Transport Canada Transports Canada

Staff Instruction

Subject: **Drone Management Portal (DMP)**

Issuing Office:	Civil Aviation, Strategy and Emerging Technologies	Document No.:	SI 901-004
File Classification No.:	Z 5000-32	Issue No.:	01
RDIMS No.:	21260140-V3	Effective Date:	2026-06-25

Table of contents

1.0 Introduction 3
1.1 Purpose 3
1.2 Applicability 3
1.3 Description of changes 3
2.0 Reference documents 3
2.2 Cancelled documents 3
2.3 Definitions and abbreviations 3
3.0 Background 4
4.0 Internal users 5
4.1 Internal DMP access 5
4.2 Internal DMP navigation 5
5.0 Accounts 7
5.1 Overview 7
5.2 Personal account – Canadian citizen / permanent resident of Canada 7
5.3 Personal account – foreign operator 8
5.4 Business Account 8
5.5 Verification of account ownership procedure 9
5.6 Signs of possible fraud 9
6.0 Internal access actions 10
6.1 Overview 10
6.2 Disposal of Transitory Personal Information 10
6.3 Prerequisites 10
6.4 Citizenship adjustments 10
6.5 Date of birth adjustments 11
6.6 Exam resets 11
6.7 Account resets 12
6.8 Certificate of registration adjustments 13
7.0 External access actions 13
7.1 Overview 13

7.2 Purchases 13
7.3 Exams 13
7.4 Flight review submissions 13
7.5 Contact information permissions 14
8.0 Strategy and Emerging Technologies Directorate actions 14
9.0 Duplicate accounts 15
10.0 Refusal of client inquiries related to the DMP 15
11.0 Information management 16
11.1 Digital records 16
11.2 Physical records 16
12.0 Document history 16
13.0 Contact us 16

1.0 Introduction

1.1 Purpose

(1) This Staff Instruction (SI) describes the procedures associated with the Drone Management Portal (DMP). These procedures are to be followed by Transport Canada (TC)'s Service Team Support Staff when:

(a) Answering general questions/inquiries from clients related to the DMP

(b) Changing/updating information on the client's DMP account.

1.2 Applicability

(1) This document applies to the National Transport Canada Civil Aviation (TCCA) Service Team Support staff.

1.3 Description of changes

(1) Not applicable.

2.0 References and requirements

2.1 Reference documents

(1) It is intended that the following reference materials be used in conjunction with this document:

(a) *Aeronautics Act* (R.S.C., 1985, c. A-2)

(b) Part IX, Subpart 1 of the *Canadian Aviation Regulations* (CARs) — Small Remotely Piloted Aircraft and Medium Remotely Piloted Aircraft

(c) Part IX, Subpart 3 of the *Canadian Aviation Regulations* (CARs) — Special Flight Operations – Remotely Piloted Aircraft Systems

(d) Standard 921 — Remotely Piloted Aircraft – Canadian Aviation Regulations (CARs)

(e) Transport Canada Publication (TP) 14371, TC Aeronautical Information Manual (Transport Canada AIM) — Remotely Piloted Aircraft

(f) Knowledge Requirements for Pilots of Remotely Piloted Aircraft Systems, 250 g up to and including 150 kg, Basic and Advanced Operations – TP 15263

(g) Regulations Amending the Canadian Aviation Regulations (CARs) issued in Canada Gazette Part II (March 26, 2025), governing Level 1 Complex – SOR/2025-70

(h) FAQ For Part IX of the CARs – RDIMS #14541555

(i) Drone Management Portal (e-Learning) – TCCampus, Product code: CIV_DMP

2.2 Cancelled documents

(1) Not applicable.

2.3 Definitions and abbreviations

(1) The following **definitions** are used in this document:

(a) **Configurable element**: A system that can be added to an RPA to enhance aspects of the operation.

(b) **Exam instance**: The breakdown of the knowledge points of a completed exam and summary of results

(c) **Medium RPA:** An RPA with an operating weight of more than 25 kg but not more than 150 kg

(d) **Micro RPA**: An RPA with an operating weight of less than 250 g

(e) **Safety Assurance Declaration**: A declaration made by the manufacturer of an RPA or configurable element that legally declares the system meets the criteria set out in the regulations to be used in the operational environment specified.

(f) **Small RPA**: An RPA with an operating weight of at least 250 g, but not more than 25 kg

(2) The following **abbreviations** are used in this document:

(a) **BVLOS**: Beyond Visual Line-of-Sight

(b) **CARs**: Canadian Aviation Regulations

(c) **DMP**: Drone Management Portal

(d) **RPA**: Remotely Piloted Aircraft

(e) **RPAS**: Remotely Piloted Aircraft System

(f) **RPOC**: RPAS Operator Certificate

(g) **SFOC**: Special Flight Operations Certificate

(h) **SFOC-RPAS**: Special Flight Operations Certificate of a Remotely Piloted Aircraft System

(i) **VLOS**: Visual Line-of-Sight

3.0 Background

(1) In 2019 Part IX of the *Canadian Aviation Regulations* was released governing Remotely Piloted Aircraft Systems (RPAS) from 250 g to 25 kg in weight. All previous guidance and policies related to RPAS, model aircraft, unmanned aerial vehicles, and drones were superseded by the new regulations. No grandfathering of previous exemptions and permissions or interim regulations was permitted.

(2) To implement the new regulations, DMP, a digital web-based application, was developed to facilitate exam delivery, submission of manufacturer's safety declarations, and the issuance of pilot certificates and Remotely Piloted Aircraft (RPA) registrations. The DMP also enabled payment of applicable fees for pilot certificates and certificates of registration.

(3) To comply with the new regulations, RPAS pilots must obtain the appropriate pilot certificate (Basic Operations, Advanced Operations, or Level 1 Complex Operations) and hold an RPAS Operator Certificate (RPOC) for complex or beyond visual line-of-sight (BVLOS) operations. The RPAs being operated must be registered and, if operated under Advanced Operations or Level 1 Complex Operations, the RPA must have an appropriate manufacturer's Safety Assurance Declaration.

(a) These requirements do not apply to micro-RPA (under 250 g), which are exempt from registration, pilot certification, and Safety Assurance Declaration requirements.

4.0 Internal users

4.1 Internal DMP access

(1) Service Team Support staff require access to the internal DMP to make edits to the information within the system. To obtain access, email the Strategy and Emerging Technology Branch (SET - formerly known as the RPAS Task Force) inbox to make the request as soon as possible once inducting a new team member who will be addressing RPAS inquiries. This request should include:

- (a) name of Service Team Support member
- (b) email of Service Team Support member
- (c) operational role:
  - (i) Oversight: Supervisors or management may need access to the information in the DMP for tracking changes made by team members but do not need to make changes within their role.
  - (ii) National Service Team Support: Service Team Support staff will be helping clients directly with their accounts and will need access for the ability to make direct changes in the DMP.
- (d) Access can take some time to be processed depending on workload, as with all tech support requests. Once granted, a link to the internal DMP will be provided.

4.2 Internal DMP navigation

(1) The primary use of the internal DMP for Service Team Support staff will be to access accounts to confirm information and make changes to the account and the documents therein. While completion of the online training session is recommended, below are the steps needed to reach a client's account:

- (a) From the welcome page, hover over the accounts drop down box, and select search for an account.
- (b) Input the information of the account holder.
  - (i) Less is more. This is a keyword search, so if information is inputted incorrectly, or not all the information matches perfectly (for example, the client provides a middle name but there isn't one listed on the account) it will not turn up any results.
  - (ii) First/last name or email are the recommended search options. Name might turn up more results, but if a client has accidentally created multiple accounts with multiple emails, this will also provide more information and help with communicating with the client.
  - (iii) Using a personal name will generate results for both business accounts and individual ones, but using business information will not pull up any individual accounts.
- (c) Change the country drop down from Canada to all countries.
  - (i) This step is not necessary if a reference number is being used to search rather than contact information.
- (d) Select search.
- (e) Find and select the account that matches the information provided by the account owner.

(i) Name, account number, address, phone number, and email are all listed in the search results. Cross checks the information to narrow down the list.

(ii) There may be more than one account that has matching information. This means the account owner has created multiple accounts. Some further investigation/information might be needed to resolve the issue the client is experiencing or to narrow down which account the client is having issues with.

(iii) As organizations can register RPAS, there may be a mix of personal and business accounts. These will be separated by tabs labeled accordingly at the top of the search results.

(f) On an individual account, there will be up to 6 tabs visible on the account that can be moved between. These include:

(i) Account details – Contains all the details of the account owner, such as name, phone number, email, date of birth, address, and citizenship or residency status.

(ii) Services – Contains any document information the account owner might have acquired throughout their usage of the DMP, including number of registrations, pilot certificate number, RPOC number, most recent passed exam number of each level, most recent passed flight review, and (if applicable) any flight school associations. Each of these items will have a link to further details pertaining to their respective subjects. So, if more details are needed from their certificate(s) of registration, select the number and a page will load that lists all the RPAS the individual or organization has registered.

(iii) Activity history – A list of the historical actions taken on the account. Includes any actions taken by the account owner and by TC, specifying which made the change. Only track actions that change the information on the account in some way, such as transactions or edits to data.

(iv) Notifications – A list of all automated emails that have been sent by the DMP to the email address on the account, as well as when the notification was sent.

(v) Related accounts – Only visible if there is a business account related to the personal account in the DMP. Lists all related other accounts the account owner has access to.

(vi) System – Specifies the last time someone has logged into this account and contains the account reset button.

(g) On a business account, there will be 5 tabs visible on the account. These include:

(i) Account details: Contains all the details of the business, such as legal name, operating name, business number, and address.

(ii) Services: Contains the quantity of registered and deregistered RPAS the business has processed throughout their time on the DMP, as well as the associated RPOC number. Each of these numbers is a link to further details pertaining to their respective subject. So, if more details are needed from their certificate(s) of registration, select the number and it will load a page that lists all the RPAS the individual or organization has registered.

(iii) Activity history: A list of the historical actions taken on the account. Includes any actions taken by any associated individuals and by TC, specifying if the latter made the change. Only track actions that change the information on the account in some way, such as transactions or edits to data.

(iv) Notifications: A list of all automated emails that have been sent by the DMP to the email list on the account, as well as when the notification was sent.

(v) Account access: A list of all individual accounts that maintain access to the business account. For a business account to exist in the DMP there must always be at least one individual account with full access to the business account. There is no limit to the number of people who can be associated with a business account. Some personal information on each individual is listed here, along with their access type, last login, some action buttons, and a link to their individual accounts.

5.0 Accounts

5.1 Overview

(1) The DMP is primarily an external use system. The main objective of all National Service Team Support members should be to assist clients with navigating the DMP and related resources to effectively engage with RPA in a legal and safe manner. Apart from the situations detailed in this SI, clients should be encouraged to perform actions themselves, and the emphasis should be on assisting clients on how to find answers for their inquiries.

(2) A key educational resource is TC's Drone Safety website. All procedures are described in detail there, and at any time it is possible to do so; clients should be directed to the instructions laid out on that forum. This is to ensure that all clients receive consistent information.

(3) To best help the clients, a basic understanding of how the DMP account type of function is important. While the Service Team Support members should undergo practical training, a summary of the different accounts is provided below.

5.2 Personal account – Canadian citizen / permanent resident of Canada

(1) The most common type of account on the DMP is the personal account for Canadian citizens and permanent residents of Canada. This account type grants clients access to the processes required to obtain RPAS related CADs and the associated documents therein, as well as the space to store the documents after acquisition. (as laid out in the CARs Part IX and the related standards). These include:

(a) RPAS exams

(b) exam knowledge breakdowns

(c) certificates of registration

(d) RPAS pilot certificates

(e) flight reviews

(f) RPOCs

(g) Transaction information (including receipts)

(2) This is the central hub in which an individual should compile and update all necessary information to meet the CARs and related standards requirements. The only key documents inaccessible to the DMP are a handful of recency documents and SFOCs. This is due to the documents being sourced from external resources (e.g. Standard 921.04 for more details on these items). The onus is on the pilot to provide proof of recency if requested.

(3) The only person who should have access to the login information for these accounts should be the account owner. Discourage all sharing of this information. Since the login information is controlled by an external agency (GCKey & Sign-in Partner), even Service Team Support members should not have access to these details.

5.3 Personal account – foreign operator

(1) This account type is designed for individuals operating RPAS in Canadian airspace without a Canadian citizenship or permanent residency within Canada. Typically, this is someone visiting the country or residing here on a temporary visa. A foreign operator does not require a Special Flight Operations Certificate of a Remotely Piloted Aircraft System (SFOC-RPAS) if piloting a Canadian-registered RPAS. However, an SFOC-RPAS is required in two cases:

(a) When operating a foreign registered RPAS in Canadian airspace (as RPAS cannot be registered in more than one country).

(b) When conducting operations that require an RPOC under CAR 901.213(a).

Note: Exceptions may apply for certain business operators under free trade agreements, but these do not extend to personal accounts.

(2) Foreign operator accounts can hold exams, pilot certificates, flight reviewer ratings, and flight reviews. However, foreign operator accounts cannot hold certificates of registration or RPOCs as both certifications are legally restricted. In place of these features, an advisory is provided directing the operator to apply for the required SFOC-RPAS instead.

(a) Micro RPA do not need to be registered. This applies to foreign operators as well as Canadian citizens, and permanent residents of Canada. If a foreign operator contacts TC about the regulations regarding micro-RPA, direct the client to the resource outlined below.

(b) Drone Safety website → Drone pilot licensing → Getting permission for special drone operations → Apply for a foreign pilot or operator SFOC-RPAS → Drones under 250 g

(3) If an individual's status changes and they become a citizen or permanent resident of Canada, their account can be updated accordingly. The client must contact the Service Team Support member to initiate the process. The details on this process are addressed in Section 7.0 of this SI.

5.4 Business Account

(1) If an organization wishes to register their RPAS or hold an RPOC, as per the CARs, a representative of the organization can do so by registering a business account. The organization does not necessarily have to be a legally registered business to have a business account on the DMP. While these are called business accounts, any organizational structure meeting the requirements outlined in the CARs Part IX can have a business account to fulfill their needs.

(2) Only individuals are eligible to hold an RPAS pilot certificate. Consequently, exams, exam instances, and pilot certificates are not available on business accounts.

(3) A Business Account must always have a minimum of one personal account with full access to it. There is no upper limit to the number of personal accounts that can have access to it. The individual(s) with full access have decision-making authority over the actions taken on the business account and serve as the point of contact for any arising issues.

(4) While the full access user does have a lot of control over the account and the certificates therein, this does not necessarily mean they have automatic liability for what happens with the operations performed. The full access user is primarily the contact point and decision maker of the organization when it comes to RPAS related issues.

5.5 Verification of account ownership procedure

(1) To make any edits to a client's account internally, first verify that the client being communicated with is the owner of the DMP account. To proceed, verify that at least two of the following pieces of information match what is listed on the account in question:

- (a) full name
- (b) email
- (c) phone number
- (d) address
- (e) pilot certificate number
- (f) registration number(s)
- (g) flight review number(s)
- (h) exam number(s)
- (i) operator certificate number

(2) Verifying this information can be done by analyzing the initial email for pieces offered in the communications, or by directly asking the client for information from the list above.

(3) Verifying ownership of a business account:

- (a) The client must have full access to the business account (listed under the business account's account access tab).
- (b) The linked individual account can be where the rest of the verified information comes from, or it can be matched with the details listed under that individual name on the business account.
- (c) Ownership of a business account does not allow the client to make changes to other individual accounts listed under the account access tab. Additionally, a client cannot make requests on another individual's behalf. As such, no movement of RPAS certificates of registration between the business and individual accounts can be made without direct permission from the business account owner and the individual account owner. These may be the same person, or it may be multiple people. Always verify the information on all accounts in question before making any changes.
  - (i) A one-way transfer from a personal account to a business account is possible, and the client can make this change directly through their DMP account. However, if a business owner is looking to transfer RPA(s) from a business account to a personal account, this transfer can only be completed internally by TC staff.

5.6 Signs of possible fraud

(1) If a client is asking for a change to be made to the date of birth on an account and there are signs that they have changed all the other personal details to an entirely new set of information (or are requesting this along with the date of birth changes), this is a sign of fraud and no edits should be made. The reasons for this are:

- (a) A client changing all their personal details still cannot change the day they were born. As such, even if the client does make changes to their name, contact details, and residence, there is no reason they should require an updated birth date.

(b) To change certificates of registration between entities, the certificate must be transferred or deregistered and then reregistered.

(c) The change of birth date has no effect on an RPAS pilot certificate. This is required information should there be a potential enforcement action, not information that is reflected on the certificate itself.

(2) If a client claims to have permission from an account owner to make changes to an account, service team support members should not make any changes. If changes need to be made, service team support members may contact the individual in question, using the details on their account, for approval. If the details on their account are out of date, it is up to the account owner to contact TC if there are issues related to accessing their account. Do not accept contact details that are obtained from anywhere but the DMP to talk to the person in question.

6.0 Internal access actions

6.1 Overview

(1) There are a handful of actions that can only be performed by a Service Team Support member. These are allocated to internal access actions due to their sensitive nature. The information in the items below has limited reasons for modifications, and edits should only be done if the requirements are met.

6.2 Disposal of Transitory Personal Information

(1) When performing internal access actions, staff may temporarily handle personal information provided by clients. In accordance, with Transport Canada's Information Management Directive, any transitory records containing personal information must be securely and irretrievably deleted once no longer required for the action, in order to prevent unauthorized access, use, or disclosure.

6.3 Prerequisites

(1) Verify that the client making the request is the owner of the account using the details outlined in Subsection 6.1 of this SI.

6.4 Citizenship adjustments

(1) Changing one's citizenship is a rare and lengthy process. Because it occurs so infrequently, TC requires proof when such a change is requested. This is due to the potential increase in violations of CARs by individuals who might decide to misrepresent their status after realizing the restrictions associated with being a foreign operator. If a client contacts a Service Team Support member to request a change in citizenship, the client must provide valid proof of Canadian citizenship or permanent residency of Canada. Any one of the following documents, if issued by Canada, is acceptable:

(a) citizenship certificate

(b) citizenship Card

(c) birth certificate

(d) passport

(e) permanent resident card

(2) If a client has mistakenly indicated they are a Canadian citizen or a permanent resident of Canada, but are not, no proof is required to update their account. This type of change only adds restrictions to their ability to operate RPAS in Canadian airspace and therefore does not increase the risk of regulatory violations.

(3) If either of the above conditions are met, make the requested changes to the account. To do so:

(a) Find the correct account

(b) Select the account details tab

(c) Select edit account details

(d) Select the drop-down box under Canadian citizen or permanent resident

(e) Select yes or no as appropriate

(f) Select save changes.

(4) If the account has any RPAS registered, the RPA must be deregistered before the change can be made. Deregistration requires permission from the account owner and is not refundable. The same will apply for RPOCs; however, at this time only the technical team can remove an RPOC from an account.

6.5 Date of birth adjustments

(1) At no point in time is it possible for a client's date of birth to require a change. As such, there are two situations that would result in the need to change this information:

(a) Accidental input of incorrect information, such as account opening date or official languages reversion (e.g.: Jan 5th or May 1st)

(b) Fraudulent actions

(2) Due to the latter issue, if a client wishes to change the date of birth on their account, they must provide a valid government document that lists their date of birth. The document information should match the information listed on the account.

(3) If the client meets the above requirement, make the necessary change to the account. To do so:

(a) Find the correct account

(b) Select the account details tab

(c) Select edit account details

(d) Enter the birth date as specified on the government document

(e) Select save changes.

6.6 Exam resets

(1) Exams are non-refundable purchase and should only be reset or refunded if the client experiences a technical issue while taking the exam that originates from within TC's network of systems.

(2) In addition to the client experiencing a technical issue originating from within TC's network of systems during the exam, the following conditions must also be met:

(a) The client has not passed the exam

(b) The client has not purchased any newer exams of the same level

(3) A full overview of the exam reset requirements can be found in SI 901-002. Please ensure the client's information has been verified before proceeding with a reset. If the criteria are met, the Service Team Support member can perform an exam reset. To do so:

(a) Find the correct account

(b) Select the services tab

(c) Select view all exam results

(d) Under the action column, select allow retake. This option will only be visible next to the most recently taken exam of each level. Make sure the exam being reset is the exam that was referred to in the issue report.

(e) Exam resets do not result in an automated email, so the Service Team Support member must inform the client if one has been performed.

6.7 Account resets

(1) If a client has forgotten their login information and cannot recover it on their own, the Service Team Support member can reset it. This will allow the client to create a new login for all future use with the account. The new login chosen will replace the old one. It should be recommended to the client that they ensure the login information is kept in a secure location for future use.

(2) To reset the account:

(a) Find the correct account.

(b) Confirm that the email listed on the account is up to date and accessible by the account owner.

(i) Update the email if it is not.

(c) Select the system tab.

(d) Select reset account.

(e) An automated email will be sent to the client (a copy of which can be found under the "Notifications" tab). The link in the email is valid only for 24h. If the client does not reset their login information within 24h of the email being sent, repeat steps a - d. Should the client not reset their login within 24 hours, another reset can be requested. Throughout, the content of the client's file remains whole.

(f) The client must follow the instructions in the email as specified. If the client does so correctly, the login information associated with the account will be changed to the new information that has been inputted. This is the login that must be used to access the account from this point on.

(i) Service Team Support members should not request new login information from any client. TC does not have access to the login used on the DMP, as authentication is managed through GCKey and their banking partners.

(ii) Accessing the DMP is often infrequent for clients, so it is worth advising them to have a secure place to store the login data separately for future access attempts.

(g) If a customer stops responding to communications after a reset email is sent, a service team member can check if the issue is resolved by checking the time and date shown in the "Service" tab. If their last login was after the reset email was sent, this means they have regained access, and the issue should be considered resolved.

6.8 Certificate of registration adjustments

(1) Several processes related to certificates of registration are accessible only through internal access. These include:

(a) Transferring a certificate of registration from a business account to a personal account

(b) Deregistering an RPAS for select reasons.

(i) Business amalgamated or ceased operations

(ii) Lost (60 days or longer)

(iii) Owner no longer qualified under section 900.13

(iv) Registrant died

(v) Stolen

(c) Editing the make and model of an RPAS.

(2) These processes are restricted to minimizing a person's ability to supersede processes outlined in the CARs Part IX and related standards, and to recoup administrative costs. Refer to SI 901-001 for detailed information on these processes.

7.0 External access actions

7.1 Overview

(1) Just like there are some actions only internal access users can make, there are also specific actions only the account owners themselves can make. Below are the items that must be completed by the account owner. The Service Team Support members can only provide informational assistance.

7.2 Purchases

(1) All purchases, regardless of type, must be completed by the account owner. The process of each type of purchase is accessible on the Drone Safety website and detailed throughout the purchasing process in the DMP.

(2) Payments cannot be made on behalf of the client. The entire process, including payment, is digital. There is no phone or physical alternative to the online payment system.

7.3 Exams

(1) Exams must be completed solely by the account owner. No assistance should be given with the exam content. The client can be directed to resources such as schools, study guides, and/or knowledge guides. Any inquiries requesting specific answers to exam questions should not be addressed.

7.4 Flight review submissions

(1) Flight reviews must be submitted to the DMP by the flight reviewer. If an individual has completed a flight review and experiences delays in the process, they must contact their reviewer directly. The Service Team Support member cannot submit a document on behalf of a user. Official complaints about a flight school or flight reviewer should be sent on to the SET flight school inspector for review.

7.5 Contact information permissions

(1) When creating a business account, the individual will be asked for consent to disclose their business contact information. This feature exists to help prevent the creation of duplicate business accounts, but as it pertains to privacy, we allow clients to opt out. Only the individual can choose to opt in/out after the creation of the business account. This minimizes TC's liability by removing the possibility of accidental changes. If an account owner wishes to modify that option, they can do so under account settings in their business account.

8.0 Strategy and Emerging Technologies Directorate actions

(1) There are a few actions that remain under the purview of the SET. This is because the subjects SET covers require consistent oversight or dealing with subjects that have yet to be fully expanded. If any of the following items are encountered and there is no relevant information pertaining to the subject in the FAQ or on the Drone Safety website, forward the inquiries on to the contact point currently being used within SET:

(a) Accessibility requests: Some clients have accessibility needs that require adjustments to the administrative standards laid out (most commonly time extensions on exams). Due to the sensitive and variable nature of these requests, they are currently being processed by a dedicated team in the SET Branch and should be sent to the RPAS info inbox. Over time, these may be given to the Service Team Support members as standards are established.

(b) Document suspension and cancellation: This action is reserved solely for inspectors. Send any requests for the voluntary surrender of a pilot certificate or an RPOC to the RCE inbox for processing.

(c) Exam review requests: To ensure TC exams are relevant and accurate we conduct oversight into questions that are reported as being problematic. If a client reports that a specific question on their exam was incorrect and requires review, the inquiry should be sent to the RPAS info inbox for processing by the exam oversight team. General complaints about the exams (ie: technical issues, complaints about difficulty or cost) remain in scope for the Service Team Support members.

(d) External policy inquiries: Many clients will reach out about issues related to RPA that are not within TC's purview. These should not be addressed by the Service Team Support members, but staff can direct the client to the correct authority if the relevant information is on hand. Common subject areas include the nav drone app, the importing and exporting of RPA, the transportation of dangerous goods, or issues regarding the *Privacy Act* and/or *Criminal Code*.

(e) Flight school declarations and associations: Flight schools must declare themselves to TC to perform activities related to RPAS training for operations in Canadian airspace. Flight reviewers must be associated to a flight school with the appropriate declaration to perform reviews of that type. All inquiries related to these subjects should be passed on to the RPAS info inbox for review by the flight school oversight personnel.

(f) Incident reports: There is an incident reporting portal on the Drone Safety website. All incidents and accidents related to RPA must be reported by the client through this portal.

(g) Law enforcement agency delegations: Law enforcement agencies external to TC may request to become part of the delegated agency program to perform oversight on RPA under Part IX of the CARs. These inquiries should be directed to the law enforcement agency declaration inbox for processing.

(h) Police requests: Requests submitted by the police should go through an REU or the RCE and should be passed onto either of those groups.

(i) Policy issues: The FAQ and Drone Safety website are meant to be as comprehensive as possible in covering subjects pertaining to RPAS but are living documents and may have gaps. If an issue is brought to a Service Team Support member that is not covered by these documents, please send the inquiry onto the RPAS info inbox for review. These inquiries may result in one or both sources being updated to cover the subject in the future.

(j) RPAS and configurable element declarations: RPA and configurable elements must be declared to be used in certain operational conditions. Anything complex related to these declarations should be sent onto the declaration inbox. General inquiries (ie: what is a declaration, where to apply for a declaration) remain in scope for the Service Team Support members.

(k) SFOC inquiries: As in the rest of the TCCA, SFOCs are required to perform certain types of RPAS operations that require additional and nuanced review. Anything complex related to SFOCs should be sent to the SFOC inbox. General inquiries (ie: what is an SFOC, where to apply for an SFOC) remain in scope for the Service Team Support members.

9.0 Duplicate accounts

(1) Currently there is no way to merge or remove duplicate accounts within the DMP. If a client has created redundant accounts in the system:

(a) The client can ignore whichever account(s) is not necessary.

(b) The client can edit the information on the account to note that it should not be used. (IE: Change the name on the account to REDUNDANT ACCOUNT)

(2) If a client has multiple documents spread across different accounts and requests to have these documents deleted/merged under one account, the Service Team Support members will not be able to assist in resolving this issue. It is the client's responsibility to keep track of the information and services they obtain through the DMP. Any services completed under the incorrect account are non-refundable. While certificates of registration may be transferred between accounts in specific cases, no other documents can be moved once issued.

(a) Fake business accounts cannot be created to help a client move certificates of registration from one personal account to another.

10.0 Refusal of client inquiries related to the DMP

(1) Pursuant to section 6.71 of the *Aeronautics Act*, the Minister of Transport can decide to refuse to amend a Canadian aviation document such as the RPAS pilot's certificate, the RPAS certificate of registration, or the RPOC. Care must be taken to distinguish between a determination that a request is not yet complete from a decision to refuse to amend a document.

(2) If a client has not submitted all the required material, staff should advise the client that the request cannot be processed until specified additional documentation or information is provided.

(3) When available information demonstrates that the client is not qualified to amend or acquire the document noted in the request, staff must advise the applicant of the decision not to amend the document, using the "TC Notice of Refusal Form 26-0654".

11.0 Information management

11.1 Digital records

(1) The National Service Team determines the record keeping practices with regards to DMP interactions for all of TCCA. As RPAS inquiries are now integrated into the TCCA standards, all policies laid out by the National Service Team should be followed. Service Team Support members should contact their direct supervisor for clarification on any relevant record keeping procedures as needed.

11.2 Physical records

(1) No physical records are kept regarding RPAS inquiries of any kind at this time. If for some reason a Service Team Support member obtains physical records of anything pertaining to RPAS, the records should be disposed of in the appropriate way based on the privacy outlines defined in the TCCA information security protocols.

12.0 Document history

(1) Not applicable.

13.0 Contact us

For more information, please contact:

Law enforcement agency delegation related inquiries:
Email: RPASEnforcement-ApplicationdelaloiSATP@tc.gc.ca

RPAS & configurable element declarations related inquiries:
Email: TC.RPASDeclaration-DeclarationSATP.TC@tc.gc.ca

SFOC or RCE related inquiries:
Email: TC.RPASCentre-CentreSATP.TC@tc.gc.ca

All other inquiries unable to be answered by Service Team Support members using available resources, including access requests and SI update suggestions:
Email: TC.RPASInfo-InfoSATP.TC@tc.gc.ca

We invite suggestions for amendments to this document.

Document approved by

Ryan Coates
Director, Strategy and Emerging Technologies