shall be prepared and updated by the legal representative from time to time.

4.13.4 The legal representative shall apply proper version control, indicating at least the version number and the date upon which any subsequent version would come into effect.

5 INFORMATION CLASSIFICATION, LABELLING AND RETENTION

Objective: Other than information defined as public, all information should be accessible on a "need to know basis" to specifically identified, authenticated and authorised entities for agreed periods.

5.1 Purpose

ONEVAP is required to protect certain records from loss, destruction and falsification. These records may need to be securely retained to meet statutory or regulatory requirements, as well as to support business activities.

5.2 5.2 Scope

This policy applies to all ONEVAP data that exist in any information systems, on any media during any part if its life cycle (generation, use, storage and disposal).

5.3 Classification

5.3.1 To assist in the appropriate handling (and processing) of information, the following uniform sensitivity classification scheme has been developed by ONEVAP:

i. Public: This information has been explicitly approved by ONEVAP management for release to the public. Examples include product and service brochures, advertisements, job opening announcements, press releases, information posted on the ONEVAP website.

ii. Internal use only: This information is intended for internal ONEVAP use only, not falling within the classification "Confidential" or "Secret". While its unauthorised disclosure is against policy, it is not expected to seriously or adversely impact ONEVAP or third parties. Examples include new employee training materials and internal policy manuals.

iii. Confidential: This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Its unauthorised disclosure could adversely impact ONEVAP or third parties. Examples include employee performance evaluations, transaction data, agreements, unpublished market research, passwords and internal audit reports as well as all client information.

iv. Secret: This classification applies to the most sensitive business information which is intended strictly for use within ONEVAP to those with a legitimate business need for access. Its unauthorised disclosure could seriously and adversely impact ONEVAP or third parties. Examples include merger and acquisition documents, corporate level strategic plans, litigation strategy memos, new innovations and trade secrets, as well as all ONEVAP IP and sensitive client information such as account numbers or personal information of client customers.

5.4 Information ownership

5.4.1 In order to classify information, it is necessary that an owner be identified for all information assets. Unless otherwise stated in this policy, the creator of an information asset shall be deemed the owner thereof for purposes of labelling, as herein envisaged.

5.4.2 In the event of doubt, the records coordinator will nominate an owner.

5.5 Labelling

5.5.1 It is the responsibility of the owner of information (i.e. the creator thereof) to designate an appropriate sensitivity label.

5.5.2 Users of the information must in turn adhere to and consistently maintain the assigned label.

5.5.3 If information is not assigned a sensitivity label, it will be deemed to fall within the "Internal use only" category. Information that falls within the "Internal use only" sensitivity label does not have to be marked.

5.5.4 Upon receipt of externally supplied information, the relevant employee must assign a sensitivity label to such information, taking care to preserve information pertaining to restricted dissemination and intellectual property rights.

5.5.5 When information with different sensitivity labels is stored together, the handling instructions for the highest sensitivity label will apply.

5.6 Handling

The matrix in annexure A to this policy stipulates ONEVAP' requirements for the handling (and processing) of information according to its sensitivity label.

5.7 5.7 Retention

5.7.1 All ONEVAP information shall be categorised into four main classifications for purposes of these retention rules, namely:

i. Business information: Any information relevant to business transactions, clients (and customers of clients) or products, including communications regarding performance, legal opinions and specifications.

ii. Administrative information: All company secretarial, human resource and related information.

iii. Fiscal information: All information related to revenue and expense of ONEVAP, including accounting records, tax returns

iv. Other information: All correspondence not falling within the above categories, including personal email, updates and status reports.

5.7.2 ONEVAP information shall be retained in accordance with the provisions set out in annexure B to this policy.

5.7.3 Notwithstanding the aforesaid general retention requirements, the records coordinator may issue directives with a view to complying with statutory retention requirements, including the respective periods of time for which they are required be retained. The records coordinator shall, in consultation with each departmental manager, establish and document procedures for complying with the aforesaid retention requirements.

5.8 Cryptographic keys

Employees must disclose cryptographic keys associated with encrypted archives or digital signatures, which will be kept securely and made available to authorised persons when needed by the records coordinator.

5.9 Deletion and disposal

Information must be deleted or disposed of when no longer needed. Information owners must accordingly periodically review the continued value of information in light of this policy and any directives issued by the records coordinator. Due regard must be had to the minimum legal periods that information must be retained in complying with this policy and ONEVAP' statutory obligations.

6 INTELLECTUAL PROPERTY AND CONFIDENTIALITY

Objective: To ensure the correct and secure operation of electronic communications systems.

6.1 Ownership of intellectual property

6.1.1 The employee shall disclose to ONEVAP all intellectual property made by him or her during the course of carrying out of duties in terms of this agreement, irrespective of whether such works were made during office hours or otherwise or were made at the premises of ONEVAP or otherwise. The ownership of all such intellectual property shall vest in ONEVAP.

6.1.2 To the extent required, the employee shall co-operate to procure that the intellectual property is transferred to ONEVAP and undertakes to execute all such documents as may be required for ONEVAP to secure and/or register its rights in respect of the said intellectual property.

6.1.3 The employee hereby waives in favour of ONEVAP any so-called moral rights which may accrue to the employee in any of the intellectual property.

6.2 Intellectual property in third party agreements

6.2.1 In the event that a third party is contracted in terms of an engagement where intellectual property will be created on behalf of ONEVAP, an agreement in writing must be secured containing at least:

i. an assignment of all intellectual property rights; and
ii. a warranty of non-infringement in respect of the assigned rights by the third party.

6.3 External use of intellectual property

6.3.1 ONEVAP intellectual property may only be used by third parties in terms of a licence agreement concluded between the parties in writing.

6.3.2 The licence agreement must reserve all intellectual property rights not expressly granted.

6.4 Registration of intellectual property

6.4.1 It is the policy of ONEVAP to protect intellectual property though registration in appropriate cases.

6.4.2 The legal representative shall be notified of any new registerable intellectual property that has been developed prior to same being made public. Registerable intellectual property includes:

i. trademarks: any sign capable of being represented graphically, including a device, name, signature, word, letter, numeral, shape, configuration, pattern, ornamentation, colour or container for goods or any combination of the aforementioned to be used by a person in relation to goods or services for the

purpose of distinguishing the goods or services in relation to which the mark is used or proposed to be used from the same kind of goods or services;

ii. domain names: an alphanumeric designation that is registered or assigned in respect of an electronic address or other resource on the Internet;

iii. patents: any new invention (idea) which involves an inventive step, and which is capable of being used or applied in trade or industry or agriculture;

iv. designs: any design applied to any article having features which appeal to and are judged solely by the eye, irrespective of the aesthetic quality thereof or having features which are necessitated by the function which the article to which the design is applied, is to perform, and includes an integrated circuit topography, a mask work and a series of mask works.

6.5 Confidentiality

The employee undertakes to maintain the confidentiality of any confidential information to which the employee should be allowed access by ONEVAP. The employee will not divulge or permit to be divulged to any person any aspect of such confidential information, otherwise than may be allowed in writing by ONEVAP, or is otherwise permitted in terms of this policy.

6.6 Use of meta tags

ONEVAP websites shall not utilise terms in its meta tags which may constitute an infringement of intellectual property (trademarks).

6.7 Publication of terms of use on all websites

6.7.1 All websites shall display terms of use, which shall be prepared and updated by the legal representative from time to time.

6.7.2 The legal representative shall apply proper version control, indicating at least the version number and the date upon which any subsequent version would come into effect.

6.8 Software

6.8.1 Employees are notified that breach of software licensing conditions may render ONEVAP and/or the employee liable to civil and/or criminal prosecution. Employees are accordingly not allowed to install ONEVAP software on any computer or device or make copies thereof, unless expressly authorised thereto by the technical representative.

6.8.2 Documentation pertaining to licences should be retained for the term of use of the software.

6.8.3 Questions pertaining to licensing can be directed to the technical representative.

6.9 Materials from the Internet or unknown sources

Employee should assume that all materials obtained from the Internet or unknown sources are the subject of copyright or other intellectual property rights. Accordingly, unauthorised

use thereof may constitute an infringement of the aforesaid rights, rendering ONEVAP potentially liable.

7 PROTECTION OF PERSONAL INFORMATION IN TERMS OF POPI

Objective: To ensure ownership of intellectual property and confidentiality of information.

7.1.1 Purpose for processing of personal information

i. Before ONEVAP can process personal information, the purpose for processing of personal information must be determined:
ii. whether the processing / sharing is necessary to carry out actions for the conclusion or performance of an agreement to which ONEVAP and the data subject is party; and/or
iii. processing complies with an obligation imposed by law; and/or
iv. processing protects a legitimate interest of the data subject.

7.1.2 For purposes of this policy, personal information shall be broadly classified in two categories:

i. "Internal personal information", being personal information relating to business clients of the company ("Clients") and employees of ONEVAP; and
ii. "External personal information", being personal information relating to data subjects who are clients of ONEVAP' Clients, which ONEVAP may be required to process in terms of a written contract with a Client as an operator.

7.1.3 In respect of Internal personal information, ONEVAP shall comply with the provisions of POPI as a responsible party.

7.1.4 In respect of External personal information, ONEVAP shall comply with the provisions of POPI as an operator. In these circumstances, ONEVAP shall comply with the instructions of the responsible party in respect of the classification and processing of the relevant personal information.

7.1.5 ONEVAP shall secure the integrity of the personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of, or damage to, or unauthorised destruction of the personal information or unlawful access to or processing of the personal information and which provide a level of security appropriate to the risk represented by the processing and the nature of the personal information to be protected – as set forth in the remainder of this policy.

7.1.6 ONEVAP has in place rules, procedures and systems to ensure that any third party it authorises to have access to the personal information, including operators, will respect and maintain the confidentiality and security of the personal information.

7.1.7 In the event that ONEVAP makes use of operators in respect of processing of personal information, it shall do so only by way of written agreement with the sub-contractor involved which imposes the same obligations on the sub-contractor as are imposed on ONEVAP.

7.1.8 In addition to the other obligations set out in this section, the ONEVAP shall:

i. take reasonable steps to ensure the reliability of any of its staff who have access to personal information;
ii. limit access to the personal information only to those staff who need to know to enable ONEVAP to achieve the purposes and objectives of any agreement in terms of which processing is required and ensure that staff used by it to process the personal information have undergone training in the care and handling of the personal information;
iii. promptly inform any relevant third party or data subject of its inability to comply with the provisions of this section, in which case such party is entitled to suspend the sharing of personal information;
iv. provide the owner of the personal information with full co-operation and assistance in relation to any requests for access or correction or complaints made by data subjects;
v. at the request of the owner of the personal information or any regulatory body, submit its personal information processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the owner of the personal information (or any independent or impartial inspection agents or auditors) to ascertain compliance with POPI, with reasonable notice and during regular business hours.

7.2 Trans-Border flows of Personal Information:

7.2.1 Section 72 of POPI deals with transfers of personal information outside South Africa or trans-border information flows. A responsible party may not transfer personal information about a data subject to a third party who is in a foreign country, unless certain protections are in place. For example, if:

i. the foreign country has a law that provides adequate protection;
ii. there are binding corporate rules that provide adequate protection;
iii. there is an agreement between the sender and the receiver that provides adequate protection;
iv. the data subject consents to his/her personal information being so transferred; or
v. the transfer is necessary for the responsible party to perform in terms of a contract.

7.2.2 In light of the above, ONEVAP shall ensure that one or more of the appropriate aforementioned actions have been taken and the applicable measures have been put in place to ensure compliance with POPI in the event that it is required to participate in a cross-border transfer of personal information for a client.

8 NETWORK AND OPERATIONAL SECURITY

Objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

8.1 Access control: principle of “need to know”

8.1.1 Information should only be disclosed to employees who have a legitimate business need for the information.

8.1.2 An employee’s manager must initiate the access control approval process.

8.1.3 All non-employees (e.g. contractors, consultants) must also go through an access control request and authorisation process initiated by the project manager. It is the project manager’s responsibility to continually evaluate the non-employee’s need for continued privileges and to notify the technical representative when they may be terminated.

8.2 Change control

8.2.1 Employees are not permitted to install, replace or upgrade or otherwise alter the configuration of any information system (“configuration changes”), unless authorised to do so.

8.2.2 All requests for configuration changes shall be directed to the helpdesk in the format to be specified from time to time by the technical representative.

8.3 Testing prohibition

8.3.1 Employees are not allowed to test, or attempt to compromise any information security mechanism.

8.3.2 Employees are prohibited from possessing any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to intercept or monitor electronic communication (for example password cracking software, network sniffers etc.).

8.4 Termination of employment or contract

Upon termination of employment or a contract of service, an employee's information system access and electronic communication system accounts must be terminated.

8.5 Passwords management

8.5.1 Employees must choose difficult to guess passwords. This means to avoid using any of your names, surnames or children’s names as well as any variation of the word “password”, “qwerty”, “12345678910”, etc.

8.5.2 Passwords must be at least 8 characters long and contain alphabetic (including capital letters), numeric and special (!@#$ etc.) characters.

8.5.3 Employees must keep their passwords confidential and cannot store passwords on any computer or other files where the same can be compromised, unless it is protected using encryption software authorised by the ISO.

8.5.4 Employees may not use the password or username belonging to another person, at any time and for any reason.

8.5.5 Employees are not permitted to transmit passwords or usernames through any medium, including e-mail and internet relay chat. For RTL instances, a process needs to be put in place to facilitate the required access without the need to transmit passwords.

8.5.6 Should any entity attempt to obtain your password from you, you are requested to report this to the ISO immediately.

8.5.7 ONEVAP passwords automatically expire every 60 days and 12 previous passwords are remembered by Active Directory to ensure that passwords are not reused.

8.6 Viruses and malicious software

8.6.1 Virus checking systems will be in place on all information systems susceptible to viruses or malicious software (e.g. firewalls with external network connections, all electronic mail servers).

8.6.2 All data files originating from external sources must be checked by ONEVAP' virus checking systems before execution or usage.

8.6.3 Employees are not authorised to turn off or disable virus checking systems.

8.6.4 No person may insert removal storage media into any information system without it first having been scanned for viruses in accordance with the procedures issued by the technical representative.

8.6.5 In the event that an employee suspects that his or her information system has been infected with a virus or malicious software, the following rules must be observed:

i. the employee must immediately cease use of the affected information system; and
ii. contact the IT Department by telephone for assistance.

8.7 Remote access

8.7.1 Remote access to ONEVAP' information systems will be granted to employees to the extent that they have a demonstrable business need for such access.

8.7.2 Remote access privileges are subject to periodical review and the procedures issued by the technical representative and the ISO from time to time.

8.7.3 Employees who are granted remote access should keep connection information strictly confidential.

8.8 Use of private connections

Under no circumstances may employees leave modems or other communication devices linked to ONEVAP information systems in unattended auto-answer mode, unless written permission has been granted by the ISO, who may issue such permission subject to such directions as he or she may deem fit. ONEVAP 3G modems may only be used for ONEVAP business related downloads and client connections such as RTL and not for any personal purposes.

8.9 Telecommunications legislation

8.9.1 No employee shall, without prior approval from the information security management forum:

i. commission or decommission a new information system; or
ii. interconnect with any ONEVAP information system.

9 PHYSICAL AND ENVIRONMENTAL SECURITY

Objective: To prevent unauthorised access, damage and interference to business premises and information.

9.1 Clean desk and screen policy

9.1.1 When not in use, sensitive information shall be protected from unauthorised disclosure. Employees shall at all times endeavour to maintain a clean desk when same is unattended. In any event, information labelled as “confidential” or “secret” shall not be left in the open.

9.1.2 Employees shall take care not to leave sensitive information displayed on information systems when same is unattended.

9.1.3 Employees shall utilise password-protected screensavers.

9.2 Accountability of assets

9.2.1 ONEVAP shall at all times retain and continually update a list of assets.

9.2.2 Employees shall not tamper with any asset tags.

9.2.3 No ONEVAP assets may be removed from the premises without appropriate approval.

9.2.4 Portable assets are to be signed out before leaving the premises and signed back in when the employee brings it back.

9.3 Office access

Physical access to facilities containing sensitive information shall be restricted in a manner directed by the ISO.

Entry to the office is by means of fingerprint readers or access tags. Server rooms are access controlled by means of access tags and physical keys. Only a select few have access to the server rooms and should be approved by management.

Should a 3rd party require access to a server room, such 3rd party must be supervised by a member of the ONEVAP IT department (or person nominated by the IT department) for the duration that such 3rd party access is required.

10 VIOLATION

10.1 Employee accountability

10.1.1 Employees who share individual passwords expose themselves to responsibility for the actions the other party takes with the password.

10.1.2 Employees are responsible for terminating open sessions and logging out of Electronic communication systems when any such systems are left unattended. The Employee will be held responsible for any activities that may take place as a result of a failure to comply with the aforementioned, which may include, without limitation, any account or damage that may be occasioned.

10.2 Consequences of violation

10.2.1 Violation of any of the provisions of this policy may result in: 10.2.1.1 the restriction or termination of an Employee's access to the electronic communications systems, including the summery suspension of his or her privileges pending further disciplinary action;

i. the initiation of legal proceedings by ONEVAP including but not limited to criminal prosecution under appropriate laws that may prevail in South Africa from time to time; and

ii. disciplinary proceedings being instituted against the employee which may result in dismissal.

10.3 Risk acceptance

In rare cases non-compliance with this policy may be authorised by means of a risk acceptance process, which requires a risk acceptance memo to be signed by a manager and approved by the ISO in writing prior to such non-compliance taking place.

ANNEXURE A: INFORMATION HANDLING

	Sensitivity label			
	Public	**Internal Use Only**	**Confidential**	**Secret**
Granting of access to information	Yes.	May share internally	Strictly need to know	Strictly need to know
Release to third parties	Yes	No, not without NDA	No, not without NDA	No, not without NDA, and preferably not at all
Storage on fixed media (e.g. hard drive)	Yes	Yes	To be encrypted/extra precautions	To be encrypted/extra precautions
Storage on removable media (e.g. flash disk)	Yes	Yes	Not without special precautions/passwords etc.	No
Copying	Yes	Yes	Not unless absolutely necessary	Not unless absolutely necessary
Printing	Yes	Yes	Not unless absolutely necessary	Not unless absolutely necessary
Faxing	Yes	Yes	No	No
Sending by public network (e.g. Internet)	Yes	Yes	No, not unless encrypted	No, not unless encrypted
Disposal	Normal disposal methods	Normal disposal methods	To dispose safely of printed material in shredding bins/or shred immediately	To dispose safely of printed material in shredding bins/or shred immediately

ANNEXURE B: INFORMATION RETENTION

	Business information	Administrative information	Fiscal information	Other information
Physical documents	As long as is required	As long as is required	At least 5 years	According to need
Electronic files stored on network drives	As long as required	As long as required	At least 5 years	According to need
Electronic files stored on local disk	As long as required	As long as required	At least 5 years	According to need
Electronic mail messages	As long as required	As long as required	At least 5 years	According to need
Retention period	As long as is required	As long as is required	At least 5 years	According to need