

Motor Vehicle Division Policy Memo # 19-08

Appropriate Use of DOT-Provided Internet

DATE: October 11, 2019

FROM: Melissa Spiegel, Director, Motor Vehicle Division

TO: All Motor Vehicle Division staff, Iowa County Treasurers and County Treasurers' staff that issue driver's licenses and non-operator's identification cards

SUBJECT

This policy memo explains our policy on conducting internet searches using Department of Transportation (DOT)-provided internet.

EXPLANATION

While the DOT already has a policies and procedures document (PPM 030.09) on appropriate use of the DOT's Internet resources, we are providing this policy memo to further communicate and document our policy regarding the appropriate and inappropriate use of DOT-provided internet resources as county treasurers will now have DOT-provided internet available on their driver's license issuance machines. We thought it would be helpful to develop one policy memo that applies to both Iowa DOT motor vehicle division staff and county treasurers that utilize DOT-provided internet to bring existing guidance on this topic under one umbrella.

DOT GUIDANCE

This policy memo adopts Section II, Use of the Internet, of DOT PPM 030.09 (attached at the end of this memo), which outlines what constitutes an appropriate or inappropriate use of DOT-provided internet. The following attachments related to DOT-provided internet resources may be found at the end of this memo:

- DOT PPM 030.09
- A sample 28E agreement with the county treasurers

HELPFUL QUESTIONS AND ANSWERS

The following questions and answers provide additional information that will be helpful to you and to customers.

WHAT GUIDELINES SHOULD WE FOLLOW TO DETERMINE WHAT IS AN APPROPRIATE OR INAPPROPRIATE USE OF DOT-PROVIDED INTERNET?

Section II, Use of the Internet, of DOT PPM 030.09 (attached at the end of this memo), outlines what constitutes an appropriate or inappropriate use of DOT-provided internet. There may be some provisions in the PPM that do not directly apply to county treasurer staff, such as accessing DOT public wifi, however, the applicable sections to your work should be fairly evident. Please familiarize yourself with this document and if in doubt about the applicability of this document to your work, or if you have any questions, please follow-up with your county liaison.

WHY ARE WE ISSUING A POLICY MEMO ADDRESSING APPROPRIATE USE OF DOT-PROVIDED INTERNET?

As part of the county connectivity project, the DOT is providing internet resources to county treasurers performing driver's license and non-operator identification card issuance, and while the DOT already has a policy and procedures document governing appropriate use of DOT-provided internet resources for DOT employees, there was no policy established for county treasurer staff use of DOT-provided internet.

DOES THE DIS 28E AGREEMENT WITH COUNTIES THAT ISSUE DRIVER'S LICENSES AND NONOPERATOR IDENTIFICATION CARDS ONLY APPLY TO THE COUNTY OFFICIAL THAT SIGNS THE AGREEMENT?

No. Although the county treasurer or chairman of the county board of supervisors may be the one signing the 28E agreement on behalf of the county, the requirements of the agreement apply to any county employee performing driver's license transactions. Section VIII(B) of the agreement states that "all equipment, hardware, software, forms, supplies, data line communications...materials and other propriety placed and provided by the department at the county's facilities...shall remain department property." This section means that any property or equipment provided by the DOT remains DOT property, and thus is subject to DOT use policies, including the policy on the appropriate use of DOT internet resources.

DOES THIS POLICY APPLY TO COUNTY TREASURERS THAT DON'T ISSUE DRIVER'S LICENSES AND NONOPERATOR IDENTIFICATION CARDS?

This policy applies to any county employee who uses DOT-provided Internet for any reason. County computers used solely for vehicle titling and registration and/or property tax transactions do not use DOT-supplied Internet and therefore users of those machines should follow Internet usage policies or procedures set forth by their county treasurer's office.

DOES THIS POLICY APPLY TO MOTOR VEHICLE DIVISION STAFF (I.E., NOT COUNTY TREASURERS)?

Yes. DOT employees have always been required to abide by the requirements in PPM 030.09.

WHAT HAPPENS IF I VIOLATE THE PROVISIONS OF DOT'S POLICY ON APPROPRIATE USE OF DOT INTERENT RESOURCES?

For DOT employees, your supervisor will follow existing investigation/disciplinary procedures in consultation with the Employee Services Bureau if a violation of this policy occurs, as outlined in PPM 030.09, Section IV, Misuse, Monitoring, and Filtering. For county treasurer's offices that issue driver's licenses and nonoperator identification cards, we may follow the procedures outlined in the 28E agreement regarding system access rights. For county treasurer's offices that do not have a 28E agreement, we will consider discontinuing access to any DOT-provided internet as an appropriate consequence for continued noncompliance with this policy.

Iowa DOT Policies and Procedures

Title Internet Services		Policy No. 030.09
Responsible Office Information Technology Division	Related Policies and Procedures 030.02, 230.09	
Effective/Revision Dates 5-21-1996/4-17-2018	Approval(s) <i>Annette M. Dunn</i>	

Authority: Director of the Information Technology Division (IT Division).

Contents: This policy establishes appropriate and inappropriate use of the DOT's Internet resources, both wired and wireless, including file uploads and downloads.

Affected Offices: All

Who to Contact for Policy Questions: Director of the IT Division, telephone 515-239-1284.

Definitions: None

Authorized Device – An authorized device is a DOT-issued desktop computer or portable device, such as a laptop or smartphone; or a non-DOT device, such as a personal device, the user of which has obtained the appropriate approvals as required by the IT Division and which has been loaded with DOT security and monitoring software, including, as necessary, Mobile Device Management for remote wiping of the device's data in the event of loss, theft, or other compromise.

Authorized Guests Only Wireless Network – The DOT guest wireless network is provided for DOT guests, such as vendors, contractors, and other professional contacts. The guest wireless network requires a user ID and password, which the guest must secure by providing a DOT contact to validate and approve the request. The DOT's guest wireless connections do not allow direct access to secured networking resources.

Iowa DOT Employees Only Wireless Network – This wireless network can be accessed only with authorized DOT employee LAN credentials (User ID and Password). Authorized devices will be allowed access to the data that the employee has access to on the DOT's secured networks. Nonauthorized devices (including personal devices) will be granted access only to the Internet.

Public Access Wireless Network – The DOT's public access wireless network is free and available for DOT customers and the public to use. It does not require a user ID or password, although it does require the user to agree to acceptable use terms before access is granted. **DOT employees in work status shall not connect to a DOT public access network because unnecessary overuse renders the network unavailable to the public.**

Forms: None

Policy and Procedure:

I. Internet Access

- A. By default, the IT Division shall ensure employees are provided with access to the Internet. Except as provided in this policy, employee access will be blocked by the IT Division for specific categories of sites that are deemed inappropriate for a work environment.
- B. Supervisors shall determine whether their employees will be blocked from Internet access or whether access to sites which are otherwise restricted, should be granted. A supervisor must complete a System Access request from the IT Division to block an employee's Internet access or to request access to restricted sites.

II. Use of the Internet

- A. The Internet is provided for business use for employees to accomplish their assigned job duties and responsibilities.
- B. Personal, or non-DOT business, access to the Internet through DOT infrastructure is limited as follows:

- 1. To the employee's lunch break or immediately before or after work when the employee is in a non-work status;
- 2. When the employee is authorized by the employee's supervisor to be at the work site.

Such personal access shall be consistent with all other requirements of this policy and other DOT policies.

- 3. During emergency situations (e.g., to determine if there is a school or business closure for severe weather or other emergency).
- 4. An exception for wireless use also applies: As explained in PPM 010.18, *Cellular Telephones and Smartphones*, a wireless exception to network connections reads as follows:
 - (1) This prohibition does not apply to DOT employees using personal devices to log into the "IADOT_Employees_Only" wireless network using their LAN credentials. The DOT's wireless connections allow unauthorized devices (such as personal devices) access only to the Internet.
 - (a) At DOT facilities that offer Wi-Fi access, an employee in work status shall secure supervisor approval to connect a personal device to "IADOT_Employees_Only" in order to access such services as streaming music. Employees should remain conscious of their use of DOT resources and understand they are limited. Connecting personal devices must never interfere with an employee's work duties.
 - (b) **Employees shall not access DOT Public Wi-Fi networks.** These are strictly for the public's convenience, and if employees use the service, the network would become overloaded and therefore unavailable to the public.

- C. The Internet, whether accessed through wired or wireless connections, or whether onsite or from a remote location, shall never be used:
1. For any unlawful purpose.
 2. To engage in or maintain a personal business or engage in personal business activities which includes but is not limited to the offering of services or merchandise for sale.
 3. Unless the use is assigned for a valid business reason, to send, request, search, display, view, print, download or otherwise disseminate material involving or relating to:
 - obscenity, pornography, profanity, libel, slander, fraud, defamation, forgery, plagiarism, harassment, discrimination, intimidation, impersonation; or
 - language which is malicious, false, inaccurate, sexually oriented, racially offensive, illegal, threatening, abusive, embarrassing; or involves solicitation for illegal pyramid schemes and computer tampering (e.g., spreading of computer viruses).
 4. To stream audio or video that is not work related, except as allowed in section II.B.4, above.
 5. To remote to any non-DOT unauthorized computers.
 6. To engage in partisan political activities of any nature.
 7. To intentionally seek information on, obtain copies of, reveal, publicize, or modify files or other data that are private, confidential, proprietary, or not open to public inspection or release unless specifically authorized to do so.
 8. To gamble, wager, bet or sell chances.
 9. To intentionally seek information on, obtain copies of, or modify files or data belonging to others without the authorization of the file owner.
 10. To intentionally develop programs designed to harass other users or infiltrate a computer or damage or alter its software components.
 11. To upload or download commercial software, mobile applications, or other materials unless specifically authorized to do so. In no case shall authorization be given to violate licenses, copyrights, or other state or federal laws regarding intellectual property or computer activities.
 12. To access or distribute computer games, except as allowed in section II.B.4, above..
- D. If an employee accesses an inappropriate site, even inadvertently, or receives or downloads materials, including but not limited to those specified in II.D.3. of this policy, the employee shall immediately report the incident to the employee's supervisor. The supervisor shall contact the DOT Service Desk.

III. Internet Support

The IT Division shall:

- A. Determine the hardware and software needed for Internet access and the transfer of information.
- B. Write necessary instructions for Internet access and data transfer or storage.
- C. Establish procedures to secure Internet services from tampering and/or unlawful access.
- D. Audit invoices received and ensure payment is made for all charges for data networks.

IV. Misuse, Monitoring and Filtering

- A. Internet activity occurring on DOT computers, networks, and accounts is monitored. DOT utilizes filtering software to limit access to sites on the Internet. If activities are discovered which do not comply with applicable law or policy, records retrieved may be used to document the wrongful content.
- B. Violators of this policy may be subject to disciplinary action up to and including discharge and to such criminal charges as may be appropriate. Allegations of misconduct will be investigated according to Policy No. 230.09, *Investigations*.

Any exceptions to this policy must be approved by the Director of the IT Division.

**AMEMORANDUM OF AGREEMENT BETWEEN THE IOWA DEPARTMENT OF TRANSPORTATION
AND ██████ COUNTY, IOWA**

This Agreement is made and entered into this ██████ day of ██████ 2017, by and between ██████ County, Iowa, ("the county") and the Iowa Department of Transportation ("the department").

RECITATIONS

WHEREAS, the county is authorized to issue driver's licenses, non-operator's identification cards, and persons with disabilities devices ("county issuance") on a permanent basis under section 321M.3 of the Iowa Code, and;

WHEREAS, the county wishes to exercise its authority to participate in county issuance, and;

WHEREAS, section 321M.5 of the Iowa Code requires the department and a county participating in county issuance to execute an agreement pursuant to Chapter 28E of the Iowa Code that details the relative responsibilities and liabilities of each party to the agreement;

NOW, THEREFORE, the county and department enter into the following agreement to facilitate county issuance by the county.

TERMS AND CONDITIONS

I. AUTHORITY

This agreement is entered into pursuant to the provisions of Iowa Code Chapters 28E and 321M.

II. DURATION

This agreement shall become effective upon filing with the Secretary of State of Iowa in accordance with Iowa Code § 28E.8 and shall remain valid until terminated as set forth herein.

III. PURPOSE

The purpose of this agreement is to establish the terms and conditions whereby the county will participate in county issuance under Chapter 321M of the Iowa Code.

IV. COUNTY TREASURER AS PROGRAM ADMINISTRATOR

The county's treasurer shall administer the county's issuance program and shall be responsible for performance of county issuance functions under this agreement.

V. SUPERVISORY AUTHORITY AND AGENCY RELATIONSHIP

Pursuant to Iowa Code § 321M.10, the department shall retain all supervisory authority over the county's issuance program. The county treasurer and the county treasurer's employees shall be considered agents of the department when performing county issuance functions pursuant to this agreement.

VI. AUTHORIZATION OF COUNTY TREASURER EMPLOYEES

- A. **County as employer.** The county treasurer shall employ at the county's expense and designate such employees as are necessary for performance of the county's issuance program, including the county treasurer if the county treasurer elects to perform such functions. Persons employed and designated for such purposes remain employees of the county and the department shall have no responsibility for their wages, taxes, benefits, or other employment rights or obligations. The county shall defend, indemnify, and hold harmless the department from any and all claims related to or arising out of any person's employment with the county, including any termination or discharge from employment. The county shall not use or allow any person not employed within the county treasurer's office to perform county issuance functions, except an employee of another county designated by that county to perform county issuance functions, and shared between the counties under an agreement between the counties.
- B. **Department approval.** The department shall have the right to approve the county employees that may perform county issuance functions, and the county treasurer shall not use or allow any county employee that has not been approved by the department to perform county issuance functions. The department's exercise of the right to approve county employees is not an exercise of employment rights or an employment decision but an exercise of program governance and control; all employment rights and decisions relative to any person employed or to be employed by the county remain the county's. When determining whether to approve a county employee to perform county issuance functions, the department shall adhere to the following procedures and standards:
1. **Background checks.** The county shall not use or allow any person to perform county issuance functions, and the department shall not approve any person to perform county issuance functions, unless the person has been subjected to and successfully passes the background check requirements of 6 C.F.R. § 37.45 and 49 C.F.R § 384.228. The county shall inform any employee or prospective employee subject to a background check that he or she is subject to the background check and the contents of the background check. The content of the required background checks is set forth in subparagraphs 2 and 3 below.
 2. **Verification of prior employment and employment eligibility.** The county shall conduct at its expense that part of the background check required by 6 C.F.R. § 37.45 that consists of verification of references from prior employment and employment eligibility verification, and shall provide proof of completion of such checks to the department before the department grants or denies approval for any county employee or prospective county employee.
 3. **Criminal history records check.**
 - i. The department shall conduct at its expense that portion of the background check that consists of a criminal history records check that meets the requirements of 6 C.F.R. § 37.45 and 49 C.F.R § 384.228.
 - ii. The county shall not use or allow to perform county issuance functions, and the department shall not approve to perform county issuance functions, any employee or person that has a disqualifying offense, crime, or conviction under 6 C.F.R. § 37.45 or 49 C.F.R § 384.228.

- iii. The department shall impose the same criteria for determining a disqualifying offense, crime, or conviction that the department imposes for persons employed by the department that are subject to the background checks. In the event the county employee or prospective county employee is determined to have a disqualifying offense, crime, or conviction, the department shall notify the county treasurer, who shall notify the county employee or prospective county employee.
 - iv. In the event the county treasurer has been designated to perform county issuance functions and is determined to have a disqualifying offense, crime, or conviction, the department shall notify the county treasurer and the chair of the county's board of supervisors.
 - v. The county treasurer shall immediately notify the department if a county employee that has successfully passed the required background checks has committed or is determined to have committed or incurred a disqualifying offense, crime, or conviction, and the department shall revoke the county employee's approval to perform county issuance functions and terminate the county employee's access to the department's issuance system. The department shall also revoke a county employee's approval to perform county issuance functions and terminate the county employee's access to the department's issuance system if the department independently learns or otherwise determines that the county employee has committed or is determined to have committed a disqualifying offense, crime or conviction.
- C. **Change of employment status or function.** In the event a county employee designated by the county treasurer for any reason ceases to be employed by the county or is otherwise assigned to another position or functions and responsibilities and will no longer perform county issuance functions, the county treasurer shall immediately notify the department that the county employee is no longer employed and/or designated to perform county issuance functions, and the department shall withdraw the county employee's approval and terminate the county employee's access to the department's issuance system.

VII. FACILITIES AND FURNISHINGS

- A. **County to provide.** The county shall provide at the county's expense all facilities and furnishings necessary for performance of the county's issuance program. The department shall have no responsibility to provide facilities or furnishings to the county and shall have no responsibility for any expense, cost, or liability related to or arising out of the county's facilities or furnishings, including but not limited to rent or utilities. The county shall defend, indemnify, and hold harmless the department from any and all claims related to or arising out of operation, maintenance, or provision of the county's facilities or furnishings.
- B. **Access by department.** The county shall grant department employees, vendors, and contractors reasonable access to the county's facilities during the county's regular business hours for the purpose of guiding and auditing the county's issuance program and providing, installing,

maintaining, replacing, inspecting, or otherwise servicing the issuance equipment, hardware, software, systems, data or networks lines, and materials provided by the department to the county for performance of the county's issuance program, and at all other times agreed upon by the county and department or as reasonably necessary to protect said items in the event of any breach in or damage to the county's facilities or security safeguards.

VIII. ISSUANCE EQUIPMENT, HARDWARE, SOFTWARE, SYSTEMS AND MATERIALS

- A. **Duty to provide.** The department shall provide from funds allocated to the department for the purpose of supporting county issuance all equipment required to be provided by the department under section 321M.9, subsections 2 and 3 of the Iowa Code, including all issuance and testing equipment, hardware, software, data line communications, forms, supplies and materials determined by the department as necessary for conduct of the county's issuance program. The department shall not provide and shall not be responsible for other equipment specifically excepted under section 321M.9, subsection 3. The parties acknowledge that permanent driver's licenses, non-operator's identification cards, and other cards that may be issued as part of the county's issuance program are produced at a secure third-party facility, and that the department is solely responsible for the production and mailing of permanent cards through the department's card production vendor and through funds allocated to the department for that purpose.
- B. **Property rights.** All equipment, hardware, software, forms, supplies, data line communications, forms, supplies, materials and other property placed and provided by the department at the county's facilities under this agreement shall remain department property. The department may assign and reassign or replace property as it deems appropriate. In the event this agreement is terminated, property placed and provided by the department shall be returned to the department unless the parties otherwise mutually agree. The department shall bear the cost of removing said property, but shall not be responsible for returning the county's facilities to any prior condition.

IX. TRAINING, EDUCATION AND RESOURCES

- A. **Department to provide.** The department shall provide all training, continuing education, and resource materials (manuals, technical guidance, policies, memos and other resources intended to guide activities covered by this agreement, whether in written or electronic format) determined by the department as necessary for the proper implementation and performance of the county's issuance program, at times and places determined by the department. Training, continuing education, and resource materials shall be entirely consistent with and integrated wherever possible with the training, continuing education, and resource materials provided for department employees.
- B. **Costs and expenses covered by the department.** The department shall provide all resource materials at the department's cost, and shall cover the travel expenses for county employees that are required to travel to attend training, continuing education, or conferences required by the department from funds allocated to the department for the purpose of supporting county issuance. As used in this paragraph, travel expenses shall include reasonable mileage, meals, and lodging expenses, all of which shall be subject to and paid at the rates and according to the conditions and limitations set forth in the department's policy for department employees, "Personal Expense

Reimbursement and Travel," department policy no 120.02, as published and updated by the department on the department's intranet site. All such training, continuing education, or conferences shall be within the state of Iowa; the department shall neither require nor be responsible for out-of-state travel or associated costs or expenses for county employees.

- C. **County adherence to training and continuing education.** The county shall require all county employees designated to perform issuance functions to complete all training and continuing education required by the department, and where such training or continuing education is required as a condition to perform or to continue to perform a task or activity within the issuance program, shall not permit a county employee to perform or to continue to perform that task or activity until the employee has successfully completed the required training or continuing education. The department may withdraw the county employee's approval to participate in the county's issuance program and terminate the county employee's access to the department's issuance system if the employee fails to successfully complete required training and continuing education.
- D. **Training and continuing education content.** Training and continuing education subject to this division shall encompass all topics and content determined by the department to be reasonable and necessary for the proper, effective and well-governed administration of the state and county issuance programs, as well as all training or education currently required or to be required by state or federal law or regulations, including but not limited to the federal REAL ID regulations established at 6 C.F.R. part 37 and the federal commercial driver's license regulations established at 49 C.F.R. parts 383 and 384.
- E. **Certification of examiners.** For purposes of this division, an examiner is a county employee designated by the county to administer or initiate commercial driver's license knowledge tests or to perform commercial, noncommercial, or motorcycle skills (driving or operation) tests. A county employee designated for such purposes shall not perform such tasks unless the employee has and properly maintains the proper certification to do so, as set forth in the following:
 - 1. **Commercial driver's license knowledge test examiner.** The county employee must successfully complete all training, refresher training, and examination required for certification as a knowledge test examiner under 49 C.F.R. § 384.228.
 - 2. **Commercial driver's license skills test examiner.** The county employee must successfully complete all training, refresher training, and examination required for certification as a skills test examiner under 49 C.F.R. § 384.228.
 - 3. **Non-commercial driver's license skills test examiner.** The county employee must successfully complete all training, refresher training, and examination required for certification as a driver examiner under the International Driver Examiner Certification program established by the American Association of Motor Vehicle Administrators.
 - 4. **Motorcycle skills test examiner.** The county employee must successfully complete all training, refresher training, and examination required for certification as a motorcycle examiner in accordance with the standards of the Motorcycle Safety Foundation as adopted by the department.

All county employees designated as participants in the county issuance program are considered commercial driver's license knowledge test examiners and must attain and maintain such

certification. The county may determine which employees it may designate as commercial or noncommercial driver's license skills test examiners or motorcycle skills test examiners. All county commercial driver's license knowledge or skills test examiners as agents of the department are considered state examiners and not third-party examiners for purposes of 49 C.F.R. §§ 383.75, 384.228, and 384.229, and are subject to the requirements set forth therein for state examiners, including but not limited to the auditing and monitoring requirements of 49 C.F.R. § 384.229. Nothing in this division requires the county to offer commercial driver's license skills test exams or motorcycle skills test exams or to designate county employees to perform such services.

X. PROTECTION OF PERSONAL INFORMATION

- A. **Duty to protect personal information.** The county and its employees shall only access and use personal information regarding a driver's license or non-operator's identification card holder or applicant or otherwise contained in a department data-base or record in the course of the county's official functions, and shall not access or use such information for any other reason or purpose, personal or otherwise. Any release, disclosure or re-disclosure of such personal information must comply with the requirements Iowa Code § 321.11 and the federal Driver's Privacy Protection Act, 18 U.S.C. § 2721 et seq ("the DPPA). Personal information as used in this agreement means as defined in Iowa Code § 321.11(2).
- B. **Duty to report.** The county shall immediately report to the department any actual or suspected access, use, release, disclosure, or re-disclosure of personal information that is not permitted under Iowa Code § 321.11 or the DPPA, whether intentional or unintentional.
- C. **Duty to cooperate.** The county shall fully cooperate with the department to investigate and mitigate any actual or suspected access, use, release, disclosure, or re-disclosure of personal information that is not permitted under Iowa Code § 321.11 or the DPPA, and shall grant the department all access to the county's facilities and employees reasonably necessary to complete the investigation and fully mitigate the incident, including but not limited to securing personal information, recovering personal information, and protecting against further access, use, release, disclosure, or re-disclosure of personal information that is not permitted under Iowa Code § 321.11 or the DPPA.
- D. **Termination of authority and denial of approval or access.** The department reserves the right to:
 - 1. Terminate authorization of the county's issuance program should the county fail to protect personal information as required by this division;
 - 2. Withdraw approval to participate in the county's issuance program and terminate access to the department's issuance system for any county employee that engages in or permits access, use, release, disclosure, or re-disclosure of personal information that is not permitted under Iowa Code § 321.11 or the DPPA.

XI. SECURITY

- A. **County safeguards.** The county shall establish, provide, and maintain reasonable administrative, technical, and physical safeguards to protect the security of the county's facilities dedicated to performance of the county's issuance program and to protect the security, confidentiality, and

integrity of the issuance equipment, hardware, software, systems, data or network lines, and materials housed, stored, or accessed in or at the county's facilities and any personal information collected, stored, accessed, or maintained in the course of performance of the county's issuance program, and agrees to comply with any security policies or protocols established by the department and made known to the county. The county's safeguards shall, at a minimum, be sufficient to comply with the department's security plan established under the federal REAL ID regulations, 6 C.F.R. § 37.41.

- B. Protection against unauthorized access.** In no event shall the county allow any person not authorized by the department to access or use the issuance equipment, hardware, software, systems, data or network lines, and materials housed, stored, or accessed in or at the county's facilities or any personal information collected, stored, accessed, or maintained in the course of performance of the county's issuance program, nor shall the county allow or require county employees to share, disclose, or otherwise disseminate the individual user names and passwords provided by the department to the county employee for the county employee's access to the department's systems, records and data.
- C. Duty to report.** The county shall immediately report to the department:
1. Any actual or suspected breach in or damage to its facilities or the security safeguards employed by the county that would threaten the security, confidentiality or integrity of the issuance equipment, hardware, software, systems, data or network lines, and materials housed, stored, or accessed in or at the county's facilities or any personal information collected, stored, accessed, or maintained in the course of performance of the county's issuance program.
 2. Any actual or suspected unauthorized access to or use of the issuance equipment, hardware, software, systems, data or network lines, and materials housed, stored, or accessed in or at the county's facilities or any personal information collected, stored, accessed, or maintained in the course of performance of the county's issuance program.
 3. Any actual or suspected misappropriation or theft of the issuance equipment, hardware, software, systems, data or network lines, and materials housed, stored, or accessed in or at the county's facilities or any personal information collected, stored, accessed, or maintained in the course of performance of the county's issuance program.
 4. Any other act or occurrence that would reasonably be suspected to impair the security, confidentiality or integrity of the issuance equipment, hardware, software, systems, data or network lines, and materials housed, stored, or accessed in or at the county's facilities or any personal information collected, stored, accessed, or maintained in the course of performance of the county's issuance program.
- D. Duty to cooperate.** The county shall fully cooperate with the department to investigate and mitigate any actual or suspected breach, unauthorized access or use, or theft or misappropriation and shall grant the department all access to the county's facilities and employees reasonably necessary to complete the investigation and fully mitigate the incident, including but not limited to securing, recovering, and protecting against further breach, unauthorized access or use, or theft or misappropriation of the issuance equipment, hardware, software, systems, data or network lines, and materials housed, stored, or accessed in or at the county's facilities or any personal information

collected, stored, accessed, or maintained in the course of performance of the county's issuance program. This includes any acts necessary to protect and recover such items in the event of damage to the county's facilities, whether intentional or unintentional and whether natural or man-made.

- E. **Termination of authorization and denial of approval or access.** The department reserves the right to:
1. Refuse and prohibit the conduct of issuance activities at any county facility that is not reasonably secured as required in this division;
 2. Terminate authorization of the county's issuance program should the county fail to establish, provide, and maintain reasonable safeguards as required by this division;
 3. Withdraw approval to participate in the county's issuance program and terminate access to the department's issuance system for any county employee that engages in or permits a breach, unauthorized access or use, or theft or misappropriation of the issuance equipment, hardware, software, systems, data or network lines, and materials housed, stored, or accessed in or at the county's facilities or any personal information collected, stored, accessed, or maintained in the course of performance of the county's issuance program.

XII. PERFORMANCE OF SERVICES

- A. **General.** The county shall perform all services within the county issuance program consistently with and according to the requirements of all state and federal laws and regulations, including the regulations of the department and all policies and procedures established by the department and made known to the county.
- B. **Service not limited to county residents.** The county shall serve all Iowa residents that present for services, without regard to whether the person is a resident of the county.
- C. **Commercial driver's license services.** The county's issuance of commercial driver's licenses shall be subject to the requirements of sections 321M.6. The department shall certify the county's issuance of commercial driver's licenses by separate letter to the county, which shall document whether the county offers commercial driver's license skills tests and the terms and conditions under which the county may do so. Nothing in this paragraph or this agreement shall require the county to offer commercial driver's license skills tests.
- D. **Acknowledgment of general obligations under anti-discrimination laws.** The county acknowledges that the county's issuance program is subject to Title VI of the federal Civil Right Acts of 1964, 42 U.S.C. 2000d – 2000d-7 (Title VI), and to Iowa Code § 216.7. These laws create the following obligations:
1. **Title VI.** Under Title VI, no person in the United States shall, on the ground of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under the county's issuance program.
 2. **Iowa Code § 216.7.** Under Iowa Code § 216.7, it is an unfair or discriminatory practice for a public accommodation to:
 - i. Refuse or deny to any person because of race, creed, color, sex, sexual orientation, gender identity, national origin, religion, or disability the accommodations, advantages, facilities, services, or privileges thereof, or otherwise to discriminate

against any person because of race, creed, color, sex, sexual orientation, gender identity, national origin, religion, or disability in the furnishing of such accommodations, advantages, facilities, services, or privileges.

- ii. Directly or indirectly advertise or in any other manner indicate or publicize that the patronage of persons of any particular race, creed, color, sex, sexual orientation, gender identity, national origin, religion, or disability is unwelcome, objectionable, not acceptable, or not solicited.

The county agrees that it will operate and offer access to its facilities and performs its issuance program in conformance with these obligations.

- E. **Acknowledgment of specific obligations under anti-discrimination laws.** The county further acknowledges that its obligations under the anti-discrimination laws set forth in the preceding paragraph "C" specifically include but are not limited to the following obligations, and agrees to operate and offer access to its facilities and perform its issuance program in conformance with these specific obligations:

1. **Service to foreign nationals.** The county shall not deny or refuse to perform services to a person on the basis that the person is a temporary or permanent foreign national, and will not refuse to issue credentials intended for such persons. As used herein a foreign national is a person who is not a U.S. citizen but can properly demonstrate lawful presence in the U.S.
2. **Service to persons of limited English proficiency.** The county shall not deny or refuse to perform services on the basis that the person is of limited English proficiency, and in conjunction with the department shall provide reasonable translation and interpretation services as needed to facilitate services to persons of limited English proficiency.

XII. FEES

- A. **Consideration.** The county's sole consideration for services performed under this agreement shall be retention of fees as set forth in Iowa Code § 321M.9(1).
- B. **Daily remittance of fees and penalties collected.** The county shall remit daily to the state treasurer all fees and civil penalties collected in the performance of the county's issuance program under chapter 321M.
- C. **Monthly reconciliation of fees retained.** The fees retained by the county under Iowa Code § 321M.9(1) shall be deducted from the moneys collected under chapter 321 and otherwise transferred to the state treasurer on the 10th of each month, pursuant to Iowa Code §§ 321.152 and 321.153, and shall be reported to the department in conjunction with other fees retained by the county, as provided in Iowa Code § 321.152.
- D. **Daily and monthly reporting and reconciliation procedures.** The department shall provide procedures for daily and monthly reporting and reconciliation of fees and penalties transferred and retained to assure accurate accounting of all penalties and fees collected, transferred, and retained.

XIII. TERMINATION

- A. **Termination by the county.** The county may terminate this agreement with 30 days' notice to the department.
- B. **Termination by mutual agreement.** The county and department may terminate this agreement upon mutual written agreement at any time, with or without notice.
- C. **Termination for cause.** Pursuant to Iowa Code § 321M.4, the department may terminate the county's authorization to conduct the county issuance program if the county fails to meet the department's standards for issuance. Termination for cause may occur under any of the following circumstances:
 - a. The county fails to comply with or satisfy any of the provisions of this agreement.
 - b. The county fails to comply with the department's policies and procedures for performance of the county's issuance program.
 - c. The county fails to comply with any state or federal law or regulation that applies to performance of the county's issuance program.
 - d. The county commits an act or omission that comprises the integrity of the state's issuance program or threatens the integrity or security of the state's systems, hardware, software, networks, or databases.
 - e. The county commits an act or omission that warrants termination of the county's authorization under the specific terms of any other division of this agreement.
 - f. The county falsifies any record or information provided or used in the performance of the county's issuance program or fraudulently approves a credential, benefit, permission or privilege for which a person is not legally entitled or due.
 - g. The county misappropriates or otherwise fails to properly account for fees collected under this agreement and chapter 321M, or fraudulently assesses any person a fee or penalty that is not legally due.

As used in this paragraph, "county" includes the county, its officers, agents and employees. In lieu of terminating the county's authorization, the department in its discretion may withdraw approval to participate in the county's issuance program and terminate access to the department's issuance system for any county officer, agent, or employee that commits an act or omission that would warrant termination of the county's authorization.

- D. **Notice for termination with cause.** The department will exercise good faith efforts to resolve performance issues and issues of noncompliance informally and without the need for termination of authorization for cause and formal notice. However, where the performance issues are serious or ongoing and have not been resolved informally or are not amenable to being resolved informally, the department will give the county formal written notice of intent to terminate authorization that details the performance or compliance deficiencies that have been found and the measures the county must take to remedy the deficiencies. The written notice shall give the county a reasonable period of time to remedy the deficiencies before termination of authorization becomes effective, which shall be at least thirty days. Anything in this paragraph notwithstanding, however, the

department reserves the right to immediately terminate authorization where the deficiency poses an imminent threat to the integrity or security of the state's systems, hardware, software, networks, or databases or will or may result in the unauthorized release, disclosure, or exposure of personal information contained in the department's records or databases.

- E. **Duty upon termination.** Upon termination the county shall not conduct any activity within the county issuance program until the department reauthorizes the department to do so. However, the county shall retain and protect all program records and records and property of the department and shall grant the department, its employees, vendors, and contractors reasonable access to protect and recover said records and property.
- F. **Reauthorization.** Upon correction of any deficiencies the county may apply in writing for reauthorization of the county's issuance program. The department will not grant reauthorization until the deficiencies have been corrected to the department's satisfaction. The department shall not unreasonably withhold reauthorization.

XIV. LEGAL ENTITY

No new legal or administrative entity is created by this agreement.

XV. ASSIGNABILITY

The rights and interests of the parties to this agreement are not assignable.

XVI. PRIOR AGREEMENTS

This agreement replaces and supersedes all prior agreements between the county and the department under chapter 321M.

IN WITNESS WHEREOF, the department and the county have caused this agreement to be executed in two counterparts, each of which shall be considered an original.

IOWA DEPARTMENT OF TRANSPORTATION

 IOWA