POLICY SECTION I
MEMBERSHIP

Table of Contents

POLICY SECTION I
MEMBERSHIP

I. Purpose and Scope

This document outlines the eligibility, requirements, and benefits of membership in NASTF. The document also details the Code of Ethics and Conduct applicable to all members. Members must abide by the policies set forth in this document.

II. Eligibility

A. NASTF is a membership-based organization open to:

1. Individuals legally residing in, or authorized to be employed in, the United States of America or Canada, and
2. Involved professionally with the automotive industry, and
3. Provided they are properly licensed and registered as required in all municipalities, counties, states, or provinces in which they do business, and
4. Their business is registered as a sole proprietorship, partnership, limited liability corporation, corporation, or other recognized formal business structure, and
5. Their business is in good standing in the jurisdictions where they conduct business, and
6. They do not have any felony convictions relating to crimes involving theft, larceny, fraud, crimes of violence or crimes committed with deadly weapons if application is submitted within 5 years of release from confinement, parole, probation, and/or final court ordered restitution.
7. Individuals without a business affiliation are not eligible for membership.

III. Membership Categories

The corporation has three categories of membership:

A. Active Membership

1. Active members are individuals who have direct business affiliations with the automotive repair industry including, but not limited to:
    a. Individual automotive shop owners
    b. Automotive technicians including, but not limited to:
        i. Service
        ii. Security (includes automotive locksmiths)
        iii. Diagnostic
        iv. Collision
    c. Original Equipment Manufacturers (OEMs) also known as Vehicle Manufacturers

i. OEM technicians
ii. OEM Automotive Service Writers

d. Active Members have full voting privileges.
e. Active Members are qualified for all positions within the Board of Directors.

B. Associate Membership

1. Associate members are individuals who do not meet the requirements for Active Membership by their business, association, company, or entity ties to the automotive industry; however, they wish to participate and support the mission of NASTF. Examples of individuals who are eligible for Associate-level membership include, but are not limited to:
   a. Individuals from automotive service-related associations
   b. Automotive tool and equipment companies
   c. Automotive educators and trainers
   d. Other automotive professionals
2. Associate members have voting privileges; however, if there is more than one individual from the same business, association, company, or entity, the Associate Members are limited to one vote per business, association, company, or entity.
3. Associate Members are qualified for all Board of Director positions except Chair and Vice-Chair of the Board of Directors. The only exception to this rule is:
   a. If an automotive repair member or automaker board member cannot serve as Chair or Vice-Chair an exception may be made for an Associate to serve as either Chair or Vice-Chair to fill the vacancy.
   b. Only one of those positions may be filled by an Associate member at any given time.
   c. Such action requires a majority vote from the Board of Directors.

C. Affiliate Membership

1. Affiliate members are individuals who do not meet the requirements for Active or Associate Membership; however, they have expertise or vested interest in the actions of NASTF, and they support the mission of NASTF.
2. Affiliate members do not have any voting privileges.
3. Affiliate members do not qualify for any Board of Directors position, and their access to resources may be limited by NASTF policies.

IV. Application for Membership

A. All applications for membership shall be submitted to NASTF electronically through the NASTF website.

B. The submission of an application does not constitute any contractual obligation to accept an applicant as a member.
C. Submission of an application constitutes the applicant's agreement to abide by the bylaws, policies, and requirements set forth by NASTF.
D. NASTF reserves the right to conduct background checks on applicants.
E. The Executive Officer, or their appointee, will have the final authority to approve membership.

V. Denied Applicants

A. The submission of an application does not guarantee the issuance of, nor does it constitute any membership privileges.
B. NASTF reserves the right to deny membership applicants who do not meet the minimum eligibility requirements or who may not be aligned with NASTF's mission.
C. Notwithstanding the foregoing, any failure to disclose convictions on the application is cause for denial of membership privileges, and such denial is not appealable.
D. The Executive Officer, or their appointee, shall have the authority to deny an application for membership.
E. The Dispute Resolution and Appeals Process outlined in Policy Section II, titled Dispute Resolution and Appeal Process, does not apply to applicants.

VI. Applications:

A. If application remains uncompleted for more than sixty (60) days, without any attempt to finish the application or submit for review and approval, it becomes "dormant".
B. If the membership application becomes dormant, the application process will be placed in suspension.
C. To reactivate a dormant membership account, the applicant must send an email to NASTF Support at https://support.nastf.org/ and clearly state their intention to reactivate their dormant membership account.
D. The applicant should continue to use the original email address to complete the application.
E. Multiple attempts to gain membership from different email accounts will be blocked to mitigate any security risks.

VII. Membership Fees

A. Membership is currently free to everyone who meets the eligibility qualifications, completes an application, and agrees to abide by NASTF bylaws and policies.

VIII. Notification Requirements

A. Members are required to notify NASTF of any of the following changes:
   1. Change in employment (e.g. loss of employment, change of employer, etc.)
   2. Change in residency status (e.g. moving from one state to another)
   3. Arrests or convictions for either misdemeanor or felony crimes that are incurred after membership approval
B. Members shall notify NASTF support at https://support.nastf.org/ of any such changes.
C. Members are expected to maintain their member profile within NASTF's official web-based membership list.
D. Failure to comply with these requirements may result in suspension or revocation of membership.

IX. Benefits

A. The following list provides examples of resources available as part of NASTF membership:
   1. Automaker information and tool links
   2. NASTF's Knowledge Base of Module Reprogramming
   3. Meeting Calendars, minutes, and presentations from membership and team meetings
   4. NASTF Learning Center
   5. NASTF Brand Guidelines
   6. NASTF Diagnostic Network member portal
   7. NASTF Support documents and help desk
   8. NASTF Service Information Request (SIR) Assistance which is utilized to report and resolve problems with Original Equipment Manufacturer tools, training, or service information
   9. Options to choose the types of communications members wish to receive from NASTF
   10. Options to choose the Original Equipment Manufacturer brands members wish to follow
   11. Options to choose the NASTF Teams members wish to participate in.

B. Options to choose credential profiles designed to enhance profession.
   1. All credential profiles are voluntary and require members to "opt in."
   2. Detailed information about the eligibility requirements, benefits, costs, and policies of each credential profile can be found in the respective policy sections.

X. Membership Meetings

A. At least one member meeting will be held each calendar year.
B. The purpose of this meeting will be to report to the membership pertinent information regarding the activities, goals, and financial standing of the organization.

C. Members will be notified of the date, time, location, and overall agenda sixty (60) days prior to a member meeting taking place.
D. Notice will be given by posting the meeting details on the NASTF website, in the NASTF newsletter, by e-mail, or by other methods deemed suitable by the NASTF Executive Director.
E. Members are invited and encouraged to attend membership meetings; however, members are responsible for their own financial obligations and travel arrangements associated with such attendance.

XI. Code of Ethics and Conduct

A. Integrity

1. Accurately represents qualifications, training, and experience
2. Use knowledge and skills to enhance the industry and the member's specific profession
3. Avoid alliances with any practices that would be considered inconsistent with NASTF's purpose
4. Maintain the highest standards of integrity and conduct themselves in an honorable manner
5. Use only legal and ethical means to obtain service or repair information.
6. Not share NASTF user identification, password, or account
7. Be required to keep location services enabled on the devices used to access NASTF restricted/credentialed systems to ensure compliance with location-based security protocols.
    a. Use of Virtual Private Networks (VPNs) or any technology designed to mask or conceal true geographical location while accessing restricted/credentialed NASTF system is prohibited.
8. Comply with NASTF's Bylaws and Policies.

B. Professionalism and Courtesy

1. Perform work in accordance with all appropriate, local, state, and federal laws
2. Uphold NASTF's reputation and maintain a supportive public attitude towards NASTF.
3. Avoid any practice that is contrary to the law or would discredit the member or NASTF.
4. Refrain from making statements claiming to represent the views of NASTF without NASTF's consent.
5. Communicate respectfully with colleagues, employers, other NASTF members, and individuals in their professional interactions.
6. Refrain from negligently, maliciously, or intentionally harming the reputation, prospects, or business of another member of NASTF.

C. Confidentiality

1. Maintain confidentiality for customers, clients, and other members
2. Comply with all applicable local, state, and federal privacy requirements
3. Respect the sensitive nature of all confidential or proprietary information and exercise due care to prevent its unlawful or improper disclosure
4. Use official or sensitive information in accordance with legislative and regulatory standards, their employer instructions, and the source's specific instructions

D. Harassment

1. Refrain from verbal, written, or image-based slander, defamation, impersonation, or other derogatory statements about:
    a. Fellow members of NASTF,
    b. The NASTF Board of Directors,
    c. The NASTF staff or,
    d. The NASTF organization,
    e. OEM employees,
    f. OEM organizations.

1. Treat others with courtesy, respect, and dignity, and refrain from discriminating directly or indirectly based on:
    a. Gender
    b. Race
    c. Culture
    d. Age
    e. Marital status
    f. Ethnic or national origin
    g. Sexual orientation
    h. Religious beliefs
    i. Cultural or philosophical beliefs
    j. Language
    k. Disability

E. Sexual Harassment

1. NASTF has zero tolerance for all forms of harassment, especially sexual harassment, expressly prohibited by the law. It considers such behavior in all its forms to be a serious offense that will bring serious consequences to the offending individual(s) because such behavior violates individuals' fundamental human rights and dignity.
2. NASTF's commitment to zero tolerance of such behavior applies to every incident whether occurring at a NASTF sponsored event or elsewhere whenever involving NASTF.
3. Whenever NASTF becomes aware of such behavior it will investigate promptly, impartially, and thoroughly.

4. If NASTF finds that such behavior is occurring or has occurred, it will take such steps as are necessary to permanently stop the offensive behavior and to protect the victim.
5. Sexual harassment may include:
    a. Any offensive and/or unwelcome sexual invitations
    b. Offensive and/or unwelcome conduct of a sexual nature, including sexually graphic spoken or written comments—or the possession of, display, or use of sexually suggestive objects, images, or graphics
    c. Offensive and/or unwelcome intentional physical contact of a sexual nature, including the intentional and unwelcome or offensive touching of another's body, psychological harassment, or a course of conduct or series of incidents that can constitute sexual harassment even if one of the incidents considered on its own may not be harassing.
    d. Persisting in making sexual or romantic advances despite the indication that such advances are unwelcome, or despite rejection of such advances
    e. Deliberately creating an offensive environment, including the use of vulgar language of a sexual nature; gestures; indecent exposure; telling sexually explicit jokes; displaying, storing, or transmitting sexually explicit photographs or other materials.

F. Duty to Report and Cooperate

1. Other than the victim, all NASTF members, staff, managers, Board of Directors, appointed or elected leadership, consultants, and contractors have a duty to report and cooperate with inquiries of sexual or other forms of harassment, especially those expressly prohibited by the law.
2. Once a NASTF member, staff, manager, Board of Directors member, appointed or elected leadership, consultant, or contractor becomes aware of an allegation of sexual harassment they shall immediately report such by contacting NASTF at: https://support.nastf.org or nastf-rm@nastf.org.
3. Excluding the victim, failing to report, or failing to cooperate with an inquiry, is grounds for suspension or termination of membership and all privileges associated with such membership.
4. All reports, complaints, or allegations of sexual harassment are treated confidentially, to the greatest extent legally possible, except as necessary to conduct an appropriate inquiry or investigation, or as otherwise required by law.
5. Disclosure of the inquiry or investigative findings are also considered confidential, to the greatest extent legally possible, and limited in scope to the Executive Committee.

G. Bribery and Kickbacks

1. Members may not engage in bribery or offer "kickbacks" to any governmental or non-governmental organization (NGO) entity, officer, appointee, or elected official.
2. Bribery and kickback complaints are taken with the utmost seriousness by NASTF.

H. Trade Secrets/Corporate Espionage

1. Members may not engage in any "trade secret" violations affecting other members, OEMs, or other automotive industry entities.
2. Similarly, members may not engage in any "corporate espionage" affecting another member, OEMs, or other auto industry entity.

I. Authority to Conduct Inquiry

1. Upon receipt of complaint of violation of any NASTF policy, including but not limited to the foregoing, the Executive Director shall have the authority to appoint an individual(s) to complete an objective fact-finding inquiry into the allegation.
2. The member who is the focus of the inquiry will be notified in writing and provided with an opportunity to respond to the allegation.
3. The target completion time will be thirty (30) days; however, depending on circumstances some inquiries may take longer.
4. All complaints, allegations, and inquiries, are treated confidentially, to the greatest extent legally possible, except as necessary to conduct an appropriate inquiry or as otherwise required by law.
5. The Executive Director may temporarily suspend, or remove a member, including their credentials, during the inquiry into the allegations.
6. Upon completion of the inquiry, the Executive Director will report the findings to the NASTF's Chair of the Board of Directors for handling of the matter and rendering final judgement.
7. The member who was the focus of the inquiry will be notified of these findings and the decision of the Board of Directors.
8. The decision of the Board of Directors on such matters is final and there is no dispute resolution or appeal process available.

XII. Suspension or Termination

A. Membership may be suspended or revoke by the Board of Directors, Executive Officer, Registry Manager, or NASTF designee for:
   1. Conduct deemed detrimental to the corporation or,
   2. Conviction of any crime involving vehicle theft, fraud, embezzlement, dishonesty, breach of trust or,
   3. For administrative or non-governmental organization finding of action involving vehicle theft, fraud, dishonesty or breach of trust or,

4. When it has been determined by the Board of Directors the member is or has been a member of any subversive organization or,
5. For violation of these Bylaws, Policies, or any rule of the corporation or,
6. For any action inconsistent with the corporation's Code of Ethics and Conduct.

B. Revocation of membership does not relieve a member of any outstanding obligation to NASTF
C. Members (not applicants) are entitled to appeal suspension or revocation of membership through the Dispute Resolution and Appeal Process.
    1. Detailed information can be found within Policies, Section II, titled Dispute Resolution and Appeals Process.
D. NASTF reserves the right, in its sole discretion, to determine a breach of any policies set forth herein, and all determinations upheld by the NASTF Appeals Review Process are final.

XIII. Voluntary Withdrawal

A. Nothing prohibits a member from voluntarily resigning their membership at any time.
B. Members who wish to resign from NASTF must create a Support Ticket at https://support.nastf.org and request to be unsubscribed from NASTF membership.
C. Resignation does not prohibit NASTF from sanctioning a member for violations of NASTF Bylaws, Policies, or rules of an Original Equipment Manufacturer.

XIV. Reservation of Rights

A. NASTF reserves the right to monitor user activity and employ technology to detect and prevent the use of VPNs or any other location-masking software.
B. NASTF reserves the right, in its sole discretion, to change these policies at any time as needed to respond to security threats.
C. Policy updates and/or changes will be posted to the NASTF website.
D. A member's continued use of NASTF resources after notification of policy updates constitutes acceptance of the new terms.

POLICY SECTION II
DISPUTE RESOLUTION AND APPEALS PROCESS

Table of Contents

POLICY SECTION II
DISPUTE RESOLUTION AND APPEALS PROCESS

I. Purpose and Scope

This document outlines the procedures of the Dispute Resolution and Appeals Process and details the structure of the Appeals Review Committee. Members, including credential applicants and existing credential holders. Members must abide by the policies set forth in this policy.

II. Appeals Review Committee Structure

A. The NASTF Appeals Review Committee consists of seven (7) members who are appointed by the NASTF Chairman of the Board of Directors. The Appeals Committee members:
   1. Serve a two-year term
   2. May be reappointed after their first term
   3. May be reappointed to serve in this capacity with no term limits

B. The Appeals Review Committee is comprised of seven members from NASTF's membership (or member principals, as the case may be) and are structured as follows:
   1. One (1) Director from the NASTF Board of Directors
      a. This member serves as the Chairman of the Appeals Review Committee
   2. Six (6) members from across all stakeholders in SDRM (Security Data Release Model), including:
      a.Service Repair
      b. OEM (Original Equipment Manufacturers)
      c. Locksmiths
      d. Tool companies
   3. Committee members' identities shall remain confidential and will not be shared with the appellant or membership
   4. The committee balloting process is secret and voting results will not be shared with the appellant or membership.

III. Eligibility for Appeal

A. The Appeals Process provides an opportunity for individuals to have their voice heard by a committee of their peers and applies to:
   1. General members whose membership privileges have been suspended or revoked.
   2. Members whose applications for credentials have been denied.
   3. Credential holders whose credential privileges have been suspended.
   4. Credential holders whose Registry privileges have been denied.
   5. Applicants for general membership do not qualify for appeal under this policy.

B. The credentials included in the Appeals Process are:
    1. Diagnostic Professional
    2. Assisted Immobilizer Reprogramming (AIR) Field Technician
    3. Assisted Immobilizer Reprogramming (AIR) Service Provider
    4. Primary-Vehicle Security Professional
    5. Subordinate-Vehicle Security Professional
    6. Company Administrator

IV. Appeals Process

A. Notifications of general membership suspension or revocation will be sent from NASTF to the email address listed in the member's profile.
    1. Upon notification that a member has been suspended, or their membership revoked, the member has ten (10) business days (defined as Monday through Friday, not including Federal Holidays recognized in the United States) to provide a written notice of appeal with NASTF.

B. Notifications of credential application denials, suspensions, or Registry access denials will be sent from NASTF to the email address listed in the member's profile.
    1. Upon notification that a member's application for credentials has been denied, their credentials have been suspended, or their Registry access has been denied, the member has ten (10) business days (defined as Monday through Friday, not including Federal Holidays recognized in the United States) to provide a written notice of appeal with NASTF.

A. In order to fill a written appeal, members (including credential applicants and credential holders) shall reply to the notification received from NASTF Registry Manager (NASTF-RM@nastf.org).
    1. Appeals should contain all supporting documents or other information that refutes the decision to:
        a. Suspend general membership
        b. Revoke general membership
        c. Suspend member's Registry credentials
        d. Deny members Registry access
    2. Submission of supporting documents and information constitutes consent to share all documents received with the NASTF Executive Officer, the NASTF Appeals Review Committee, and any other NASTF staff deemed necessary to process the appeal.
    3. Submission of supporting documentation and information constitutes consent for NASTF to retain all documents received regardless of the outcome of the appeal.
    4. NASTF reserves the right to request additional information prior to appeal submission to the Appeals Review Committee.

B. Correspondence from NASTF sent to the email address listed in the member's profile constitutes NASTF's good faith attempt to notify the member of action against them.
   2. NASTF fulfills its obligation to notify the members by sending such email.
C. The responsibility to ensure the member's profile always contains the most current email address rests solely on the member. Similarly, the member's responsibility to regularly check said email rests solely on the member.
D. Failure to file a notice of appeal within ten (10) day timeframe will be considered a forfeiture of the member's right to an appeal.

V. Executive Officer Review

A. The Executive Officer serves as the intermediary responsible for review of disciplinary action taken by the Registry Manager, or NASTF staff, against a member.
B. All appeals supporting documentation supplied by the appellant, along with NASTF's internal documentation used to invoke disciplinary action against the member will be provided to the Executive Officer for review.
C. NASTF's internal documentation may contain sensitive or confidential information therefore it is not available to the appellant for review or dispute.
D. The Executive Officer may request:
   1. Additional information and/or documentation from NASTF staff.
   2. Additional information and/or documentation from the member filing the appeal.
E. Once the Executive Officer has sufficient information necessary to complete a review they will either:
   1. **Reverse** the disciplinary action against the appellant and rescind the:
      a. Suspension of membership
      b. Revocation of membership
      c. Suspension of credentials
      d. Denial of Registry access; or
   2. **Affirm** the disciplinary action against the appellant
      a. If the Executive Officer affirms the disciplinary action, they will call the Appeal Review Committee to order and begin the Appeals Process.
F. The Executive Officer has the right to recommend a different form of disciplinary action than the action initiated by the Registry Manager, or NASTF staff.

VI. Appeals Review Committee Process

A. The NASTF Appeals Review Committee will convene a meeting within ten (10) business days of receiving supporting documentation from the NASTF Executive Officer or staff.
B. The NASTF Appeals Review Committee will review the documentation and:
   1. Request additional information from NASTF staff,
   2. Direct NASTF staff to obtain further information from the appellant,

3. Call for a vote on the Appeal, and
    a. **Reverse** the disciplinary action against the appellant and rescind the:
        i. Suspension of membership
        ii. Revocation of membership
        iii. Suspension of credentials
        iv. Denial of Registry access; or
    b. **Affirm** the disciplinary action against the appellant.

C. The Appeals Review Committee has the authority to revise initial disciplinary actions.
D. The Appeals Review Committee will submit its findings to the NASTF Board of Directors and staff for notification of final judgement to the appellant.
E. NASTF will notify the Appellant within ten (10) business days of the Appeals Review Committee's final decision by sending correspondence to the email address listed in the Appellant's member profile.
    1. The responsibility to ensure the member's profile always contains the most current email address rests solely on the member. Similarly, the member's responsibility to regularly check said email rests solely on the member.
F. Members whose applications for credentials are denied may not reapply for credentials for at least one year from the date they receive the Appeal Review Committee's final decision unless otherwise noted in the final disposition.
G. The Appeals Process is the final arbitration process. Members have no right to appeal against the decisions of the Appeal Review Committee and there is no legal recourse available as NASTF membership and credentials are a privilege.

VII. Resignations

A. Nothing herein prohibits a member from voluntarily relinquishing credentials and/or membership.
B. Members who wish to relinquish their credentials and/or membership must unsubscribe by creating a support ticket at https://support.nastf.org/, and requesting to be unsubscribed from their credentials or membership.
C. Resignation of VSP credentials does not relieve the member from financial obligations to NASTF.
D. There will be no refunds if VSP credentials have been utilized to access vehicle security information.
E. Relinquishment of either membership or VSP credentials does not prohibit NASTF from sanctioning a member for violations of NASTF Bylaws, Policies, or OEM terms and conditions.

POLICY SECTION III
DIAGNOSTIC PROFESSIONAL

Table of Contents

POLICY SECTION III
DIAGNOSTIC PROFESSIONAL

I. Purpose and Scope

This document outlines the eligibility, requirements, and benefits for the Diagnostic Professional credential. The Diagnostic Professional credential is a benefit available to NASTF general members. Members must abide by the Policies set forth in this document.

II. Benefits

A. The DP credential allows access 2018MY and newer Hyundai, Genesis, and KIA brands Secure Vehicle Gateways (SVG) utilizing a J2534 subscription with the DP's diagnostic software suite.
B. DP credentials do not allow any access to security-related information as only Vehicle Security Professionals ("VSPs") can perform vehicle security-related functions.

III. Eligibility

A. Requirements for Diagnostic Professional ("DP") credentials are as follows:
    1. DP credentials are issued to an individual natural person, and not a business
    2. Individuals must already be, or become, NASTF Members in good standing
    3. Individuals must maintain their Membership in good standing
    4. Individuals must have a business affiliation with the automotive repair industry, including, but not limited to:
        a. Professional Automotive Service Technicians
        b. Individual shop owners
        c. Original Equipment Service Employees
        d. Other automotive industry professionals not listed herein
    5. The individual's affiliated business must be registered as one of the following:
        a. Sole Proprietorship
        b. Partnership
        c. Limited Liability Company
        d. Corporation

IV. Fees

A. The DP credential is available for <u>free</u> to all NASTF General Members but requires members to voluntarily "opt in" by selecting the DP credential within their member profile.
B. Once selected, and approved, they will be issued a DP Identification ("DPID") number.

V. Requirements for DP credentials:

A. Must provide full business name and business address.
B. Must provide Federal Employer Identification Number ("FEIN").
C. Must provide mobile telephone number of a "smartphone" capable of downloading an application from either the App Store or Google Play.
    1. A mobile telephone number will be used for NASTF's multi-factor authentication app.
    2. DP's responsibility to ensure the mobile telephone number used for registering the NASTF multi-factor authentication app is the same number listed in its NASTF member profile.
D. Must agree to install NASTF's multi-factor authentication app on their mobile phone, linking their DPID to the NASTF.org website.
    1. NASTF provides the multi-factor authentication app free of charge; however, the DP is responsible for mobile phone subscription fees, data, and usage charges.
E. Must abide by all policies, rules, and requirements set forth by the applicable Original Equipment Manufacturer ("OEM") for use of its system and services.
F. DPs are prohibited from sharing DPID and/or multi-factor authentication code with others.
    1. Exception: When requesting support from NASTF, or upon receipt of a valid inquiry from NASTF.

VI. Misuse of Credentials

A. Sharing user logins and passwords between individuals is expressly prohibited.
B. Any Diagnostic Professional who is aware of any misuse of the NASTF's Diagnostic Professional Program shall immediately report said misuse directly to NASTF Support at https://support.nastf.org/.
C. Violations of these Policies are grounds for the Diagnostic Professional accounts to be suspended and/or removed from the Diagnostic Professional Program or have the Diagnostic Professional's general NASTF membership (and related benefits) terminated.
D. Credentials, and membership, may be suspended by the Registry Manager, or NASTF designee, for:
    1. Conduct detrimental to NASTF, conviction of any crime involving moral turpitude (e.g., theft, fraud, embezzlement, dishonesty, breach of trust, etc.), or violation of these policies, bylaws, or any rule of the corporation.
E. The Member involved shall be given due notice and shall be entitled to a hearing before the Appeals Review Committee.
F. Suspension or denial of Registry access credentials does not relieve a member of any outstanding obligation to NASTF
G. NASTF reserves the right, in its sole discretion, to change these policies at any time as needed to respond to security threats.
H. For more information, see Policies, Section II, titled Dispute Resolution and Appeals Process.

VII. Dispute Resolution and Appeals Process

A. NASTF reserves the right, in its sole discretion, to determine a breach of any policies set forth herein, and all determinations upheld by the NASTF Appeals Review Committee are final.
B. Detailed information about the Appeals Process can be found in Policies, Section II titled Dispute Resolution and Appeal Process.

VIII. Voluntary Withdrawal of Membership

A. Nothing prohibits a member from voluntarily relinquishing their credentials or voluntarily resigning from membership.
B. Members who wish to resign from NASTF must unsubscribe from by creating a Support Ticket at https://support.nastf.org and request to be unsubscribed from NASTF membership.
C. Resignation does not prohibit NASTF from sanctioning a member for violations of NASTF's rules, policies, policies of an OEM, or engaging in illegal or criminal activity.

POLICY SECTION IV
ASSISTED IMMOBILIZER REPROGRAMMING PROGRAM

Table of Contents

I. Purpose and Scope

This document outlines the benefits, fees, eligibility, and requirements of the Assisted Immobilizer Reprogramming ("AIR") Program. AIR credentials are a benefit available to NASTF general members. Members must abide by the Policies set forth in this document.

II. Benefits

A. Modern vehicles often require module reprogramming, which includes access to vehicle security information, after certain repairs or component replacements. The investment in specialized tools and training for these infrequent procedures can be prohibitive for many repair and collision shops. To address this, NASTF, in concert with Original Equipment Manufacturers ("OEMs"), developed the AIR Program.

B. The AIR Program enhances general membership benefits by offering additional credential profiles:
   1. Assisted Immobilizer Reprogramming Field Technician ("AIR Field Tech")
   2. Assisted Immobilizer Reprogramming Service Provider ("AIR Service Provider")

C. AIR credentials facilitate secure connections between an AIR Field Tech and an AIR Service Provider. This enables AIR Field Tech (e.g., repair and collision shop employees) to connect with an approved AIR Service Provider, who has the necessary expertise and equipment, to remotely perform critical vehicle security reprogramming sessions.

D. All NASTF support and technical assistance requests must originate from the registered AIR Field Tech or AIR Service Provider.

III. Fees

A. The AIR Field Tech credential itself is free; however:
   1. There is a $45 transaction fee for each of the first five transactions within a 12-month period.
   2. After the first five transactions ($225), all subsequent transactions are free for the remainder of the consecutive 12-month period.
   3. The $45 fee is reset annually on the anniversary of the first transaction.
   4. The $45 fee does not include any fees charged by the AIR Service Provider.

B. The AIR Service Provider credential itself is free; however:
   1. The AIR Service Provider must maintain their VSP-Primary credentials in good standing.
   2. The AIR Service Provider may set their own fee schedule independent of the NASTF transaction fees.

IV. AIR Field Technicians – Eligibility Requirements

A. AIR Field Techs must:
   1. Maintain general membership in good standing with NASTF.
   2. Abide by policies for both AIR Program and general members.
   3. Complete an AIR Field Tech credential application by selecting "Assisted Immobilizer Reprogramming" from the profile menu.

B. If the AIR Field Tech applicant is an individual employee, they must:
   1. Provide proof of employment in the form of a Wage (pay stub) and Tax Statement (W-2 or T4 for Canadians).
   2. Provide a color copy of the applicant's government-issued identification.
   3. Maintain credentials by updating information annually or whenever a change in employment occurs.

C. If the AIR Field Tech applicant is also the business owner, they must:
   1. Provide proof of business ownership or Wage (pay stub) and Tax Statement (W-2 or T4 for Canadians)
   2. Provide Federal Employer Identification Number (EIN) or Canadian Business Number (T1).
   3. Provide payment method information.

D. Successfully pass a criminal background check by NASTF.

V. AIR Field Tech – Responsibilities

A. In order to utilize the AIR system, the AIR Field Tech must log into NASTF.org website and navigate to the Assisted Immobilizer Reprogramming tab on the left navigation pane and provide the following vehicle information:
   1. Vehicle Identification Number
   2. Make
   3. Model
   4. Color
   5. License plate number and State of Issuance
   6. Mileage, if available
   7. Provide ownership documents required for the transaction and upload legible color copies.

B. For privately owned vehicles, the following must be provided:
   1. Driver's license for the vehicle owner
   2. Ownership documentation such as the title or registration that matches the driver's license information

C. For fleet-owned vehicles, the following must be provided:
    1. Ownership documentation such as the title or registration that matches the company ownership information
    2. Collision repairers who have Power of Attorney for repair may use that in place of the driver's license but still must provide an ownership document such as insurance card or registration.
    3. A Power of Attorney may not be used with a bill of sale or vehicle title that does not have the customer's name and information imprinted by the issuing state or province.

D. No Personally Identifiable Information ("PII") gathered during the repair process may be stored or shared except as required to satisfy the ownership documentation requirements.

E. AIR Field Techs may not share, retain, database, or electronically transfer any security-related service

F. AIR Field Techs are required to either perform the work on the vehicle or directly supervise the work of an employee or contract technician who is performing the work.
    1. Providing credentials to an employee or contract technician does not constitute "supervision" and is strictly prohibited.

G. AIR Field Tech must confirm they are not attempting to originate or program keys/fobs.
    1. AIR Service Providers will not perform these functions except in the following circumstances:
        a. If keys need to be programmed back into a vehicle as part of immobilizer reprogramming the AIR Service Provider will be responsible for determining the proper course of action that aligns with NASTF policies and Vehicle Security Professionals (VSP) Program.
        b. Only NASTF SDRM Registered VSPs who are on-site, present with the vehicle, are allowed to access and utilize key codes, originate keys, or program transponders.

H. Under no circumstances may data obtained be used to create, mail, ship, or otherwise transmit keys, fobs, control modules, or other security-related devices.

I. AIR Field Techs may not share usernames, assigned security credentials, passwords, or multi-factor authentication codes.

J. AIR Field Techs must ensure that no connection to vehicles or transfer of any information outside of the United States and Canada is performed.

K. It is the responsibility of the AIR Field Tech/AIR Service Provider to ensure that tools with End-User License Agreements (hereafter referred to as "EULA") stating that customer information is gathered and shared with other countries or governments are NOT used in the AIR process.

L. AIR Field Techs must comply with all applicable federal, state, and local regulations and statutes.

VI. AIR Service Providers – Eligibility Requirements

A. AIR Service Providers must:
   1. Maintain general membership in good standing with NASTF
   2. Be credentialed as a Vehicle Security Professional-Primary ("VSP-P").

B. The AIR Service Provider must be in good standing with both NASTF and OEMs and cannot have any disciplinary actions taken against them within the past twenty-four months.

C. AIR Service Providers must apply for AIR Service Provider credential enhancement to their existing VSP-Primary credential.

D. AIR Service Providers must sign and agree to the AIR Program terms and conditions and sign a non-disclosure agreement ("NDA") with NASTF. This NDA contains additional policies beyond the standard VSP policies.

E. AIR Service Providers must complete a telephone interview and program introduction training conducted by the NASTF Registry Manager or the Registry Manager's designee.

VII. AIR Service Providers – Responsibilities

A. AIR Service Providers must:
   1. Demonstrate that their remote programming technique is secure and compliant with OEM End-User License Agreements (EULA) through the NASTF website.
   2. Confirm compliance with customer ownership/authorization documents as outlined in the Customer Authorization Documentation/D1 Policies.
   3. Maintain the security of vehicle security-related information by adhering to all measures required by OEMs and NASTF.
   4. Use security-related information only once per vehicle service. In the event a vehicle is to be serviced again by the same AIR Service Provider, the complete access protocol must be repeated.
   5. Be granted advanced administrative access to SDRM. AIR Service Providers will essentially review and approve security-related repairs before performing them either remotely or in person.
   6. Not remotely originate keys/fobs or reprogram keys/fobs back to a vehicle.
   7. Agree to assist clients with registering to become NASTF AIR Field Techs by reviewing and understanding application requirements for AIR Field Techs and referring to the NASTF Support Team when questions arise.
   8. Review pending AIR service requests within five (5) days of the request being submitted and either:
      a. Accept the request
      b. Deny the request

B. Any use of data that was not acquired through the NASTF-approved OEM process is a violation, and:
    1. The AIR Service Provider must deny the transaction and immediately notify NASTF of any such incident or security concerns via https://support.nastf.org/ or nastf-rm@nastf.org.

VIII. AIR Service Providers – Multiple Techs

A. If there are multiple AIR Service Providers registered within one business, the business may:
    1. Have all AIR service requests sent to every Air Service Provider or;
    2. Designate which AIR Service Provider will receive service requests and act as lead
B. The lead AIR Service Provider can:
    1. Review incoming AIR service requests
    2. Confirm customer documentation (D1s)
    3. Assign AIR service requests to another registered AIR Service Provider
    4. Approve or deny AIR requests
    5. Edit rejection notification templates for AIR requests to match their company business model and adjust templates to fit the specific rejection reasons

IX. Compliance

A. The AIR Program shall not be used to originate or program keys/fobs.
    1. If reprogramming requires keys/fobs to be programmed back to the vehicle to complete component repair or replacement, such action must be documented within the OEMs procedures.
B. Sharing user logins and passwords between individuals is expressly prohibited.
C. Any AIR Field Tech or AIR Service Provider who is aware of any misuse of the NASTF's AIR Program shall immediately report said misuse directly to NASTF Support at https://support.nastf.org/.
D. Violations of these policies are grounds for the AIR Field Tech and/or AIR Service Provider accounts to be suspended or removed from the AIR Program, or have their general membership suspended or terminated.

X. Dispute Resolution and Appeals Process

A. NASTF reserves the right, in its sole discretion, to determine a breach of any policies set forth herein, and all determinations upheld by the NASTF Appeals Review Process are final.
B. Detailed information about the Dispute Resolution and Appeals Process (Appeals Process) can be found in Policies, Section II titled Dispute Resolution and Appeal Process.

XI. Voluntary Withdrawal of Membership

A. Nothing prohibits a member from voluntarily relinquishing its credentials or resigning its membership
B. Members who wish to resign from NASTF must unsubscribe by creating a Support Ticket at https://support.nastf.org and requesting to be unsubscribed from NASTF membership.
C. Resignation does not prohibit NASTF from sanctioning a member for violations of NASTF rules or policies, policies of an OEM, violation of law, or criminal activity.

POLICY SECTION V
VEHICLE SECURITY PROFESSIONAL REGISTRY & SECURE DATA RELEASE MODEL

Table of Contents

POLICY SECTION V
VEHICLE SECURITY PROFESSIONAL REGISTRY & SECURE DATA RELEASE MODEL

I. Purpose and Scope

This document outlines the Vehicle Security Professional Registry ("Registry") and the Secure Data Release Model ("SDRM") used for access to the Registry. Members who hold credentials authorizing access to the Registry must abide by the Policies set forth in this document.

II. Benefits

A. The Registry and SDRM provide Original Equipment Manufacturers ("OEMs") with a flexible system for continuous access to vehicle security information.
   1. The Registry enables access for automotive professionals

B. NASTF provides credentials to access the Registry for:
   1. Automotive Professionals
   2. Commercial entities

C. With demonstrated vehicle ownership, the SDRM provides the ability for VSPs to:
   1. Add a security device (e.g. key, fob, or immobilizer)
   2. Originate All Keys Lost (AKL)
   3. Reset immobilizers
   4. Access/perform OEM designated security functions

D. Registry access includes:
   1. Mechanical key codes
   2. Electronic key codes
   3. Immobilizer reset codes
   4. PIN codes
   5. Radio lockout codes
   6. Remote codes
   7. Access to vehicle security networks
   8. Confirmation of credentials for:
      a. Theft-relevant parts purchases
      b. Tool access authorization
      c. Successor technologies
   9. Upon acceptance into the Registry, each Vehicle Security Professional (VSP) is assigned a unique Vehicle Security Professional Identification number (VSPID).

III. Vehicle Security Professional (VSP) Credential Requirements for Registry Access

A. Access to the Registry is through the SDRM portal and requires NASTF VSP credentials.
B. Credential holders are required to:

1. Maintain general membership in NASTF
2. Have a business affiliation with the automotive repair industry, including:
    a. Automotive Technicians
    b. Locksmiths
    c. Vehicle Manufacturers
    d. Individual shop owners
    e. Automotive Service-Related Associations
    f. Service Writers
    g. Tool and Equipment Companies
    h. Educators and Trainers
    i. Original Equipment Service Employees
    j. Other automotive industry professionals.
3. Have a business registered as:
    a. Sole Proprietorship
    b. Partnership
    c. Limited Liability Company
    d. Corporation
4. Successfully pass a background screening
5. Complete all application requirements

C. VSP Credentials:
    1. Are assigned to owners or W2 employees of the business, not the business itself.
    2. Do not extend to other employees within the business.
    3. Require each employee utilizing the Registry have their own VSP credentials.
        a. Business owners should review the various VSP credential types, and may consult with NASTF staff, before adding additional VSP accounts to ensure alignment with business operations.
D. VSP Credential Profiles:
    1. Primary-Vehicle Security Professional (VSP)
    2. Subordinate-Vehicle Security Professional (VSP)
    3. Company Administrator
E. The Registry policies are developed by the NASTF Vehicle Security Team, which includes OEMs, locksmiths, service technicians, and law enforcement.

IV. VSP Credential Dues and Fees

A. All applicants must pay the required Credential Dues and Background Screening Fees (biennial) in full at the time of application.
   1. Primary-Vehicle Security Professional (VSP) credential dues: $335.00.
      a. Requires Background Screening: $100.00.
   2. Subordinate-Vehicle Security Professional (VSP) credential dues: $150.00.
      a. Requires Background Screening: $100.00.
   3. Company Administrator: No-Cost.
      a. No Background Screening required.

B. All dues and fees are established by the NASTF Board of Directors and subject to change.

V. VSP Credential Application Rejections and Denials

A. Due to the stringent application process, approval of VSP credentials is not guaranteed. Applicants notified of a rejected application or missing documentation will be provided with an opportunity to:
   1. Complete their application
   2. Correct their profile information
   3. Submit or resubmit necessary documentation
   4. Provide explanations, if requested by NASTF.

B. Misrepresentation: Submission of any false, fraudulent, or misleading information is grounds for immediate denial.
   1. In cases of misrepresentation, all dues and fees are strictly non-refundable.

C. This policy applies to both new and renewing VSP applicants, regardless of expiration date, renewal status, or renewal approval date.

D. Applicants rejected or denied for reasons other than misrepresentation may appeal the decision by following the procedures in Policies, Section II, titled Dispute Resolution and Appeals Process.

VI. Dormant VSP Applications

A. A VSP application becomes “dormant” if it remains incomplete for more than sixty (60) days from the origination of application without an attempt to finish or submit for review.

B. Dormant applications will be nullified.
   1. Refund requests for Credential Dues of dormant (nullified) applications must be made within ninety (90) days of the origination of the application.
   2. Background screening fees are non-refundable if the screening process has started.

VII. VSP Credential Application Withdrawals

A. Applicants may voluntarily withdraw their VSP application by submitting a support ticket at https://support.nastf.org/.
B. Requirements:
    1. Withdrawal requests must be received within twenty-four (24) hours of the initial application submission to ensure eligibility for a full refund.
    2. The applicant must provide a specific reason for the withdrawal at the time of their request.
C. Members who voluntarily withdraw their VSP applications will not be granted access to the Registry and are not eligible to appeal.
D. Voluntary withdrawal of VSP applications does not change general membership status.

VIII. Refunds of VSP Credentials

A. VSP Credential Dues:
    1. Applicants who do not meet VSP requirements, or whose application becomes dormant, may request a refund of their Credential Dues within ninety (90) days of originating their application.
    2. Applicants who voluntarily withdraw their VSP application within twenty-four (24) hours of originating their application may request a refund of their Credential Dues.
    3. Credential Dues are non-refundable if the VSP credentials have been utilized to access vehicle security information.
B. Background Screening Fees:
    1. Background screening fees will only be refunded if the VSP application is voluntarily withdrawn within twenty-four (24) hours of originating the application, and
    2. The background screening process has not yet been initiated.
    3. Otherwise, background screening fees are non-refundable as they are paid to third-party providers.
        a. This includes applicants who fail the background screening.
C. Approved refunds will be issued to the original payment method used during the application process.

IX. Access to Registry and Use of SDRM

A. Access to the Registry and use of the SDRM portal:
    1. Vehicle security information obtained from the Registry through SDRM is for single use only.
    2. Collection and recording of Personally Identifiable Information (PII) from customers, as detailed in Policies, Section VII, titled Customer Authorization Documents.
    3. Proper disposal of PII.

4. Strictly prohibits the use of Virtual Private Networks (VPNs) or any technology designed to mask or conceal the true geographical location while accessing the Registry and SDRM.
5. Require users to keep location services enabled on the devices used to access the Registry and SDRM to ensure compliance with location-based security protocols.
6. No unauthorized access or mishandling of data from the Registry, SDRM, or OEM websites.
    a. Such infractions result in immediate suspension of VSP credentials, and possible denial of Registry access without the right to appeal.
    b. Any such infractions may result in referral to appropriate authorities.

B. VSP holders shall:
1. Not share usernames, security credentials, passwords, or multi-factor authentication codes.
2. Treat vehicle security information as confidential.
3. Secure vehicle security information as required by OEMs and NASTF.
4. Not sell, buy, trade, barter, or share security-related information or devices.
5. Not retain, database, transfer, or transmit vehicle security-related information.
6. Upon “request” the registered owner may be provided with the key code (code only); however:
    a. The registered owner must be physically present with the vehicle and VSP
    b. Under no circumstances shall any code be transmitted electronically
    c. Under no circumstances shall any code be stored either physically or electronically
7. Not provide vehicle security devices such as keys, fobs, control modules, or other devices to others outside of the authorized NASTF D1plus1 process.
8. Not mail or ship vehicle security devices such as keys, fobs, control modules, or other devices created with vehicle security information obtained with VSP credentials.
9. Be present with and verify customer’s legal ownership/possession and perform services on the vehicle or directly supervise the work, except as outlined under the D1plus1 process.

C. Vehicle security information shall not be used for unauthorized purposes.

X. Vehicle Security Information Audits

A. NASTF reserves the right to conduct security audits to ensure compliance at any time with any user, and without any required justification.
B. Anyone who accesses the Registry or uses SDRM, including but not limited to VSPs, is subject to audits.
C. Cooperation with audit requests is mandatory, and refusal to cooperate is grounds for immediate suspension, and possible denial of Registry access and SDRM.

D. Audit notifications will be sent to the email address listed within the member profile.
E. Members have five (5) business days to respond to an audit inquiry.
F. Failure to respond, provide requested information, or cooperate within the allotted five (5) days may result in suspension and possible denial of Registry access and SDRM.

XI. NASTF Duty to Cooperate

A. NASTF has a duty to cooperate with law enforcement and other organizations regarding possible criminal activity.
    1. If the inquiry involves use of the Registry and/or involvement of a VSP(s), the involved party may:
        a. Be immediately suspended without notice pending the disposition of the law enforcement report and,
        b. Undergo an Audit by the Registry Management team to determine their involvement in the matter.
B. NASTF reserves the right to provide basic information to law enforcement, prosecutors, and other government officials in response to official inquiries of activity involving the Registry without any notification requirement to the VSP. Basic information includes:
    1. VSP name
    2. Business name
    3. Business address
    4. Business telephone number
    5. Vehicle identification information
    6. Ownership information
    7. Date/Time of transaction
    8. Location of transaction
    9. Production of records, copies of photographs, and other materials will be provided upon request to law enforcement and prosecutors pursuant to court orders.
    10. NASTF reserves the right to withhold notification to user(s) as such notification may compromise sensitive law enforcement investigations or other official proceedings.
C. VSPs shall immediately report all interactions with law enforcement related to NASTF, SDRM, the Registry, or NASTF-OEM involved transactions at https://support.nastf.org/.
D. Anyone who accesses the Registry or uses SDRM also has a duty to cooperate with NASTF's inquiry into their actions, access to the Registry, use of SDRM, or use of their credentials in the matter.
E. Failing to cooperate with audits or inquiries constitutes a serious violation and may result in immediate suspension and possible denial of access to the Registry and SDRM.

XII. Registry Management – Registry Manager

A. The Registry Manager oversees the Registry, the Registry Team, SDRM, VSPs, Assisted Immobilizer Reprogramming (AIR) Field Technicians, Assisted Immobilizer Reprogramming (AIR) Service Providers, Diagnostic Professionals (DP), and other members of NASTF.
B. The Registry Manager duties include, but are not limited to:
    1. Authority to review, approve, or deny issuance of General Members access
    2. Authority to review, approve, or deny issuance of VSP credentials
    3. Authority to review, approve, or deny issuance of AIR Field Technician credentials
    4. Authority to review, approve, or deny issuance of AIR Service Provider credential enhancement
    5. Authority to initiate audits and determine violations of policies
    6. Preliminary review of all reports of improper use of the Registry, SDRM, and related OEM software
    7. Conducting inquiries into the allegation of improper use of the Registry
    8. Authority to suspend or revoke credentials when it appears the preponderance of information sustains the allegation of a policy violation
    9. Manage appeals and refer any "official" appeals to the NASTF Executive Director for review by the Appeal Review Committee
    10. Forward any evidence established during the inquiry of the violation, to the Appeals Review Committee and/or law enforcement as appropriate or requested.
    11. Upon final disposition by the Appeals Review Committee the Registry Manager, or their designee, with the concurrence of the Executive Director, will notify the appellant of the final disposition.

XIII. Compliance

A. Registry and SDRM users must report misuse of the Registry, SDRM, VSP credentials, or OEM websites to NASTF support at https://support.nastf.org/
    1. Failure to report misuse may result in:
        a. Suspension of credentials, or
        b. Denial of Registry access.
B. NASTF will review the seriousness of the misuse, and may take such action as it deems in its sole discretion to be appropriate under the circumstances
C. NASTF will conduct inquiries into misuse allegations and alleged violations of policies
D. Initiating a dispute or chargeback with credit card companies without first opening a support case with NASTF violates these policies and may result in denial of Registry access.
E. Credit card chargebacks made after the approval of an application for Registry access (VSP credentials) will be considered fraud and whenever appropriate referred to proper authorities.

F. Attempting to mislead NASTF staff by providing fraudulent information or altered documents during application, renewal, audit, or inquiry may result in denial of Registry access.

XIV. Dispute Resolution and Appeal Process

A. Unless otherwise provided above, Registry and SDRM users have the right to appeal:
   1. Denial of credential issuance
   2. Suspensions of credentials
   3. Denial of Registry access
B. NASTF reserves the right, in its sole discretion, to determine whether a breach of any policy set forth herein has been committed, and to determine the seriousness of any such breach.
C. All determinations upheld by the NASTF Appeals Review Process are final.
D. Detailed information about the Dispute Resolution and Appeals Process can be found in Policy Section II titled Dispute Resolution and Appeal Process.

POLICY SECTION VI
VEHICLE SECURITY PROFESSIONALS

Table of Contents

POLICY SECTION VI
VEHICLE SECURITY PROFESSIONALS

I. Purpose and Scope

This document outlines the Vehicle Security Professional ("VSP") credentialing program which is used to access the Vehicle Security Professional Registry "(Registry") through the Secure Data Release Model ("SDRM") portal. This policy applies to all members who apply for the VSP credential, or who already hold the VSP credential of: Primary-VSP, Subordinate-VSP, or Administrative-VSP.

II. Benefits

A. The VSP credential greatly enhances general membership by offering additional credential profiles
B. The VSP credential is NASTF's premier credential and is recognized across the industry as signifying professionals who prioritize their customers' vehicle security.

III. Eligibility Requirements for VSP Credentials

A. Requirements for VSP credentials are as follows:
    1. Credentials are issued to an individual natural person, and not a business
    2. Individuals must be, or become, NASTF (general) Members
    3. Individuals must maintain their NASTF (general) Membership in good standing
    4. Individuals must have a business affiliation with the automotive repair industry, including, but not limited to:
        a. Professional Automotive Service Technicians
        b. Locksmiths specializing in automotive
        c. Individual shop owners
        d. Automotive Service-Related Associations
        e. Service Writers
        f. Tool and Equipment Companies
        g. Educators and Trainers
        h. Repossession Agents
        i. Collision Repair Specialist
        j. Original Equipment Vehicle Manufacturers (OEM)
        k. Original Equipment Manufacturers (OEM) Service Employees
        l. Other automotive industry professionals not listed herein who wish to participate with NASTF
    5. The individual's affiliated business must be registered as one of the following:
        a. Sole Proprietorship
        b. Partnership
        c. Limited Liability Company
        d. Corporation
B. The applicant or registered member:
    1. Must undergo and successfully pass a background screening check.

2. Must not have been arrested or convicted of a crime involving theft or misuse of motor vehicle, even if adjudication has been withheld or deferred.
3. Must not have any felony convictions relating to crimes involving theft, larceny, fraud, crimes of violence, or crimes committed with deadly weapons if application is submitted within 5 years of release from confinement, parole, probation, and/or final court ordered restitution.
    a. Failing to disclose such convictions on the application may be cause for denial of Registry access.
4. Must be a legal resident, authorized to work in the United States or Canada.
5. Must possess and supply Federal Employer Identification Number (EIN) or Canadian Business Number
6. Must be properly licensed and registered in all states or provinces in which they conduct business.
7. Must be in good standing in the jurisdictions where they conduct business.
8. Must respond to all inquiries or requests for information by the Registry Management Team during the application process or audit notifications.

C. Documents Required for Application
    1. Applicants are required to upload current and legible copies of the following documents as proof of identification:
        a. Color copy of valid US driver's license
        b. Color copy of valid Canadian driver's license
        c. The following documents will not be accepted as proof of identification:
            i. Temporary driver's license
            ii. Passports State-issued identification card
            iii. Illegible documents
            iv. Expired driver's licenses
            v. Black and white copies

    2. Certificate of Insurance
        a. A standardized Certificate of Insurance (COI) form, generally the Acord 25 form, is utilized for Certificate of Liability Insurance. This form provides:
            i. Proof an insurance policy exists (but does not amend details of coverage)
            ii. Types and limits of coverage
            iii. Insurance provider
            iv. Policy number
            v. Named insured(s)
            vi. Policy effective periods
        b. NASTF must be named as a Certificate Holder on the policy
        c. NASTF's address for the certificate is: 7310 W. 52nd Avenue, Suite A #335, Arvada, CO 80002.

   d. All COIs should be sent by the insurance agent/insurance company to COI@nastf.org.
   e. **DO NOT** mail a Certificate of Insurance (COI) to NASTF.
3. Coverage Requirements
   a. Primary Accounts require at least one (1) million dollars of General Liability Insurance aggregate/$500,000 per event General Liability Insurance.
   b. Subordinate Accounts require a minimum of $100,000 employee dishonesty/surety bond in addition to the General Liability policy for the Primary.
   c. Please have your agent include proof of the minimum $100,000 employee dishonesty/surety bond on your Certificate of Insurance and email directly to COI@nastf.org.
   d. **DO NOT** mail a Certificate of Insurance (COI) to NASTF.
4. Documents to establish proof of business ownership or employment:
   a. Copies of your state business license, if required.
      i. Your state may not require a "General Business License;" however, in most states, a business must register with the state's Department of Revenue and file a business tax report, which would be accepted.
      ii. If business operations cross state or provincial lines, the business must be properly registered in all states or provinces in which they conduct business.
   b. Current Certificate of Good Standing from your Secretary of State
      i. These can be obtained in nearly all cases by visiting the Secretary of State website and completing a file download or screen capture.
   c. If operating as a sole proprietorship, copies of appropriate permits and licenses to operate legally within your State.
      i. If your state does not require sole proprietorships to obtain permits/licenses, provide a redacted copy of your current Schedule C (Form 1040), Profit or Loss from Business (sole proprietorship) that is signed and dated as submitted to the Internal Revenue Service.
      ii. These documents will only be accepted for sole proprietorship.
   d. If residing in California and operating as an auto repair business in the State, copies of the Bureau of Automotive Repair (BAR) license certificate.
5. Locksmith Licenses or Other Designated Specialist Licenses
   a. NASTF requires locksmith licenses for anyone who uses the Registry whose business advertises locksmithing services and business operations are conducted within one of the municipalities, cities, or states (in both the US and Canada) requiring a security professional to possess a locksmith license.
   a. NASTF does not require locksmith licenses for any repair professional who does not advertise locksmithing services and when business operations are

conducted within one of the municipalities, cities, or states (in both the US and Canada) requiring a security professional to possess a locksmith license to replace, calibrate, or reprogram modules during the repair process.

b. The VSP assumes all responsibility for compliance with their local and state rules, ordinances, and statutes.

I. VSP Credential Dues and Fees

A. All applicants must pay the required Credential Dues and Background Screening Fees (biennial) in full at the time of application.
   1. Primary-Vehicle Security Professional (VSP) credential dues: $335.00.
      a. Requires Background Screening: $100.00.
   2. Subordinate-Vehicle Security Professional (VSP) credential dues: $150.00.
      a. Requires Background Screening: $100.00.
   3. Company Administrator: No-Cost.
      a. No Background Screening required.

B. All dues and fees are established by the NASTF Board of Directors and subject to change.

II. VSP Credential Application Rejections and Denials

A. Due to the stringent application process, approval of VSP credentials is not guaranteed. Applicants notified of a rejected application or missing documentation will be provided with an opportunity to:
   1. Complete their application
   2. Correct their profile information
   3. Submit or resubmit necessary documentation
   4. Provide explanations, if requested by NASTF.

B. Misrepresentation: Submission of any false, fraudulent, or misleading information is grounds for immediate denial.
   1. In cases of misrepresentation, all dues and fees are strictly non-refundable.

C. This policy applies to both new and renewing VSP applicants, regardless of expiration date, renewal status, or renewal approval date.

D. Applicants rejected or denied for reasons other than misrepresentation may appeal the decision by following the procedures in Policies, Section II, titled Dispute Resolution and Appeals Process.

VI. Dormant VSP Applications

A. A VSP application becomes “dormant” if it remains incomplete for more than sixty (60) days from the origination of application without an attempt to finish or submit for review.

B. Dormant applications will be nullified.
   1. Refund requests for Credential Dues of dormant (nullified) applications must be made within ninety (90) days of the origination of the application.

2. Background screening fees are non-refundable if the screening process has started.

VII. VSP Credential Application Withdrawals

A. Applicants may voluntarily withdraw their VSP application by submitting a support ticket at https://support.nastf.org/.
B. Requirements:
    1. Withdrawal requests must be received within twenty-four (24) hours of the initial application submission to ensure eligibility for a full refund.
    2. The applicant must provide a specific reason for the withdrawal at the time of their request.
C. Members who voluntarily withdraw their VSP applications will not be granted access to the Registry and are not eligible to appeal.
D. Voluntary withdrawal of VSP applications does not change general membership status.

VIII. Refunds of VSP Credentials

A. VSP Credential Dues:
    1. Applicants who do not meet VSP requirements, or whose application becomes dormant, may request a refund of their Credential Dues within ninety (90) days of originating their application.
    2. Applicants who voluntarily withdraw their VSP application within twenty-four (24) hours of originating their application may request a refund of their Credential Dues.
    3. Credential Dues are non-refundable if the VSP credentials have been utilized to access vehicle security information.
B. Background Screening Fees:
    1. Background screening fees will only be refunded if the VSP application is voluntarily withdrawn within twenty-four (24) hours of originating the application, and
    2. The background screening process has not yet been initiated.
    3. Otherwise, background screening fees are non-refundable as they are paid to third-party providers.
        a. This includes applicants who fail the background screening.
C. Approved refunds will be issued to the original payment method used during the application process.

IX. Primary-VSP Credentials

D. The Primary-VSP account holder is often, but not required to be, the business owner or lead technician.
A. The Primary-VSP may apply for additional accounts for other owners, or their W2 employees, as deemed necessary to support business operations.
B. In a multiple VSP business, the primary account holder should be the person directly managing any Subordinate or Company Administrator accounts.

C. The Primary-VSP account holder is responsible for all transactions and Registry activity that occur on:
    1. Their Primary-VSP account
    2. Subordinate-VSP account
    3. Company Administrator account
D. The Primary-VSP account holder may add Subordinate-VSPs by completing an application in the SDRM portal.
    1. The Primary-VSP may add Company Administrator accounts.
    2. The Primary-VSP account holder may change account access permissions for Subordinate or Company Administrator accounts.
E. The Primary-VSP account holder shall manage account information for the business (phone numbers, addresses, e-mail addresses, etc.). Additionally, the Primary-VSP account holder is responsible for all their Subordinate-VSPs.
F. The Primary-VSP account holder must:
    1. Be located within a "reasonable distance" of the subordinate's location
        a. "Reasonable distances" will be determined by the Registry Manager based on various criteria such as:
            i. Geographic distance
            ii. Business organizational plans
            iii. Number of VSP accounts
            iv. Potential security risks
G. Sharing account access is strictly prohibited and a violation of these policies may lead to suspension or denial of Registry access.
    1. E.g., Sharing credentials with an entire shop (or multiple shops) for Mercedes-Benz Theft-Relevant Parts purchases is not an accepted use.

IX. Subordinate-VSP Credentials

A. Subordinate Accounts are only available in the United States to employees receiving an Internal Revenue Service (IRS) Wage and Tax Statement (W-2 form) to report annual wages paid to employees and taxes withheld from their paychecks from a US-based employer.
    1. Subordinate accounts are not available to independent contractors.
    2. Subordinate-VSP accounts are not available for Canadian members.
        a. All Canadian accounts must be registered as Primary-VSP.

X. Company Administrator Credentials

A. The Company Administrator account allows business support staff to:
    1. Initiate Customer Authorization Document ("D1") forms.
    2. Update company documents within the SDRM portal.

B. This profile is only available for US-based businesses and does not have access to security operations on automaker websites.
C. The Company Administrator may not access, view, handle, input, or otherwise engage with key and immobilizer codes, or any process involving keys/fobs originating from the automaker's codes.
D. Company Administrator accounts must be approved and supervised by Primary-VSP account holders and cannot be under the supervision of Subordinate-VSPs.

XI. Access to Registry, Use of SDRM, VSP Responsibilities

A. In addition to NASTF General Membership policies, the following rules apply to VSPs:
    1. Unauthorized access or use of SDRM or OEM website information constitutes a serious violation of NASTF policies.
    2. Mishandling vehicle security information risks vehicle theft and misappropriation of sensitive data. Any such action is accordingly deemed to be a severe violation of NASTF policy
    3. Vehicle security information from the Registry through SDRM is for single use only
    4. VSPs may be required to collect and record Personally Identifiable Information (PII) from customers, as detailed in Section VII titled Customer Authorization Document (D1)
        a. Once uploaded into SDRM, proper disposal of PII is required.
        b. VSPs should familiarize themselves with requirements outlined in the Customer Authorization Document (D1)
    5. VSP account holders shall:
        a. Treat vehicle security information as confidential.
        b. Not sell, buy, trade, barter, or share security-related information or devices.
        c. Take necessary security precautions to prevent loss or dissemination of vehicle security information as required by OEMs and NASTF.
        d. If requested by the vehicle owner, VSPs may provide vehicle security information to the vehicle owner, whose name appears on the vehicle title.
    6. The vehicle owner must legally possess and be physically present with the VSP and the vehicle.
    7. The VSP may not disclose the vehicle security information to another person, even with the vehicle owner's permission.
    8. The VSP shall only communicate vehicle security information verbally to the vehicle owner when present with the vehicle.
    9. If the vehicle is titled in a business or entity name, authorized business representatives may receive vehicle security information with proper identification indicating their connection to the business (such as a business card or written authorization on company letterhead with their name listed) along with government-issued identification of the authorized representative.
    10. Not provide vehicle security information if a valid and current title vehicle title is unavailable.

11. Not provide vehicle security information to lien holders or finance companies not listed on the vehicle title as owners
12. Not share usernames, security credentials, passwords, or multi-factor authentication codes.
13. Not retain, store, or electronically transfer security-related information.
14. Not mail or ship vehicle security devices such as keys, fobs, cards, control modules, or other devices which were created with security information obtained with VSP credentials.
15. Not provide security devices except as outlined in Section VIII titled D1plus1.
16. Be present to verify customer's legal ownership and possession, before performing vehicle security work on the vehicle or directly supervising the vehicle security work except as outlined in Section VIII titled D1plus1.
    a. Allowing "another" technician or individual to access the Registry, or any codes obtained from the Registry, does not qualify as supervision.
    b. Allowing an entire shop to use an individual's VSP credentials to order Mercedes parts is not considered "direct" supervision and constitutes a violation of these Policies.
17. Only perform service on vehicles physically located in the US or Canada.
18. Acknowledge that all NASTF support requests may only originate from the Primary-VSP and not from the Subordinate-VSP or Company Administrator.
19. Not register subcontractors (1099 recipients) technicians as VSPs.
20. Not use vehicle security information for any unauthorized purpose
21. VSPs are:
    a. Strictly prohibited from using Virtual Private Networks (VPNs) or any technology designed to mask or conceal their true geographical location while accessing any NASTF system.
    b. Required to keep location services enabled on the devices used to access NASTF systems to ensure compliance with location-based security protocols.
22. NASTF reserves the right to monitor user activity and employ technology to detect and prevent the use of VPNs or any other location-masking software.
    a. Use of such technology is a violation of these policies and will result in immediate suspension and possible denial of Registry access.

XIII. VSP Credentials – Validity, Expiration, and Renew

A. VSP credentials are valid for two years from the date of approval. After such time, if the VSP fails to actively apply for renewal, the credentials will automatically expire.
B. To avoid disruption of Registry access, before account expiration, a renewal application must be submitted with the appropriate fees and other information as indicated on the Registry website.
C. Renewals may be submitted at least sixty (60) days before the expiration date to avoid interruptions in validity of VSP credentials and Registry access.

1. It is the responsibility of the VSPs to submit the renewal application in a timely manner.

D. The responsibility to renew VSP credentials rests solely with the Primary-VSP.
E. When a Primary-VSP credential expires, all associated Subordinate-VSP and Company Administrator accounts will be suspended until the Primary-VSP account is reviewed, approved, and renewed.
F. Failing to respond or provide information requested by the Registry Team during the Registry renewal process may result in delay of processing the application and/or suspension of Registry credentials.
G. Submitting false or altered documents, fraudulent information, or attempting to mislead the NASTF registry team during the renewal process will result in immediate suspension and denial of Registry access.
    1. In such cases, the application fees will be forfeited and not be refunded
    2. In such cases, the applicant will have no right to appeal

XIV. Change in Status, Expired Documents

A. All accounts will be suspended if current documentation is not on file in the SDRM portal
B. If any required documentation expires, the Primary-VSP must upload current documents within fifteen days
C. Although the Registry software will attempt to provide email and login notifications before expiration, the Primary-VSP assumes all responsibility for maintaining current documentation for all associated accounts.
D. If a VSP's status changes they must report those changes to NASTF support within fifteen (15) business days. Examples of status changes include:
    1. Change in employment/employer
    2. Change in State residency
    3. Arrest for any criminal charges
    4. Conviction of any criminal charges
    5. Lapse of insurance
    6. Lapse of business in good standing
    7. Lapse of locksmith license, if applicable
    8. Criminal, Civil, or administrative action against VSP, or VSP's business, that concerns fraud, dishonesty, or mishandling of third-party information.

XV. Voluntary Relinquishment of VSP Credentials

A. Members may voluntarily relinquish their VSP credentials and still maintain their General Membership, unless otherwise noted within NASTF policies.
B. VSPs may relinquish their credentials by creating a support ticket on the NASTF website (https://support.nastf.org/) indicating they wish to relinquish their VSP credentials.
C. VSP must provide a reason for the relinquishment of their VSP credentials.

D. Relinquishment of VSP credentials does not relieve the member from their financial obligations to NASTF.
E. There will be no refunds if VSP credentials have been used to access vehicle security information.
F. Relinquishment does not prevent NASTF from sanctioning a member for violations of NASTF rules and policies.

XVI. Vehicle Security Information Audits

A. NASTF reserves the right to conduct security audits, whether at random or in the event NASTF receives a report of concern, to ensure compliance.
B. All VSPs are subject to audits
C. Cooperation with security audits is mandatory
D. Audit notifications will be sent to the email address listed within the VSP's member profile
E. VSPs have five (5) business days to respond to an audit inquiry
    1. Failure to provide requested information within five (5) business days of the auditor's request is a violation of the policies.
    2. Failure to respond to or cooperate with the audit may result in suspension or denial of Registry access.

XVII. Suspension and Denial of Registry Access

A. VSPs have the right to dispute denial of credentials, suspensions, or denial of Registry access.
B. Members who wish to file an appeal (appellants) shall follow the policies set forth in Policy Section II titled "Dispute Resolution and Appeals Process".

XVIII. Duty to Cooperate

A. NASTF has a duty to cooperate with law enforcement and other organizations regarding possible criminal activity.
B. If the inquiry involves use of the Registry and/or involvement of a VSP(s), the involved party:
    1. May be immediately suspended without notice pending the disposition of the law enforcement, administrative agency, or other organizations final ruling.
    2. Will undergo an audit by the Registry team to determine their involvement in the matter.
    3. Cooperate with NASTF's inquiry into their actions, access to the Registry, use of SDRM, or use of their credentials in the matter.
C. Failing to cooperate constitutes a serious violation and will be grounds for immediate suspension of VSP credentials, and possible denial of Registry access.

XIX. Violations

A. VSPs must immediately report misuse of the Registry, SDRM, VSP credentials, or OEM websites to NASTF support at https://support.nastf.org/
B. Failure to report misuse may result in suspension or denial of Registry access.
C. NASTF will inquire about misuse allegations and alleged violations of policies
D. Initiating a dispute or chargeback with credit card companies without first opening a support ticket with NASTF is a violation that will result in suspension of credentials and possible denial of Registry access.
E. Credit card chargebacks made after the approval of an application for VSP will be considered fraud
F. Attempting to mislead the inquiry by providing fraudulent information or altered documents may result in suspension or denial of Registry access.
G. Nothing herein prevents the removal of a member in accordance with the NASTF bylaws by the Board of Directors.

XX. Dispute Resolution and Appeals Process

A. NASTF reserves the right, in its sole discretion, to determine a breach of any policies set forth herein, and all determinations upheld by the NASTF Appeals Review Process are final.
B. Detailed information about the Dispute Resolution and Appeals Process can be found in Policies, Section II, titled Dispute Resolution and Appeal Process.

POLICY SECTION VII
CUSTOMER AUTHORIZATION DOCUMENTS

Table of Contents

POLICY SECTION VII
CUSTOMER AUTHORIZATION DOCUMENTS

I. Purpose and Scope

This document outlines the requirements and responsibilities of credential account holders when collecting Personally Identifiable Information ("PII") and vehicle identification information as outlined in NASTF Policies, Sections IV, V, VI. The collection of this information is necessary for access to vehicle security related data accessed through the Vehicle Security Professional Registry ("Registry"), obtained through the Secure Data Release Model portal ("SDRM"), or from the Original Equipment Manufacturers ("OEMs").

II. Benefits

A. Customer Authorization Document ("CADs" otherwise known as "D1") confirms a customer's legal authority and positive identification of the customer to access a vehicle
B. All Vehicle Security Professionals ("VSPs"), including Primary and Subordinate, and Assisted Immobilizer Repair Technicians ("AIR Techs") should familiarize themselves with the distinct types of CADs/D1s (defined and described below)
C. VSPs must ensure they have collected the necessary Vehicle Information, and Ownership Verification and Authorization Documentation for the transaction.
D. Registered VSPs must be present with owner(s) and vehicle(s) to verify ownership and legal possession before utilizing vehicle security information or programming keys/fobs/devices.

III. Vehicle Information Requirements

A. The requirements outlined in this section apply to all CAD/D1s unless otherwise noted.
B. Enter full Vehicle Identification Number
    1. Hit the "decode" button to decode the VIN and prepopulate specific vehicle information
    2. Ensure the decoded vehicle information is correct, if not manually enter:
    3. Vehicle year
    4. Make
    5. Model
C. The following fields will not decode and must be manually entered:
    1. Vehicle mileage
    2. Vehicle color
    3. Vehicle license plate number
    4. State/Province
D. Verify the VIN on the vehicle matches the VIN on the ownership documentation.
E. Verify the VIN on the vehicle matches the VIN stored within the vehicle's electronic control modules.

IV. Ownership Documentation Requirements

A. The requirements outlined in this section apply to all CAD/D1s unless otherwise noted.
B. At least one of the following documents is required as proof of ownership:
    1. Original Certificate of Title
        a. If title is open, buyer's name must appear on transfer section of title.
        b. If the Original Certificate of Title is held electronically, then a printout from DMV is acceptable.
    2. Registration
        a. With owner's name and address printed on it
        b. Registration must be current and match vehicle presented.
    3. Vehicle Bill of Sale
        a. Must contain name of customer presenting vehicle for service
        b. Must contain name of seller
    4. Proof of Insurance
        a. Printed card containing owner's name and vehicle identification number.
        b. Electronic cards must contain owner's name and vehicle identification number.
        c. Upload screenshot of electronic cards as proof of insurance.
C. Utilizing the Customer Authorization Document (CAD/D1), VSPs must select "Verification Type" from drop-down menu and choose:
    1. Vehicle Title
    2. Registration
    3. Bill of Sale
    4. Insurance

V. Authorization Documentation Requirements

A. The requirements outlined in this section apply to all CAD/D1s unless otherwise noted.
B. If the person (customer) in possession of the vehicle is the owner, the only acceptable forms of Ownership Verification are:
    1. United States driver's license
    2. Canadian driver's license
C. Identification documents such as State/Province issued identification cards, foreign passports, foreign identification cards, and forms of immigration identification are not accepted forms of authorization identification, except in the following circumstances:
    1. If the vehicle owner's driver's license was stolen and the vehicle owner can prove they have reported the theft of their driver's license by producing a copy of an official police report.
D. The copy of the police report must contain:

1. Law enforcement agency name
2. Law enforcement agency case number
3. Victim's name (must match that of the customer/owner present)
4. Victim's driver's license number and State of issuance

E. Upload a legible photograph of the police report to SDRM
F. In such cases, a passport issued by the United States or Canada, or other "official" government issued identification with the customer/owner's photograph may be accepted, but only in such circumstances
G. Utilizing the Customer Authorization Document (CAD/D1), VSPs must enter the following information:
   3. First Name
   4. Last Name
   5. Select "Country"
   6. Zip Code, then click "decode" and verify the detected City and State/Province are correct

VI. Corporate Entity Ownership

A. If the Vehicle Owner is a lienholder or other corporate entity, verify the customer's authority and identity through:
   1. Corporate employee's US or Canadian driver's license.
   2. Photographic proof the individual is an employee of the vehicle owner (e.g., an employee identification card with their photograph and the business name on the card).
   3. NASTF suggests the employee's identification card be photographed and uploaded; however, if they object it is not required.

VII. Family Member Authorization

A. If the person in possession of the vehicle is a family member, spouse, caretaker, or other individual designated by the owner verify the requesting individual's authority and identity is confirmed through either US or Canadian driver's license.
B. If the person in possession of the vehicle is a family member of the registered owner, verify ownership documentation matches the vehicle owner's identity by last name and address.
C. Photographic or written proof the individual in possession of the vehicle is authorized by the Vehicle Owner.
D. Photographic or written proof should be verified by the VSP/AIR Tech through direct contact with the owner.

VIII. Document and Photograph Requirements

A. Upload legible photographs of the Positive Identification documents to SDRM

B. When using a smartphone/tablet (or other device equipped with a camera) for CAD/D1 completion, photograph the Positive Identification documents with the same device and upload directly to SDRM without storing Personally Identifiable Information (PII) on a computer
C. Whenever the VSP or AIR Tech is using an actual camera, or other method, to photograph the Positive Identification documents NASTF requires them to delete/destroy all photographs containing PII after successfully uploading the photographs to the SDRM system.
D. Multiple ownership authorization documents may be provided as one file and uploaded directly to SDRM.

IX. Customer CAD/D1

A. This form is used when the customer presenting the vehicle is the owner or can provide proof of ownership.
B. Follow the vehicle ownership requirements outlined above on page 2, Section III, titled "Vehicle Information Requirements."
    1. Include the Purchase or Repair Order Number.
C. Follow the ownership verification requirements outlined above in on page 3, Section IV, titled "Ownership Documentation Requirements."
    1. The VSP confirms the vehicle ownership documentation matches the vehicle presented for service.

X. Auction, Fleet, or Dealership CAD/D1

A. Used for auctions, fleet garages, or dealerships performing services under a work or purchase order.
B. Vehicle Information: Follow the Ownership Documentation Requirements outlined above in Section III (page 2) of this document.
A. Fleet/Auction/Dealership Authorization Documentation:
    1. Business Name
    2. Business Telephone Number
    3. Business Country (must be US or Canada)
    4. Business Address
    5. Business City
    6. Business State (or Province)
    7. Business Zip (or Postal) Code
C. Obtain a work, purchase, or repair order from the auction/fleet/dealership representative; (e.g. email or other correspondence).
D. Documents must include:
    1. VIN
    2. Vehicle Year
    3. Vehicle Make

4. Vehicle Model
5. Location of Vehicle
6. Contact information for individual requesting services

E. Fleet Vehicles: Authorization may be verified by confirming employment with the business to whom the vehicle is registered.
F. Towing and Lien Sale Process (Involuntary Vehicle Transfers)
    1. This applies to non-consensual tows, impounds, abandoned vehicles, mechanics' lien, Sheriff's sale, Police auction, civil asset forfeiture, or any other form of lien sale.
    2. Towing and lien sale process is only available "post-sale" upon completion of all state statute requirements governing such sales and/or transfers.
    3. If title is present, in name of business/entity, upload copy of title.
    4. If title, in name of business/entity, is not available upload "Proof of Authority" (e.g. TX form CTR-265-M, NY form MV-901C, FL form HSMV 82040, or court order awarding ownership) in accordance with state statutes governing such sales.

XI. Contracting CAD/D1

D. This CAD/D1 is utilized whenever performing work for a third party or repair shop.
E. The third party or repair shop gathers customer authorization and provides the required information:
F. Follow the vehicle ownership requirements outlined above on page 2, Section III, titled "Vehicle Information Requirements."
    2. Include the Purchase or Repair Order Number.
G. Follow the ownership verification requirements outlined above in on page 3, Section IV, titled "Ownership Documentation Requirements."
    2. The VSP confirms the vehicle ownership documentation matches the vehicle presented for service.

H. NASTF recommends VSPs confirm that the third party or repair shop has the required customer authorization documentation before arrival to prevent incomplete CAD/D1 transactions.

XII. Repossession CAD/D1

A. Used only by VSPs servicing repossessed vehicles in a repossession, recovery, or storage facility.
B. VSP is required to upload copies of executed repossession orders from the finance company/lien holder as the authorizing party.
C. Exception: Buy Here Pay (BHPH) repossessions
    1. In jurisdictions where state law does not mandate a formal repossession order, a Purchase Order or Sales Contract may serve as a substitute for a repossession order, provided it explicitly grants the BHPH dealer the authority for immediate self-help repossession.
    2. Use of this substitute documentation is contingent upon the following:
        a. Proof of Authority: The contract must clearly outline the right to seize the collateral upon default.

b. Regulatory Compliance: VSP must satisfy all secondary requirements detailed in subsections D through H of this policy.

D. Vehicle Information: Follow the Ownership Documentation Requirements outlined above in Section III (page 2) of this document.
E. Verify the vehicle's VIN matches the VIN on the repossession order or BHPH contract.
F. Client Information/Authorization Documentation: ONLY the lienor/lessee (vehicle owner) name and social security number should be redacted (or marked out) prior to uploading the repossession order.
G. All other ownership information on the repossession order must be legible and available for review.
H. If the lien holder and client are the same, provide the following information:
    1. Business Name
    2. Business Telephone Number
    3. Business Country (must be US or Canada)
    4. Business City
    5. Business State (or Province)
    6. Business Zip (or Postal) Code
    7. If the lien holder and client are different, provide the same information for both
I. Recovery Details:
    1. Enter the Recovery Date
    2. Enter the address where the vehicle was recovered
    3. Enter the law enforcement agency notified of repossession

XIII. In-Transit CAD/D1

A. Used only by VSPs contracted by an Original Equipment Manufacturer (OEM) or OEM Vendor for in-transit or special projects (e.g., replacement of stolen or lost key/fob).
B. Vehicle Information:
    1. Select the OEM Brand.
    2. Enter the last six digits of the VIN.
    3. Click “Search” to look up the vehicle data.
C. Authorization Documentation: The OEM/Contractor provides the VSP with service request information.
    1. This CAD/D1 is for one-time use and is valid for 14 days.
    2. It may not be shared.

XIV. Mercedes-Benz Theft Relevant Part (TRP) Order Form

A. Used only by VSPs to submit a TRP parts request to a Mercedes-Benz Dealer.

I. Follow the vehicle ownership requirements outlined above on page 2, Section III, titled “Vehicle Information Requirements.”
    1. Include the Purchase or Repair Order Number.

J. Follow the ownership verification requirements outlined above in on page 3, Section IV, titled "Ownership Documentation Requirements."
    1. The VSP confirms the vehicle ownership documentation matches the vehicle presented for service.

B. If you are requested to submit any other form(s) please notify NASTF Support at https://support.nastf.org so NASTF can work with Mercedes-Benz to educate the dealer on the TRP process.
C. The dealer process has not changed; the dealer will contact you to confirm details prior to completing your order.
D. You no longer need to use the TRP form on the Startek website. NASTF will forward the order request directly to your selected dealer.

XV. Rivian CAD/D1

A. This CAD/D1 is utilized whenever performing work on all Rivian vehicles including passenger vehicles and Electric Delivery Vans (EDVs) sold to Amazon.
B. The Rivian Fob must be purchased before work begins on the vehicle.
C. Rivian requires the fob's human-readable identification (HRID) during the CAD/D1 process.
D. When the Rivian is a privately owned passenger vehicle and request is from an owner, Rivian requires:
    1. Follow the vehicle ownership requirements outlined above on page 2, Section III, titled "Vehicle Information Requirements."
    2. Follow the ownership verification requirements outlined above in on page 3, Section IV, titled "Ownership Documentation Requirements" and confirm the vehicle ownership documentation matches the vehicle presented for service.
E. When the Rivian is part of an auction, dealership, or fleet vehicle (regardless of whether passenger or EDV), Rivian requires:
    1. Copy of signed invoice/work order from the authorizing party
    2. Vehicle Identification Number
    3. Model Year
    4. Model
    5. Location of vehicle
    6. Contact Information for the requesting party
F. When the Rivian vehicle is part of a repossession/recovery, Rivian requires:
    1. Copy of the executed repossession order
    2. Vehicle Identification Number
    3. Model Year
    4. Model
    5. Lien holder/financial institution
    6. Authorizing party contact information

XVI. Compliance

A. It is imperative a CAD/D1 is completed on every transaction within five (5) days of the transaction.
B. NASTF and the OEMs view the completion of a CAD/D1 as essential to preventing unauthorized transactions.
C. All CADs/D1s are in electronic format and must be created via NASTF's SDRM portal
D. Failure to comply will result in credential suspension
E. Suspended VSPs may be required to undergo CAD/D1 training and/or be subject to an audit.
F. Failure to complete training or comply with audit requests, or repeated CAD/D1 completion violations, are grounds for denial of Registry access.
G. NASTF provides training videos for CAD/D1 completion on each CAD/D1 screen and in the Training Library on NASTF's website.
H. Contact NASTF Support at https://support.nastf.org/ for further information, if you need assistance determining which CAD/D1 to use, or you have general questions.

XVII. Dispute Resolution and Appeals Process

A. NASTF reserves the right, in its sole discretion, to determine a breach of any policies set forth herein, and all determinations upheld by the NASTF Appeals Review Process are final.
B. Detailed information about the Dispute Resolution and Appeals Process (Appeals Process) can be found in Policy Section II titled Dispute Resolution and Appeal Process.

POLICY SECTION VIII
D1PLUS1 PROCESS

Table of Contents

POLICY SECTION VIII
D1PLUS1 PROCESS

I. Purpose and Scope

This document outlines the "D1plus1 Process" (defined below) used to enhance the existing Customer Authorization Document (otherwise known as "D1") process by offering improved accuracy, transparency, security, and compliance whenever two Vehicle Security Professionals ("VSPs") are working together.

II. Benefit

A. The D1plus1 Process is an enhancement to the existing Customer Authorization Document ("CAD/D1") process, designed to increase the accuracy of recording VSP whenever two VSPs are involved in a single transaction.
B. The D1plus1 Process is crucial for maintaining transparency and accountability because it helps track the involvement of multiple VSPs in the security-related process.
C. The D1plus1 Process applies whenever the VSP obtains security-related service information using the Secure Data Release Model ("SDRM") and then personally transfers the keys, fobs, or device to another VSP.
D. The D1Plus1 Process offers a robust solution while maintaining verified customer authorization and SDRM integrity.

III. Application of D1plus1 Process

A. The D1plus1 Process applies to various scenarios involving VSPs. Some key applications include:
    1. **Customer D1s**
        a. The D1plus1 Process allows smaller NASTF member organizations to cover more areas effectively. This ensures accurate recording and verification, enhancing their operations, and helps them provide better service to member customers.
    2. **Repossession D1s**
        a. In the case of repossession D1s, where high daily inventories are handled by a team, the D1plus1 Process plays a crucial role.
        b. The D1plus 1 Process helps accurately document the involvement of multiple VSPs, ensuring that all repossessions are authorized and compliant with guidelines.
    3. **Fleet/Auction/Dealership D1s**
        a. The D1plus1 Process Allows NASTF member businesses with high volume inventories and teams to increase efficiency.

b. The D1plus1 Process streamlines the verification process, reducing the risk of unauthorized activities and enhancing overall security.

4. Limitations

a. Sharing of vehicle security information is strictly prohibited
b. Under no circumstances shall data obtained be used to create, mail, email, or otherwise transmit data, keys, fobs, control modules, or other security-related devices outside of the NASTF-approved SDRM/OEM systems.
c. All personnel involved must be owners or W2 employees of the NASTF member business working at the same location.
d. Subordinate VSPs must be assigned to the Primary VSP (use drop-down selection on D1)
e. The VSP (subordinate or primary) acquiring the code and originating the device, key, or fob must be physically located near the second VSP performing work on the vehicle for which service is required.
f. The device, key, or fob must be personally transferred from the first VSP to the second VSP.
g. The D1plus1 program must comply with all other applicable federal, state, and local regulations and/or statutes.
h. It is the responsibility of the VSP to ensure such compliance.

IV. Compliance

A. Violations of these policies or NASTF's bylaws may result in suspension or denial of Registry access.
B. VSPs may appeal against suspensions or denial of Registry access by following the procedures outlined in Policy Section II titled Dispute Resolution and Appeals Process documentation.

POLICY SECTION IX
PRIVACY POLICY

Table of Contents

POLICY SECTION IX
PRIVACY POLICY

I. Purpose and Scope

This document outlines the National Automotive Service Task Force ("NASTF" or "we") Privacy Policy. Your privacy is important to NASTF, particularly given the security-critical nature of our products and services. This Privacy Policy addresses what personal and vehicle information we collect, the specific purpose for that collection, and how we handle the information shared with us.

II. Application

A. This Privacy Policy applies to personal and vehicle information we obtain from and about individuals interacting with NASTF and its websites, products, and services, including during the VSP credentialing and SDRM transaction processes. It does not apply to data collected for internal organizational purposes, such as employment or vendor management.

B. This Privacy Policy covers all NASTF controlled subsidiaries and affiliates in the U.S. and Canada. Certain high-security programs, such as the Secure Data Release Model (SDRM) Registry and the NASTF Mobile Authentication Application, may be subject to additional or supplemental privacy policies that should be reviewed by the user.

C. Key points about our information practices:

1. **Use:** We may use your information to provide products and services, to maintain customer relationships, to provide customer support and service, and for marketing. See below to learn more.
2. **Sharing:** We share information only as necessary to maintain the integrity of our security ecosystem and fulfill our service obligations. This includes sharing with:
    a. **Regulatory & Law Enforcement:** As required by law or legal process.
    b. **Security Partners:** Specifically with Automakers (OEMs) and the SDRM Registry to verify credentials and authorize secure data releases.
    c. **Credentialed Members:** To facilitate professional interactions within the NASTF network.
    d. **Service Providers:** Trusted third parties who perform tasks on our behalf (e.g., payment processing or IT security) and are contractually prohibited from using your data for any other purpose.
3. **No Sale of Personal Information:** NASTF does not sell, rent, or lease your personal information to third parties. We do not exchange personal data for monetary or other valuable considerations. Any data shared with business affiliates or partners is strictly for the purpose of delivering NASTF-sanctioned services, verifying professional identity, or enhancing vehicle security protocols.
4. **Choices:** You have choices regarding how we use and share your information for marketing and other purposes.
5. **Cookies and Tracking:** We may use cookies, pixel tags, web beacons, and similar tracking technologies to help provide our products and services, understand and customize your preferences, and display relevant advertising.

6. **Mobile Applications:** NASTF has developed certain mobile applications that you may access on your mobile device ("NASTF Applications"). When you access any NASTF Application, there may be an opportunity for you to provide us with, or for us to obtain, information about you, or the vehicle you are servicing.
7. **Location Information:** We collect location data solely for security purposes, such as to monitor authentication attempts and help protect your account from unauthorized access.
    a. When you use our mobile app (iOS or Android), we collect your device's location data only when you are actively using the app (e.g. during login). In such cases, your operating system will ask for your permission, which you can manage in your device's settings. Note: we do not track your location when the app is closed.
    b. When you sign in to our website, we capture your approximate location based on your IP address.
    c. If you manually disable location services in your device's settings, you will be prompted to re-enable them the next time you open the app, as access to the Registry and related services cannot be granted without them.
8. **Third Party Products and Services:** Using NASTF products and services, you may be able to access third party services, applications and websites not controlled by NASTF or covered by this Privacy Policy.
9. **Access and Update:** You may access your online accounts to update your information, or you may contact us to learn about how to do so.
10. **California Privacy Rights:** California residents have certain rights regarding the personal information we disclose to third parties for their own marketing purposes.
11. **Canadian Privacy Rights:** Canadian residents have certain rights regarding the personal information we disclose to third parties for their own marketing purposes.
12. **Security Measures:** We maintain reasonable and adequate security controls to protect your information and require our service providers by contract to do the same.
13. **Retention:** We retain personal and vehicle information only as long as necessary to provide our services, maintain the security audit trail required for the SDRM Registry, or comply with legal and regulatory obligations.
14. **Children's Privacy:** NASTF websites do not target or knowingly collect any information from children under the age of 16 years.
15. **International Data Transfers:** We maintain appropriate protections for cross-border transfers as required by law for international data transfers.
16. **Contact Us:** If you have concerns or questions regarding NASTF's consumer privacy practices or this Privacy Policy, please contact us at https://support.nastf.org/.
17. **Changes:** We may update this Privacy Policy from time to time. We will do so by posting additions or modifications to this page.

III. Information Collected

A. As you interact with NASTF, there may be opportunities for you to provide us with your information.
B. Additionally, we may collect certain information about you or the vehicle you are servicing through any number of sources including, but not limited to:
    1. NASTF websites
    2. Applications
    3. Product and related events
    4. Surveys
    5. Social media platforms
    6. Through our Support (customer) call center
C. We also collect information that is publicly available for example, we may collect publicly available information you submit to a blog, a chat room, or a social media platform such as Facebook, Twitter, or Google and we may use your information for the purposes set out in this privacy policy.
D. NASTF engages with service professionals on multiple social media platforms and if you contact us on one of our social media pages, request assistance via social media or otherwise direct us to communicate with you via social media, we may contact you via direct message or use other social media tools to interact with you. In these instances, your interactions with us are governed by this privacy policy as well as the social media platform you use.
E. We also receive information about you through vehicle security transaction records provided by you during key code operations.
F. NASTF performs background checks of all Vehicle Security Professional applicants.
    1. No data sourced in this process will be shared outside of NASTF contracted partners involved solely in the credentialing and security process.
G. We may combine information that we receive from the various sources described in this Privacy Policy, including third-party sources, with information you provide and use or share it only for the purposes identified above.

IV. Types of Information Collected by NASTF

A. Information collected may include, but is not limited to:
    1. Contact information
        a. Name
        b. Address
        c. City
        d. State or Province
        e. Country
        f. ZIP code or Postal Code
        g. Email address

h. Telephone number
i. Social media contact information
j. Payment information
k. Credit card number
    i. Security code (CVV)
    ii. Security codes (CVV) are not stored after the transaction is processed as consistent with PCI standards.

2. Expiration date
3. Billing zip code
4. Information about vehicles you are servicing
    a. License plate number
    b. Vehicle identification number (VIN)
    c. Make
    d. Model
    e. Model year
    f. Vehicle owner information including, but not limited to:
        i. Owner's name(s)
        ii. Owner's address
5. Information about your connected devices
        i. Mobile phone
        ii. Computer
        iii. Tablet
6. How you interact with our products, services, apps, and websites
        i. IP address
        ii. Browser type
        iii. Unique device identifier
        iv. Cookie data
        v. Associated identifying and usage information
7. Photographs and videos that you may submit during VSP transactions or VSP profile/application updates

V. Use of Information Collected

A. The information NASTF collects about you and vehicles you service may be used:
    1. To provide products and services and maintain customer relationships
    2. To improve the quality, safety, and security of our products and services
    3. To administer your account(s) and process your payments for products and services
    4. To operate our websites and applications, including online registration processes
    5. To autofill data fields on our websites to improve your online experience
    6. To develop new products and services.
    7. To provide information and product updates

8. For research, evaluation of use, and troubleshooting purposes
9. To verify eligibility in NASTF VSP programs
10. To support the electronic customer authorization and record-keeping processes (e.g., CAD/D1) between you and your customer.
11. To customize and improve communication content
12. To comply with legal, regulatory or contractual requirements

A. Communication with you in connection with these uses may be via:
   1. Mail
   2. Telephone
   3. E-mail
   4. Text message
   5. Social media
   6. Other electronic messages
   7. Through the SDRM Registry
   8. Through websites
   9. Through other applications

B. NASTF may send you text messages using an automated telephone dialing system to the mobile phone number you have provided if you have opted in to receive text messages. Opting to receive text messages is not a requirement to buy products or services from NASTF, and message and data rates may apply.

C. See "Choices" below in Section VI to learn how to manage your communication preferences.

VI. Sharing of Information Collected

A. NASTF may share the information it collects about you or the vehicles you service in the following instances:
   1. Within NASTF
   2. With NASTF controlled subsidiaries and affiliates
   3. Transaction information within the SDRM Registry
   4. This security-critical information (including VSPID, VIN, transaction time, and location data) will be accessed and shared only with Registry Administrators, security auditors, and law enforcement as required for program integrity, audit, and legal compliance.
   5. With our service providers who work on our behalf and who are contractually restricted from using the information we disclose to them for their independent use.
   6. With our business partners: We may share information with partners solely on joint marketing of NASTF-sanctioned services or to fulfill membership benefits.
      a. We do not disclose your personal information to third parties for their own independent marketing or commercial use without your express consent.

7. When we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud or respond to a law enforcement request.
8. As required by law, such as in conjunction with a subpoena, government inquiry, litigation, dispute resolution or similar legal processes.

B. Other than the purposes listed above, NASTF will not share information about you or vehicles you service with other third parties for their independent use without your prior consent.

VII. Choices About Information Collected

A. If you do not want to receive unsolicited marketing communications from NASTF, please visit nastf.org and unsubscribe by following the process.
B. This will allow you to opt out of unsolicited marketing telephone and email communications and/or to change previously submitted opt-out preferences.
C. If you opt out of receiving marketing communications from NASTF, your personal information will not be used for marketing but may still be used for the other purposes described in this Privacy Policy (such as SDRM Registry support).

VIII. Cookies/Tracking Technologies

A. NASTF may use:
   1. Cookies
   2. Pixel tags
   3. Web beacons
   4. Other tracking technologies
B. On our:
   1. Websites
   2. Applications
   3. Email messages
   4. Advertisements
C. To gather information about your visit such as:
   1. Demographic data
   2. Browser type
   3. IP address
   4. Pages visited
   5. Activities conducted on the page
   6. Day and time of your visit
D. Using cookies provides benefits to you, such as allowing you to maintain your account login information or contact information between visits.
E. In addition, we use information gathered from cookies to autofill fields on forms such as:

1. City
2. State or Province
3. Zip code or Postal Code
4. Country
5. Information associated with your IP address
6. Information associated with your VSP information

F. The information can be corrected by you before submitting any form or inquiry, or you can disable the cookie as discussed below and the information will not be collected.

G. We place pixel tags and web beacons in our emails to measure the effectiveness of our email campaigns by identifying the individuals:

1. Who opens or acts upon an email message,
2. When an email message is opened,
3. How many times is an email message forwarded,
4. Type of software,
5. Device,
6. Operating system,
7. Browser used to deliver email, and
8. Any URL accessed through our email message.

H. To measure site activity, provide better user experience, and tailor our marketing communications, we or our service providers or business partners may compile information from:

1. Cookies,
2. Pixel tags,
3. Web beacons, and
4. Other technologies on our websites.

I. This information may also be used to evaluate our online advertising campaigns or to tailor promotions and other marketing messages to you across your devices.

J. Currently, we do not honor “do no track” signals from a web site browser. However, you may refuse or delete cookies. Please refer to your browser Help instructions to learn more about cookies and other technologies and how to manage their use.

K. If you elect to refuse or delete cookies, you will need to repeat this process if you use another computer or change browsers. If you choose to decline cookies, some of the functionality of a website may be impaired.

IX. Mobile Applications

A. NASTF has developed certain mobile applications that you may download to your mobile device or vehicle (“NASTF Applications”).

B. When you download a NASTF Application, there may be an opportunity for you to provide us with or for us to obtain information about you and for the vehicles you service.

C. Each NASTF Application will display a separate Privacy Policy that will inform you about how any information is collected, used and shared via the application and how to decline such use or uninstall the application.

X. Third Party Services, Applications and Websites

A. Using NASTF products and services, you may be able to access third party services, applications and websites not controlled by NASTF or covered by this Privacy Policy, such as those belonging to Twilio (Authy), and automaker websites offered in conjunction with NASTF website links and the SDRM Registry program.
B. We recommend that you carefully review the Privacy Policy of other third-party services, applications and websites before providing any personal information.

XI. California Privacy Rights

1. If you are a California resident, the California Consumer Privacy Act (CCPA) provides you with specific rights regarding your personal information:
2. Right to Know/Access: You may request a list of the personal information we have collected about you since January 1, 2022.
3. Right to Delete: You may request that we delete your personal information, subject to certain exceptions (such as maintaining the integrity of the SDRM Registry or fulfilling legal obligations).
4. Right to Correct: You have the right to request that we correct inaccurate personal information that we maintain about you.
5. Right to Limit Sensitive Info: You may limit our use of "Sensitive Personal Information" (including precise geolocation and government IDs) to only those uses necessary to perform our security services.
6. Non-Discrimination: We will not deny you services or provide a different quality of service for exercising these rights.

2. How to Exercise These Rights: You may submit a request by emailing **nastf1@nastf.org** or via our support portal at **https://support.nastf.org/**. We will verify your identity before processing your request.

XII. Canadian Privacy Rights

A. For residents of Canada, your personal information is managed in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial laws (such as Quebec's Law 25).
   1. Right to Access & Rectification: You may request access to your personal information and ask for corrections to be made to any inaccurate or incomplete data.

2. Right to Withdraw Consent: You may withdraw your consent to our data collection at any time (e.g., opting out of cookies or marketing); however, please note that certain security services (SDRM) require specific data to function.
3. Data Portability: You have the right to receive a copy of your personal information in a structured, commonly used format.
4. International Transfers: NASTF is a U.S.-based organization. Your data is transmitted to, stored in, and accessed from the United States. While in the U.S., your data may be subject to the laws of that jurisdiction, including lawful access by U.S. government authorities.

B. How to Exercise These Rights: You may submit a request by emailing **nastf1@nastf.org** or via our support portal at **https://support.nastf.org/**. We will verify your identity before processing your request.