**TERMS AND CONDITIONS**

**SUMMARY OF IMPORTANT ASPECTS**

* **BY AGREEING TO THESE TERMS AND CONDITIONS YOU ARE PROVIDING YOUR CONSENT TO THE DEPARTMENT TO COLLECT AND PROCESS YOUR PERSONAL INFORMATION AS WELL AS OTHER INFORMATION SET OUT BELOW. THE DEPARTMENT WILL COLLECT AND PROCESS SUCH INFORMATION IN COMPLAINCE WITH THESE TERMS AND CONDITIONS AND THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013.**
* **ALL INFORMATION PROVIDED BY A USER USING THIS ECOS SYSTEM MAY BE MADE SHARED BY THE DEPARTMENT, VIA ECOS OR OTHERWISE, TO OTHER ORGANS OF STATE OR AUTHORITIES. SUCH INFORMATION MAY, ALSO BE MADE AVAILABLE TO OTHER AUTHORISED PERSONS OR ENTITIES, AS MAY SO BE DETERMINED BY THE DEPARTMENT, ORGAN OF STATE OR, AUTHORITY, OR AS REQUIRED BY LAW.**
* **THE INFORMATION WHICH MAY BE SHARED INCLUDES, BUT ARE NOT LIMITED TO, THE FOLLOWING:**
	+ **PRODUCT INFORMATION, SUCH AS COUNTRY AND REGION OF ORIGIN OF INGREDIENTS, FINAL PLACE OF MANUFACTURE AND SPECIES COMPOSITION;**
	+ **PERSONAL INFORMATION OF THE USER BUT ONLY TO THE EXTENT AS PROVIDED FOR IN CLAUSE 12 OF THESE TERMS AND CONDITIONS;**
	+ **AGGREGRATED REPORTING INFORMATION OF EXPORTED ITEMS AND LIVE ANIMALS OR ORGANISMS; AND**
	+ **YOUR ESTABLISHMENT’S CONTACT DETAILS WHICH MAY ALREADY BE IN THE PUBLIC DOMAIN.**
* **IF THE USER ELECTED THE ‘ALLOW DATA DISTRIBUTION FOR MARKETING’ OPTION OF THE INFORMATION MADE AVAILABLE BY THE USER, THEN SUCH INFORMATION PROVIDED IS REGARDED TO BE IN THE PUBLIC DOMAIN AND WILL, APART FROM BEING PROTECTED BY LAW FROM DISTRIBUTION, NOT BE PROTECTED UNDER THE PRIVACY POLICY SET OUT IN THESE TERMS AND CONDITION AND MAY THEREFORE BE ACCESSIBLE BY ANY THIRD PARTY.**
1. **DEFINITIONS AND INTERPRETATION**

* 1. For the purposes of these Terms and Conditions, unless the context requires otherwise:

* + 1. **“Bug”** means faults, defects and problems encountered in the ECOS;

* + 1. **“Consumer Protection Act”** means the Consumer Protection Act 71 of 2008;

* + 1. **“Cookies”** means files with a small amount of data, which may include an anonymous unique identifier;

* + 1. **“Department”** means the Western Cape Government’s Department of Agriculture;

* + 1. **“ECOS”** is an acronym for Export Control Office System and is an electronic system used, owned and developed by the Department for the creation and management of information and documentation required for food traceability, location management, accreditation management and certification purposes;

* + 1. **“Department’s Privacy Policy”** means the Department’s privacy policy in clause 12 of these Terms and Conditions;

* + 1. “**Department’s Website**” means the portal, Home Page and Web Pages used by a User to access ECOS, which Website is accessible at the following internet address: <https://mygovapps.westerncape.gov.za>;
		2. **“E-Cert”** means the administration of export certificates and eligibility documents for the export supply chain of agricultural products, including but not limited to fruit, fruit products, composite products animals and animal products;
		3. “**Electronic Communications and Transactions Act**” or **“ECTA”** means the Electronic Communications and Transactions Act 25 of 2002;

* + 1. “**Home Page**” has the meaning assigned in ECTA;

* + 1. **“Internet”** has the meaning assigned in ECTA;

* + 1. “**Intellectual Property**” means, but is not limited to, all outputs of creative endeavour in any field that can be protected either statutorily or not, within any jurisdiction, including but not limited to all forms of copyright, design right, whether registered or unregistered, patent, patentable material, trademarks, Know-How, trade secrets, rights in databases, information, data, discoveries, computer software and programmes;
		2. “**Intellectual Property Rights**” means all intellectual property rights of whatever nature, including (i) all patents and other patent rights, including divisional and continuation patents, utility models; (ii) rights in and to inventions, whether patentable or not; (iii) rights in trademarks, service marks, logos, slogans, corporate, business and trade names, trade dress, brand names and other indicia of origin; (iv) rights in designs, topography rights, rights in circuit layouts and mask-works; (v) copyright, including all copyright in and to computer programs; (vi) rights in internet domain names, reservations for internet domain names, uniform resource locators and corresponding internet sites; (vii) rights in databases and data collections; (viii) know-how, show-how, trade secrets and confidential information, in each case whether or not registered and including applications for the registration, extension, renewal and re-issuance, continuations, continuations in part or per division of, any of these and the right to apply for any of the foregoing, all claims for past infringements, and all rights or forms of protection of a similar nature or having equivalent or similar effect to any of these which may subsist anywhere in the world;
		3. **“Know-How”** means all the proprietary information of the Department including information reduced to material form, which is available to the public but compiled into a usable and/or valuable format by the use of labour, skill and effort;

* + 1. **“Laws”** means any and all laws in force (whether in the Republic of South Africa or, where applicable, any other country or region whatsoever) including, but not limited to, statutes and the common law and further specifically, including but not limited to, the Consumer Protection Act, ECTA, PAIA, PAJA and POPIA;

* + 1. **“Log-in”** means the granting of access to ECOS by means of the User Authentication System and **“Logged-in”** shall have a corresponding meaning;

* + 1. **“Overseas Market Access Requirements”** means the access requirements for countries and markets that have agreements in place with the Republic of South Africa for products entering their borders;

* + 1. **“Party”** means either the Department or the User, as the context may indicate and **“Parties”** shall mean both of them;

* + 1. **“Personal Information”** means the personal information of the User as defined in the Protection of Personal Information Act but specifically excludes -

* + - * information which has been permanently de-identified in that it does not relate and/or cannot be traced back to the User specifically;
			* information collected and compiled by Department which is non-personal and statistical; and
			* information voluntarily provided by the User in an open, public environment or forum, which information is then open to unknown third parties and so does not enjoy the protections offered by clause 12 of these Terms and Conditions;

* + 1. **“Password”** means the confidential and unique sequence of numerals and/or letters, which forms part of the User Authentication System and enables the User to have access to aspects of ECOS;

* + 1. **“Promotion of Access to Information Act”** or **“POPIA”** means the Promotion of Access to Information Act 2 of 2000;

* + 1. **“Promotion of Administrative Justice Act”** or **“PAJA”** means the Promotion of Administrative Justice Act 3 of 2000;

* + 1. **“Protection of Personal Information Act”** or **“POPIA”** means the Protection of Personal Information Act 4 of 2013;

* + 1. **“State”** or **“Organ of State”** or **“Authority”** or **“Entity”** means, as the context may indicate, a local government or authority, a provincial government or authority or the national government or authority, or any other state entity of constitutional entity including, but not limited to, all institutions and entities referred to in the schedules to the Public Finance Management Act 1 of 1999;
		2. “**Terms and Conditions**” or “**T&C**” means these terms and conditions of use and the privacy policy contained herein, all of which may be amended by the Department, at its discretion, from time to time;

* + 1. “**User**” means any person (including natural and juristic persons) who has been provided with a User ID, and includes such person’s employees, agents and other authorised representatives;

* + 1. **“User Authentication System”** means the system by which the identification of the User is verified by means of a User ID and Password;

* + 1. **“User ID”** means the alphabetical and/or numerical identifier issued to the User, which forms part of the User Authentication System and enables the User to have access to aspects of the Department Online Regulation Systems;

* + 1. **“Virus”** means, in relation to ECOS, a Bug, device or thing (including any software, code, file or programme), which: (i) may prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network (including any computer software, hardware or network comprising ECOS), any telecommunications service, equipment or any other service or device; (ii) prevent, impair or otherwise adversely affect access to or the operation of any programme or data, including the reliability of any programme or data (whether by re-arranging, altering or erasing the programme or data in whole or part or otherwise); or (iii) adversely affect the user experience, including worms, Trojan Horses, viruses and other similar things or devices;

* + 1. “**Web Page**” has the meaning assigned in ECTA and “Webpage” has a corresponding meaning; and

* + 1. **“Web Site”** has the meaning assigned in ECTA and “Website” has a corresponding meaning.

* 1. Unless the context in these Terms and Conditions indicates a contrary intention, a word or expression which denotes –

* + 1. a gender includes the other genders;
		2. a natural person includes a juristic person and *vice versa*; and
		3. the singular includes the plural and *vice versa*.
	1. If any provision in a definition is a substantive provision conferring rights or imposing obligations on any Party, notwithstanding that it is only in the definition clause, effect shall be given to it as if it were a substantive provision in the body of these T&C.
	2. The cancellation or termination of this T&C shall not affect the provisions of this T&C which of necessity must continue to have effect after such cancellation or termination, notwithstanding that the clauses themselves do not expressly provide for this.
	3. The rule of construction that a contract shall be interpreted against the Party responsible for the drafting or preparation of it, in this case the Department, shall not apply to this T&C.
	4. Words and expressions defined in any clause shall, for the purpose of that clause, bear the meaning assigned to such words and expressions in that clause.

1. **INTRODUCTION**

* 1. The Department is the owner and operator of a Web Site accessible at <https://mygovapps.westerncape.gov.za> and through which Users can access ECOS.
	2. ECOS is owned and operated by the Department and used to, inter alia, process information.
	3. These Terms and Conditions apply to all Users in their access to, interactions with and use of ECOS.

1. **AMENDMENT OF TERMS AND CONDITIONS AND REMOVAL OF CONTENT**

* 1. The Department may change or modify these Terms and Conditions at any time in its sole and absolution discretion. The latest Terms and Conditions (whether amended from these Terms and Conditions or not) which are published by Department either on the Department’s Website or via ECOS, at the time of each Log-in by the User, shall be applicable to the User’s access to, interactions with and/or use of the Department Website and ECOS up and until the time of the User’s next Log-in.
	2. The Department shall be entitled to remove any and all content, material or information from the Department Website and/or the ECOS at any time.
1. **USER AUTHENTICATION PROCESS AND ACCESS TO ECOS**
	1. **Access to ECOS is restricted to those persons who have been approved by, or on behalf of, the Department and to whom a User ID has been issued. The Department shall be entitled to take all reasonable steps to validate the identity of and the information provided by any person who attempts to register as a User.**
	2. Subject to any Laws (including, but not limited to, the Consumer Protection Act), on no account shall the Department be obliged to accept any person’s application to register as a User and any such acceptance or approval shall be at the Department’s sole and absolution discretion.
	3. The User shall be required to enter its Password in order to access ECOS.
	4. **The User warrants and agrees that it shall:**
		1. **not disclose its User ID or Password to any third party whatsoever;**
		2. **not leave any device which has access to the Internet unattended and Logged-In unless the User has enabled a password-protected screensaver and such password is only know by the User;**
		3. **access ECOS only for its own personal or business purposes**; **and**
		4. **immediately notify the Department upon it becoming aware of, or reasonably suspecting that unauthorised access has been obtained to the User’s User ID and/or Password and shall take steps to mitigate any harm which may result therefrom.**

1. **FEES AND OTHER CHARGES DUE TO THE DEPARTMENT**

* 1. All fees and charges due to the Department by the User as per the Department Website or ECOS shall be paid in full (free of any deductions or the application of ‘set-off’), on demand, and via the processes and means so provided by the Department from time to time.
	2. A schedule of the applicable fees and charges shall be published by the Department and be accessible via the Department’s Website and/or ECOS.
	3. A User’s account and access to ECOS may be suspended and/or revoked if the relevant fees and charges have not been paid.

1. **INTELLECTUAL PROPERTY RIGHTS AND USE**

* 1. All Intellectual Property Rights in and to ECOS and all components thereof are the property of, or are licensed to, the Department.
	2. The User agrees that it shall -
		1. not do anything to infringe the Department’s Intellectual Property Rights or attempt to discover the source codes of any of the Department’s technology and ECOS, including but not limited to by reverse engineering, decompiling or dissembling such technology;
		2. not post, copy, reproduce, retransmit, distribute, disseminate, sell, publish or otherwise circulate or exploit the Department’s Intellectual Property (which includes but is not limited to ECOS); and
		3. comply with all laws applicable to the Department’s Intellectual Property Rights.
1. **THE DEPARTMENT’S OBLIGATIONS**
	1. The Department shall:
		1. use reasonable care and skill in making ECOS available to Users; and
		2. comply with all Laws insofar as they are applicable to the Department and/or ECOS.
	2. The Department may, from time to time, provide additional functionality in or through ECOS to accommodate the efficient transfer and re-use of data and information. This additional functionality does not constitute a responsibility on the part of Department to continue to provide this additional functionality and nor does it indicate acceptance of any related liability arising from a failure thereof.
2. **THE USER’S WARRANTIES, RESPONSIBILITIES, UNDERTAKINGS AND INDEMNITY**
	1. The User warrants and undertakes that itshall:
		1. maintain the confidentiality of its access to ECOS as well as the data, forms and templates provided by ECOS, or on the Department’s Website;
		2. only access ECOS for lawful purposes and in accordance with these Terms and Conditions;
		3. only use ECOS in a manner which is consistent with all relevant and applicable market and other requirements, and which assists in the transfer of data and information between approved agencies and Entities in the import/export supply chain;
		4. neither intentionally nor negligently upload, distribute or make available any Viruses, corrupted files or any other similar software or programs that may damage ECOS or any portion thereof;
		5. not copy, reproduce, translate, adapt or modify any aspect of ECOS;
		6. not decompile, dissemble or reverse-engineer any aspect of ECOS for any purpose;
		7. not write or develop any derivative of any software comprising of ECOS or similar any other software program based on such software or derived from it, in any way and for any purpose;
		8. not alter, infringe or erase the Department’s copyright, trademark (both registered and unregistered), service marks, logos and other proprietary notices on any complete or partial copies of ECOS or wherever else same appears; and
		9. ensure that the reputation and goodwill of the Department is in no way damaged through the User’s use of ECOS.
		10. Except and only to the extent that any Law limits or prohibits such indemnity (but otherwise, notwithstanding anything to the contrary contained in these Terms and Conditions), the User hereby indemnifies the Department against any and all claims, of any nature whatsoever, which might arise from personal injury, death, loss or damage to property or person, or any other claim of whatsoever nature, arising from negligence, gross negligence or any other cause howsoever, which any person may have or institute against the Department and where the cause of such claim can be directly or indirectly attributed to the User’s use of ECOS. **This indemnity shall survive termination of the User’s use of ECOS or termination of these Terms and Conditions for whatever reason.**
3. **NO WARRANTIES OR REPRESENTATIONS**

* 1. ECOS is (subject to the provisions of any Laws, as applicable, including the Consumer Protection Act) provided on an “as is” basis. Although the Department shall take all reasonable steps to ensure the availability, quality and accuracy of ECOS, its technology and the material, content and services available on and through it are supplied free of any warranties or guarantees.
	2. ECOS has not been compiled to meet the User’s individual requirements. It is the User’s responsibility to ensure that the ECOS meets its individual requirements and is compatible with its own technology.
	3. The Department does not make any warranties or representations that ECOS shall be available at all times.
	4. Certain links in ECOS may lead to resources maintained by third parties over whom the Department has no control. The Department makes no representations or warranties as to the accuracy of, or any other aspect relating to, those resources and does not necessarily endorse any view expressed within them.
1. **LIABILITY AND INDEMNITY**

**IMPORTANT NOTICE**

**The User is obliged to read the whole of this clause 10 carefully since it limits the Department’s liability in relation to these Terms and Conditions and use of ECOS. If the User does not understand any of the terms under this clause it is advised to obtain legal advice before using ECOS.**

* 1. **Despite anything to the contrary in this these Terms and Conditions, no term in these Terms and Conditions shall affect those legal rights of the User which cannot be lawfully limited or excluded in law, including, but not limited to, the User’s rights in terms of the Consumer Protection Act, to the extent that it is applicable.**
	2. **Except and only to the extent necessarily required by the Consumer Protection Act (if applicable), sections 43(5) and 43(6) of ECTA, and/or any other Law, and notwithstanding anything to the contrary contained in these Terms and Conditions, neither the Department nor its officials, agents, representatives, contractors or employees will be liable for any claim of any nature whatsoever which arises, directly or indirectly, from:**
		1. **Any actions or omissions by any of the Department’s employees, agents or contractors;**
		2. **the User’s use of or reliance on ECOS or any aspect thereof;**
		3. **the User’s use of or reliance on any information obtained from the Department’s Website or ECOS;**
		4. **the User’s acts or omissions or a breach by the User of these Terms and Conditions (including but not limited to a breach of the User’s warranties and undertakings as set out in clause 8);**
		5. **the Department acting on the User’s instructions;**
		6. **any mistake, error, use or omission in respect of information provided to the Department by the User;**
		7. **any Viruses; and/or**
		8. **the User’s inability to access or use ECOS for whatever reason.**

* 1. The Department will not be liable for any liability, loss or damage to the extent that such liability or damage is attributable to the Department’s breach of these Terms and Conditions or its unlawful acts or omissions.
	2. **Except and only to the extent necessarily required by the Consumer Protection Act (if applicable), sections 43(5) and 43(6) of the Electronic Communications and Transactions Act and/or any other Law and notwithstanding anything to the contrary contained in these Terms and Conditions, the Department will not be liable for any direct, indirect or consequential losses or damages whatsoever and howsoever they may arise in respect of anything done or omitted in good faith in the exercise of a power, or the performance of a duty under, or by virtue of, these Terms and Conditions, or in the rendering of any service in relation to ECOS or these Terms and Conditions or in respect of anything which may result therefrom.**
1. **LAWS AND GUIDELINES**

The User shall be entitled to all such rights and remedies as are granted to it under the Laws (insofar as they are applicable), subject to any lawful limitations on such rights and/or remedies as are contained in these Terms and Conditions.

* 1. In addition to the User’s rights as referred to in the clauses 12 and 13 of these Terms and Conditions, the User’s attention is particularly drawn to:
		1. its right to procedurally fair administrative action (to the extent that such action affects its rights or legitimate expectations) in terms of the Promotion of Administrative Justice Act; and
		2. its right to certain records in terms of and as determined in the Promotion of Access to Information Act; and
		3. its rights to protection of personal information as determined in POPIA.
1. **PRIVACY POLICY**
	1. All the Personal Information which the User provides to the Department via ECOS shall be protected by the Department’s Privacy Policy, which is set out in the remainder of this clause 12. The User’s use of ECOS is conditional upon its voluntary acceptance of the Department’s Privacy Policy.
	2. This privacy policy ensures that the Department:
		1. complies with the Protection of Personal Information Act 4 of 2013 (POPIA);
		2. protects the rights of data subjects (including the User);
		3. is transparent about how it stores and processes personal information of data subjects; and
		4. protects itself from the risks of a security breach.
	3. **By agreeing to these Terms and Conditions the User voluntary provides its consent to the Department for collecting, using, storing, processing and disclosing the User’s Personal Information within the bounds of the Department’s Privacy Policy. The User agrees that on the termination of the Terms and Conditions and/or the relationship between the Parties, Department may retain such of the information as has already been collected from the User but only for the purposes of (i) record-keeping; and (ii) such purposes as are set out in the clauses below.**
	4. **The User agrees that the Department may electronically collect, store and use the following Personal Information:**
		1. the information provided by the User in compliance with the Terms and Conditions and/or via the User Authentication System, which information shall include but not be limited to the User’s identity, contact details and employer;
		2. additional information provided by the User on a voluntary basis; and
		3. information such as the User’s computer Internet protocol address, browser type, browser version, the pages of the Department Website and the ECOS application which the User visits, the time and date of such visit, the time spent on those pages and other statistics and information, which may be automatically collected and recorded from the User’s system and interactions ECOS.
	5. **The Department collects such Personal Information: -**
		1. when the User actively submits such information to the Department (for example by means of the User Authentication System);
		2. via the User’s browser which sends such information to the Department whenever the User accesses ECOS;
		3. through the use of third party services or tracking technology that collects, monitors and analyses data (such as the data referred to in clause 12.3.2 above); and
		4. through Cookies. Cookies are sent to the User’s browser from a Website and stored on the User’s computer’s hard drive. The User may instruct its browser to refuse Cookies but then it may not be able to use some portions of ECOS.
	6. **The Department collects this Personal Information in order to fulfil a number of functions including but not limited to -**
		1. fulfilling its contractual and legal obligations;
		2. operate, maintain, enhance and provide all of the features of ECOS;
		3. manage and administer the User’s use of ECOS;
		4. verify the User’s identity and contact details;
		5. compile statistics and high-level reporting with regard to agriculture, food and food processing;
		6. for risk management purposes within the food chain including, but not limited to, for the conduct of risk analysis. This include sharing of such information with any International regulator or South African Regulator or Authority involved in the control/management or assessment of food safety risks;
		7. for sharing food chain information with the public in order to establish product origin and accreditations and standard applicable to the product and the locations where the product was produced; and
		8. comply with the Laws.
	7. **The User specifically gives Department permission to use the Personal Information for the abovementioned purposes.**
	8. The Department undertakes to follow reasonable and generally accepted standards and means in processing such information and to protect the User’s Personal Information, such as the use of firewalls, data encryption and other safeguards to its systems.
	9. **Notwithstanding the aforegoing undertaking, the User acknowledges that no method of transmission over the Internet, or method of electronic storage, is absolutely secure. The Department therefore does not guarantee the absolute security of the User’s Personal Information and it shall not be liable for any loss or damage sustained by the User due to the unlawful access to or dissemination of any of the User’s Personal Information by a third party or due to a loss of data during transmission or by any other means.**
	10. **The User gives the Department permission to disclose its Personal Information to the following third parties:**
		1. service providers who are appointed by the Department to provide administrative and communication services for the Department and on its behalf and/or to enhance ECOS;
		2. the officers, employees and agents of the Department; and
		3. any Person to whom the Department is required to disclose such information by Law.
	11. **The User also gives the Department permission to disclose its Personal Information and any and all information relating to food products, food safety and origin of products either produced, used, stored, or manufactured by the User, as well as all known producers or manufacturers of products used by the User, to the following third parties:**
		1. other regulatory bodies or entities within the food chain (for example NRCS);
		2. Organs of State relevant and related to the control of food products along the entire food chain (for example Department of Health);
		3. competent authorities of other countries responsible for ensuring compliance food safety regulations, laws and prescripts of that country; and
		4. any Entity or institution or regulatory body or authority which may require export related statistics of food or animal products, such as the South African Revenue Service, customs and excise, and law enforcement agencies, such as the South African Police Service.
	12. In addition to the terms and conditions stated above, the Department undertakes to comply with its obligations set out in the Privacy Policy Annexure attached to these Terms and Conditions.
2. **BREACH AND SUSPENSION**

* 1. Unless otherwise provided in these Terms and Conditions should either Party (**“Defaulting Party”**) breach any of the terms of these Terms and Conditions and fails to remedy the breach 7 (seven) days after delivery by the aggrieved Party (**“Aggrieved Party”**) to the Defaulting Party of a written notice requiring the Defaulting Party to remedy such breach, then the Aggrieved Party may, without prejudice to any other right or remedy which may be available to the Aggrieved Party in terms of these Terms and Conditions or in law, but subject to the indemnities and/or limitations of liability agreed to in these Terms and Conditions -
		1. immediately cancel this Agreement between the Parties and claim and recover from the Defaulting Party such damages (subject to the limitations of liability contained in these Terms and Conditions) as the Aggrieved Party has sustained as a result of such default, breach and/or cancellation; or
		2. institute action for specific performance of the provisions of these Terms and Conditions and/or for damages.
	2. Should either the Department or the User be successful in any legal claim against the other Party in the enforcement of its right/s in terms of these Terms and Conditions, such successful Party shall also be entitled to claim legal costs.
	3. Notwithstanding clause 14.1 or any other clause in these Terms and Conditions, the Department may at any time, unilaterally suspend and/or withdraw a User’s right to access ECOS should such User fail to comply strictly with these Terms and Conditions.
1. **TERMINATION IN TERMS OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT**

* 1. If the User is a consumer in terms of the Electronic Communications and Transactions Act and such Act is applicable, the User may cancel these Terms and Conditions and any related credit transaction without reason and without penalty within 7 (seven) days of agreeing to these Terms and Conditions, in which event the User will no longer be entitled to have access to ECOS.
	2. The termination or expiry of these Terms and Conditions will not affect those provisions of these Terms and Conditions which of necessity must continue to have effect after such expiry or termination, notwithstanding that the clauses themselves do not expressly provide for this.

1. **CIRCUMSTANCES BEYOND THE DEPARTMENT’S CONTROL (FORCE MAJEURE)**

* 1. The term “force majeure” in these Terms and Conditions includes: the downtime of any external telecommunications line, power failure, Virus, fire, explosion, flood, riot, war, terrorist attack, accident, act of God, embargo, legislation, regulation or directive having the force of law, civil commotion, unrest or disturbance, non-availability of electricity, labour disputes, strikes, lock-out or any other cause resulting in the impossibility of performance in terms of these Terms and Conditions which is beyond the Department’s reasonable control whether similar or dissimilar to the causes described above (**“Force Majeure Event”**).
	2. If the Department, despite its reasonable efforts, is prevented or hindered directly or indirectly by a Force Majeure Event from performing its obligations in terms of these Terms and Conditions, the Department shall be relieved of having to perform such obligations as a direct result of the Force Majeure Event.
	3. During the period that the Force Majeure Event exists and only to the extent that the Department is prevented or hindered from performing its obligations in terms of these Terms and Conditions, the Department will not be liable for any loss or damage whether direct, general, special, or consequential which the User may suffer as a direct result of the Force Majeure Event.

1. **CONFIDENTIALITY**
	1. The User shall not, during the currency of these Terms and Conditions, or at any time thereafter, utilise or cause to be utilised, and/or directly or indirectly publish or cause to be published or otherwise disclose or cause to be disclosed to any third party, any of the Confidential Information of the Department, government in any other sphere, or any government institution or organ of state.
	2. For purposes of this clause "Confidential Information" shall mean –
		1. any information disclosed, revealed or exchanged and which pertains to, but is not limited to, all Intellectual Property Rights, all trade secrets, all agreements (whether in writing or not) which exists at the time of revealing the content thereof to the User, the content of all possible future agreements which may be entered into with any other party, all knowledge obtained by way of research and development, irrespective of whether the aforementioned information that is revealed is applicable to technical, operational or financial aspects of the Department, government in any other sphere, or any government institution or organ of state;
		2. any information of whatever nature, which has been or may be obtained by the User, whether in writing or in electronic form or pursuant to discussions between the parties, or which can be obtained by examination, testing, visual inspection or analysis, including, without limitation, scientific, business or financial data or information, know-how, formulae, processes, designs, sketches, photographs, plans, drawings, specifications, sample reports, models, studies, findings, computer software, inventions or ideas;
		3. analyses, concepts, compilations, studies and other material prepared by or in possession or control of the User which contain or otherwise reflect or are generated from any such information as is specified in this definition;
		4. all information which a third party has in terms of any agreement made available to the Department and which has become known to the User in the course of having access to ECOS or thereafter; and
		5. any dispute between the Parties resulting from these Terms and Conditions;
	3. The User shall –
		1. use the Confidential Information only for its intended purpose and to comply with these Terms and Conditions;
		2. treat and safeguard the Confidential Information as private and confidential; and
		3. ensure proper and secure storage of all Confidential Information.
	4. Any documents or records (including written instructions, notes or memoranda) relating to ECOS or any organ of state, including the Department, or any third party which are to be provided to the User or which come into the User's possession during the currency of these Terms and Conditions, are deemed to be the property of the Department and shall be surrendered to the Department on demand, and in the event of the expiry or termination of these Terms and Conditions, the User will not retain any copies thereof or extracts therefrom without obtaining the prior written permission of the Department.
2. **GENERAL**

* 1. Neither Party may rely on or be bound by any representation, warranty, or promise that is not recorded in these Terms and Conditions.
	2. Subject to the Department’s rights in clause 3 above, no addition to, variation, novation or agreed cancellation of these Terms and Conditions shall be of any force or effect unless reduced to writing and signed by or on behalf of both the Department and the User.
	3. No waiver shall be of any force or effect unless reduced to writing and signed on behalf of both the Department and the User.
	4. No indulgence which either Party may grant to the other Party shall constitute a waiver of any of the rights of the grantor unless reduced to writing and signed by both Parties.
	5. The provisions of these Terms and Conditions shall bind the successors-in-title and the permitted assigns of the Parties.
	6. These Terms and Conditions supersede and cancel all prior agreements and or arrangements relating to the subject matter of these Terms and Conditions.
	7. The User may not assign or cede any of its rights or obligations in term of these Terms and Conditions without the Department’s prior written consent. The Department is entitled to cede, transfer and/or assign its rights and obligations in terms of these Terms and Conditions to its successor’s in title or to any third party without the consent of the User.
	8. Each term or condition of these Terms and Conditions is severable and in the event that any one or more of the terms and / or conditions is found to be unenforceable, then the remaining terms and conditions shall remain valid and enforceable.
	9. These Terms and Conditions shall be binding and enforceable by and against the estates, heirs, executors, administrators, trustees, assigns and liquidators of the Parties as fully and effectually as if they had signed these Terms and Conditions in the first instance and reference to any Party shall be deemed to include such Party’s executors, administrators, trustees, assigns or liquidators, as the case may be.

1. **INFORMATION DISCLOSED BY THE DEPARTMENT IN TERMS OF ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT**

|  |  |
| --- | --- |
|  **Full name and legal status:**  | Western Cape Government, Department of Agriculture  |
| **Office bearers:**  | Chief Information Officer Department of Agriculture Muldersvlei RoadElsenburgStellenbosch |
| **Place of business:**  | Muldersvlei RoadElsenburgStellenbosch  |
| **Website:**  | https://www.westerncape.gov.za/dept/agriculture  |
| **Physical Address for receipt of legal service:**  | Admin Building Muldersvlei RoadElsenburgStellenbosch  |
| **Postal Address:**  | Private Bag X1Muldersvlei RoadElsenburgStellenbosch7607 |
| **Email Address:**  | doa.info@westerncape.gov.za |
| **Contact Telephone Number:**  | 021 808 5111 or 021 808 5005 |
| **Website at which the Manual published in terms of section 14 of the Promotion of Access to Information Act is available:**  |  https://www.westerncape.gov.za/general-publication/paia-manual-2021 |

# **END OF TERMS AND CONDITIONS**

Attached: PRIVACY POLICY ANNEXURE

**PRIVACY POLICY ANNEXURE**

1. **Introduction**

The Western Cape Government Department of Agriculture(“Organisation”) needs to gather and use certain information about individuals and juristic persons, including the User (collectively referred to further as “data subjects”). These can include clients/customers, suppliers, business contacts, employees and other people the Organisation has a relationship with or may need to contact.

This policy describes how this information must be collected, handled and stored to meet the Organisation’s personal information protection standards and to comply with the law.

This policy must be read with the WCG Information Security Classification System (“ISCS”).

Definitions appear at the end for the meaning of terms used in this policy.

1. **Purpose**

This privacy policy ensures that the Organisation:

* Complies with the Protection of Personal Information Act 4 of 2013 (POPIA);
* Protects the rights of data subjects;
* Is open about how it stores and processes personal information of data subjects; and
* Protects itself from the risks of a security breach.
1. **Policy statement**

The Organisation is committed to protecting the privacy of data subjects in accordance with the obligations imposed by POPIA. POPIA describes how organisations must collect, handle and store the personal information of data subjects.

These rules apply regardless of whether the information is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected fairly, stored safely and not disclosed unlawfully.

POPIA is underpinned by the following important privacy principles. These say that personal information must:

* + be processed fairly and lawfully
	+ be obtained only for specific, lawful purposes
	+ be adequate, relevant and not excessive
	+ be accurate and kept up to date
	+ not be held for longer than necessary
	+ processed in accordance with the rights of data subjects
	+ be protected in appropriate ways
	+ not be transferred outside South Africa unless that country or territory also ensures an adequate level of protection
1. **Scope**

This policy applies to all the Organisation’s employees and any other person or entity working for or on behalf of the Organisation such as -

* + interns,
	+ volunteers,
	+ consultants, and
	+ contractors, suppliers or service providers, including their staff or agents.

It governs all business activities that involve the processing of personal information, including special personal information, for or on behalf of this Organisation. This can include -

* + names of individuals and juristic persons (together with any of the following),
	+ contact information such as postal and e-mail addresses and telephone numbers,
	+ biographical information such as date of birth, race, gender and marital status,
	+ any identifying number, location information or online identifier,
	+ biometric information such as fingerprints, and
	+ educational, medical, financial, criminal or employment history.
1. **Risks**

This policy helps to protect the Organisationfrom some very real security risks, including:

* **Breaches of confidentiality -** For instance, information being given out inappropriately.
* **Failing to offer choices -** For instance, all data subjects should be free to choose how the Organisation uses information relating to them where the personal information is not collected, used or shared in terms of a law or an agreement between the data subject and the Organisation.
* **Reputational damage -** For instance, the Organisation could suffer if hackers successfully gained access to the personal information of data subjects.
1. **Responsibilities**

Everyone who works for or with the Organisation has some responsibility for ensuring that the personal information of data subjects is collected, stored and handled appropriately to ensure the confidentiality, integrity and availability thereof.

Each Information End User, Information Owner, business unit and team that handles personal information must ensure that it is handled and processed in line with this policy and the privacy principles.

These people have key areas of responsibility:

1. The **Information Officer** is ultimately responsible for ensuring that the Organisation meets its legal obligations.
2. The Security Manager, or such other official as the Organisation may designate,is responsible for:
	* Keeping the Information Officer updated about information assets and personal information protection responsibilities, risks and issues;
	* Reviewing all personal information protection procedures and related policies, in line with an agreed schedule;
	* Arranging personal information protection training and advice for the people covered by this policy; and
	* Checking and approving any contracts or agreements with third parties that may collect, handle or store personal information on behalf of the Organisation.
3. The Information Officer’s delegate is responsible for dealing with requests from data subjects who want to see the personal information the Organisation holds about them (also called ‘data subject access requests’). The identity of anyone making a data subject request must be verified before disclosing any personal information.
4. The Information Custodian, or such other official as the Organisation may designate, is responsible for:
	* Ensuring all ICT assets used for processing personal information meet capable security standards.
	* Performing regular checks and scans to ensure security hardware and software is functioning properly.
	* Evaluating any third-party services the Organisation is considering using to process personal information. For instance, cloud computing services.
5. The Information Owner or such other official as the Organisation may designate, is responsible for:
	* Classifying personal information in line with WCG Information Security Classification System.
	* Maintaining internal procedures to support the effective handling and security of personal information.
	* Reviewing all personal information protection procedures and related policies, in line with an agreed schedule and make recommendations to the Security Manager where applicable.
	* Ensuring that all employees, consultants and others that report to the Information Owner are made aware of and are instructed to comply with this and all other relevant policies.
6. The Department’s Corporate Communications officer, or such other official as the Organisation may designate, is responsible for:
	* Approving any personal information protection statement attached to communications such as e-mails and letters.
	* Addressing any personal information protection queries from journalists or media outlets.
	* Where necessary, working with other business units to ensure all communication initiatives abide by the privacy protection principles.
7. **General staff guidelines**
8. The only people able to access any personal information covered by this policy should be those who **need it for their work**.
9. Personal information **should not be shared informally** and must never be shared over social media accounts such as Facebook, LinkedIn, Google Plus, etc.**.**
10. When access to confidential information is required, employees can request it from their line managers.
11. The Organisation **will provide training** to all employees to help them understand their responsibilities when handling personal information.
12. Employees should keep all personal information **secure**, by taking sensible precautions and following the guidelines set out herein.
13. In particular, **strong passwords must be used** and they should never be shared.
14. Personal information **should not be disclosed** to unauthorised people, either within the Organisation or externally.
15. Personal information must be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of in line with the disposal instructions.
16. Employees **should request help** from their line manager if they are unsure about any aspect of the protection of personal information.
17. Line managers should seek the assistance of Legal Services, Department of the Premier if they are unsure about any aspect of the protection of personal information.
	1. Collection

The Organisation collects information to support its service delivery mandate.

Personal information is collected directly from data subjects where practical and always in compliance with POPIA.

The types of information and the purposes for which personal information is collected is set out in the Organisations Privacy Notice.

* 1. Classification

The Information Owner classifies information in accordance with its legal requirements, value, criticality and sensitivity to unauthorised disclosure, modification or loss in terms of the WCG Information Security Classification System (“ISCS”) and as follows:

* Personal information is usually classified as CONFIDENTIAL.
* Special personal information and children’s information is usually classified as SECRET.

* 1. Use

When personal information is accessed and used it can be at the greatest risk of loss, corruption or theft. Therefore:

1. When working with personal information, employees should ensure **the screens of their computers are locked** when left unattended.
2. Personal informationshould **not be shared informally**.
3. All personal information sent over **e-mail** (as an attachment or in an email text) should be considered sensitive and protected as such. It should not be sent to someone outside of the Organisation unless it has been cleared by the line manager and Security Manager/IT/Other. This includes forwarding such e-mails to an employee’s own personal e- mail account.
4. Before sending e-mail to a co-employee confirm with the line manager that the recipient is allowed to have access thereto as not all users within the Organisation have access to the same information.
5. Data must be **encrypted before being transferred electronically**. The Security Manger/ IT Manager/Other can explain how to send data to authorised external contacts.
6. Personal information should **never be transferred outside of South Africa** without confirmation by the Security Manger/ IT Manager/Other that the country where it is transferred to ensures an adequate level of protection of personal information.
7. Employees **should not save copies of personal information to their own computers.** Always access and update the central copy of any personal information.
	1. Storage

These rules describe how and where personal information should be safely stored. Questions about storing personal information safely can be directed to the [Security Manager and/or Information Custodian/Other].

When personal information is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to personal information that is usually stored electronically but has been printed out for some reason:

1. When not required, the paper or files should be kept **in a locked drawer or filing cabinet.** Where the information is classified as **SECRET** **access** to the environment should be **restricted** and logged.
2. Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer or photocopier.
3. **Printouts that contain personal information should be shredded immediately** and disposed of securely when no longer required.

When personal information is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

1. All electronic storage requires access controls equal to those in production and file protection mechanisms such as **encryption** should be employed.
2. All electronic access must be **logged**.
3. Personal information should only be stored on **designated drivers and servers**, and should only be uploaded to **approved cloud computing services.**
4. Storing personal information on any other physical devices, including but not limited to USB drives (memory sticks), external hard drive, CD or DVD must be **pre-approved** by the [Security Manager/IT Manager/Other].
5. If personal information is **stored on removable media** (like a memory stick, external hard drive, CD or DVD) the files should be encrypted, password protected and the media should be locked away securely when not being used.
6. USB drives (memory sticks) that are found or have been handed out as a promotional item should not be plugged into any computer as these devises may contain hidden malware or viruses.
7. All lost or stolen devices (including removable media) must immediately be reported to the line manager [and the Security Incident Notification document completed].
8. Servers containing personal information should be **sited in a secure location,** away from general office space.
9. Electronic files that contain personal information should be **backed up frequently.** Those backups should be tested regularly in line with the Organisations standard backup procedures.
10. All servers, computers and other electronic devices containing personal information should be protected by **approved security software and a firewall.**
	1. Data accuracy

The law requires the Organisation to take reasonable steps to ensure personal information is kept accurate and up to date.

The more important it is that personal information is accurate, the greater the effort the business unit should put into ensuring its accuracy.

It is the responsibility of all employees who work with personal information to take reasonable steps to ensure that it is kept as accurate and up to date as possible.

1. Electronic files that contain personal information will be held in **as few places as necessary.**  Staff should not create any unnecessary additional data sets.
2. Staff should **take every opportunity to ensure personal information is updated.**  For instance, by confirming a client’s details when they call.
3. The Organisation will make it **easy for data subjects to update their personal information** the Organisation holds about them. For instance, via its website.
4. Personal information should be **updated as inaccuracies are discovered.**  For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
	1. Disposal

Working papers and copies that may be disposed of in terms of a general disposal instruction must be disposed of by using a secure disposal container or shredder.

Copies of personal information, including special personal information, classified as **SECRET** that is **stored electronically** must either be permanently destroyed or overwritten.

The disposal of all original files and electronic files must be performed in accordance with the Organisations Records Management Policy.

1. **Data subject access requests**

All data subjects whose personal information is held by the Organisation are entitled to:

* ask **what information** the Organisation holds about them, why and with who it is shared;
* ask **how to gain access** to it;
* be informed **how to keep it up to date**; and
* be informed how the Organisation is **meeting its obligations in terms of POPIA.**

If a data subject contacts the Organisation requesting this information this is called a data subject access request.

Subject access requests from data subjects should be referred to the [Deputy Information Officer/Other].

1. **Disclosing (sharing) personal information**
	1. Internal disclosure

In general, personal information is shared within the Organisation where legally permitted for reasonable and appropriate business purposes. However, even within the Organisation access is restricted to those employees or third parties who need access to carry out their assigned functions.

* 1. External disclosure

External to the Organisation disclosure is only made pursuant to an agreement, as permitted or required by law or legal process, or with the consent of the data subject.

POPIA allows personal information to be shared if it involves national security or criminal activities without the consent of the data subject. Under these circumstances the requested personal information will be disclosed. However, the [Security Manager/Deputy Information Officer/Other] will ensure that the request is legitimate and in line with POPIA, seeking assistance from [Legal Services, Department of the Premier/Other] where necessary.

1. **Notification to data subjects**

The Organisation aims to ensure that data subjects are aware that their personal information is being processed, and that they understand how the personal information is being used, what their rights are in terms of POPIA and how to exercise their rights.

To these ends, the Organisation has a privacy notice, setting out how personal information relating to a data subject is collected and used by the Organisation.

This is available on request.

1. **Enforcement**

Non-compliance with this policy by the Organisations employees will be dealt with in accordance with the relevant disciplinary processes of the Organisation. Consequences may include disciplinary action up and to termination of employment, and/or legal proceedings to recover any loss or damage to the Organisation, including the recovery of any fines or administrative penalties imposed by the Information Regulator on the Organisation in terms of POPIA.

Non-compliance with the policy by any other third party processing personal information on behalf of the Organisation will be dealt with in accordance with the agreement entered into between the Organisation and such third party. Consequences may include the recovery of any fines or administrative penalties imposed by the Information Regulator on the Organisation in terms of POPIA.

1. **Review and Update**

This policy will be reviewed and updated as required by the Organisation.

If any regulatory or business changes result in a significant addition or change to the nature or handling of personal information that may require a review of this policy the changes will be developed by the relevant officials and approved by the Information Officer.

Any questions and requests to update the policy should be directed to the Organisation’s Security Manager.

1. **Definitions**

|  |  |
| --- | --- |
| **Data subject** | Means the identifiable natural/juristic person to whom personal information relates and includes the User of the ECOS system |
| **Information assets** | Means the assets the Organisation uses to create, store, transmit, delete and/or destroy information to support its business activities as well as the information systems with which that information is processed.It includes:* All electronic and non-electronic information created or used to support business activities regardless of form or medium, for example, paper documents, electronic files, voice communication, text messages, photographic or video images.
* All applications, devices and other systems with which the Organisation processes its information, for example telephones, fax machines, printers, computers, networks, voicemail, e-mail, instant messaging, smartphones and other mobile devices (‘ICT assets’),
 |
| **Information custodian** | Means the person responsible for defining and implementing security measures and controls for Information and Communication Technology (‘ICT’) assets. |
| **Information end user** | Means a person that interacts with information assets and ICT assets for the purpose of performing an authorised task. |
| **Information officer** | Means the Director-General in the case of the Department of the Premier and the Accounting Officer in the case of the other provincial departments. |
| **Information owner** | Means a person responsible for, or dependent upon the business process associated with an information asset. |
| **Personal information** | Means information relating to an identifiable, living, natural person, and were it is applicable, an identifiable, existing juristic person, including, but not limited to –1. Information relating to the race, gender, marital status, nationality, age, physical or mental health, disability, belief, culture, language and birth of the person;
2. Information relating to the education or the medical, financial, criminal or employment history of the person;
3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person
4. the biometric information of the person;
5. the personal opinions, views or preferences of the person;
6. 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
7. the views or opinions of another individual about the person; and
8. 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.
 |
| **Processing** | Means any **operation** or activity or any set of operations concerning personal information, including:1. the collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, alteration, consultation or use;
2. dissemination by means of transmission, distribution or making available in any other form; or
3. merging, linking, as well as restrictions, degradation, erasure or destruction of information.
 |
| **Special personal information** | Means personal information as referred to in section 26 of POPIA. |