IOWA DOT
SMARTER | SIMPLER | CUSTOMER DRIVEN
www.iowadot.gov

Motor Vehicle Division Policy Memo # 18-09

Prohibition Against Sharing DOT System User IDs and Passwords

DATE: December 6, 2018
FROM: Melissa Spiegel, Director, Motor Vehicle Division
TO: All Motor Vehicle Division staff, Iowa County Treasurers and County Treasurers' staff

SUBJECT

This policy memo explains our policy on the protection of and prohibition against sharing Department of Transportation (DOT) user IDs and passwords.

EXPLANATION

While the department has issued a policies and procedures document (PPM 030.02) related to computer resources and Driver & Identification Services (DIS) has entered into 28E agreements with section XI(B) of the agreement addressing the prohibition against sharing DOT system user IDs and passwords, we are providing this policy memo to further communicate and document our policy that sharing DOT system user IDs and passwords is prohibited. We thought it would be helpful to develop one policy memo that applies to both motor vehicle division staff and county treasurers, that will bring existing guidance on this topic under one umbrella.

DOT GUIDANCE

The following four attachments related to DOT system user IDs and passwords may be found at the end of this memo:

- Iowa Code section 321.31
- DOT PPM 030.02
- A sample 28E agreement with the county treasurers
- The power point provided to all new county treasurer staff

HELPFUL QUESTIONS AND ANSWERS

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

WHY ARE WE ISSUING A POLICY MEMO PROHIBITING SHARING OF DOT USER IDs AND PASSWORDS?

On May 31, 2017, the Iowa Auditor of State issued a finding to the DOT related to use of the ARTS system by DOT staff and County Treasurers' Offices. The finding states that in two of the three counties visited by the auditor, staff shared their DOT user ID and password and in one county, all staff used the same password. This allowed staff to process transactions under user IDs that were not their own. We want to take the opportunity to remind all staff who access DOT systems, including ARTS, of their responsibility not to share their user ID or password and of the consequences that may be implemented for not adhering to this important policy.

DOES THE DIS 28E AGREEMENT WITH COUNTIES THAT ISSUE DRIVER'S LICENSES AND NONOPERATOR ID 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 XI(B) of the agreement states that the county "shall not allow or require county employees to share, disclose, or otherwise disseminate their 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." This section means that each county staff person is required to perform work under their own user ID and password, and is prohibited from sharing their DOT system user ID and password.

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

Yes. Although we do not enter into a 28E agreement with county treasurers who do not perform driver's license and nonoperator ID card functions, all county treasurers access ARTS to perform vehicle registration and title transactions, and are therefore bound by the prohibition against sharing DOT system user IDs and passwords.

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

Yes. DOT staff must abide by the prohibition against sharing DOT system user ID and passwords.

IS THERE ANY SITUATION IN WHICH IT MIGHT BE APPROPRIATE TO SHARE MY DOT USER ID AND/OR PASSWORD?

There are rare times when sharing your DOT system user ID and password may be appropriate, such as setting up a new computer or trouble-shooting your system access. However, most of these occurrences will involve DOT IT staff who will guide this process. After resolution of the issue, you are required to change your password to ensure you are adhering to the above-referenced policies. Please keep in mind that sharing a DOT system user ID or password for an everyday system transaction is not appropriate.

IS THERE ANY TRAINING MATERIAL STATING THAT I SHOULDN'T BE SHARING MY DOT USER ID AND PASSWORD?

Yes. As mentioned above, for DOT employees, there is the DOT PPM 030.02, and all new county staff receive the power point training included at the end of this memo.

WHAT HAPPENS IF I CONTINUE TO SHARE MY DOT USER ID AND PASSWORD?

For DOT employees, your supervisor will follow existing investigation/disciplinary procedures. For county treasurer's offices that issue driver's licenses and nonoperator ID cards, we will follow the procedures outlined in the 28E agreement. For county treasurer's offices that do not have a 28E agreement, we will consider discontinuing an individual's access to ARTS as an appropriate consequence for continued noncompliance with this policy.

321.31 Records system.

A state and county records system shall be maintained in the following manner:

1. *State records system.*

a. The department shall install and maintain a records system which shall contain the name and address of the vehicle owner, current and previous registration number, vehicle identification number, make, model, style, date of purchase, registration certificate number, maximum gross weight, weight, list price or value of the vehicle as fixed by the department, fees paid and date of payment. The records system shall also contain a record of the certificate of title including such information as the department deems necessary. The information to be kept in the records system shall be entered within forty-eight hours after receipt insofar as is practical. The records system shall constitute the permanent record of ownership of each vehicle titled under the laws of this state.

b. The department may make photostatic, microfilm, or other photographic copies of certificates of title, registration receipts, or other records, reports or documents which are required to be retained by the department. When copies have been made, the department may destroy the original records in such manner as prescribed by the director. The photostatic, microfilm, or other photographic copies, when no longer of use, may be destroyed in the manner prescribed by the director, subject to the approval of the state records commission. Photostatic, microfilm, or other photographic copies of records shall be admissible in evidence when duly certified and authenticated by the officer having custody and control of the copies of records. Records of vehicle certificates of title may be destroyed seven years after the date of issue.

c. The director shall maintain a records system of delinquent accounts owed to the state using information provided through the computerized data bank established in section 421.17. The department and county treasurers shall use the information maintained in the records system to determine if applicants for renewal of registration have delinquent accounts, charges, fees, loans, taxes, or other indebtedness owed to or being collected by the state as provided pursuant to section 8A.504. The director, the director of the department of administrative services, and the director of revenue shall establish procedures for updating the delinquent accounts records to add and remove accounts, as applicable.

2. *County records system.*

a. Each county treasurer's office shall maintain a county records system for vehicle registration and certificate of title documents. The records system shall consist of information from the certificate of title, including the date of perfection and cancellation of security interests, and information from the registration receipt. The information shall be maintained in a manner approved by the department.

b. Records of vehicle certificates of title for vehicles that are delinquent for five or more consecutive years may be destroyed by the county treasurer. Automated files, optical disks, microfiche records, and photostatic, microfilm or other photographic copies of records shall be admissible in evidence when duly certified and authenticated by the officer having custody and control of the records.

[S13, §1571-m2; C24, 27, 31, 35, §5010; C39, §**5001.15;** C46, 50, 54, 58, 62, 66, 71, 73, 75, 77, 79, 81, §321.31]

89 Acts, ch 185, §2; 95 Acts, ch 194, §3, 12; 2003 Acts, ch 145, §246; 2004 Acts, ch 1013, §6, 35; 2010 Acts, ch 1061, §180

Referred to in **§331.557**

Form 103050 wd07
11-09

Iowa DOT Policies and Procedures

Title	Policy No.
Computer Resources	**030.02**
Responsible Office: Information Technology Division	Related Policies and Procedures: 010.01, 010.02, 010.11, 030.06, 030.09, 030.11, 030.12, 030.13
Effective/Revision Dates: 10-01-2002/4-17-2018	Approval(s): *Annette M. Dunn*

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

Contents: This policy describes the procedures for request to purchase, acceptable use, support and disposal of computer resources.

Table of Contents:

Affected Offices: All

Who to Contact for Policy Questions: IT Division, 515-239-1284.

Definitions:

Computer Resources – All DOT computer equipment, including desktop, laptop, notebook, tablet, or any other fixed or portable device that is used for the purpose of processing data or interfacing with other devices via DOT networks. For the purposes of this policy, computer resources do not include smartphones (see *Cellular Telephones and Smartphones*, PPM 010.18).

Confidential – See the definition in Policy No. 030.06, *Records Management and Access to Records*.

Data – Documents, spreadsheets, databases, PowerPoint presentations, audio files, email messages, images, videos, etc., anything that can be created on, stored on, or transmitted by computer resources.

Information Technology Resources– Computer resources, computing systems, networks, telephony (including landlines, cellphones, smartphones, and radios), data and databases, physical facilities, infrastructure, software, hardware, computer programs and languages, procedures, processes and documentation used for inputting, outputting, securing, processing, transmitting, storing, displaying, retrieving, scanning and printing of information stored in an electronic format.

IP Plan – Information Processing Plan. See PPM 030.01, *Information Technology Processing,* for complete description of the IP Plan.

Mobile Application (Mobile App or, more commonly, App) – A category of software (see definition below) that is designed and optimized for use in mobile computing devices.

Peripherals – Refers to printers, monitors, scanners, external modems, disk drives, or any other devices permanently or semi-permanently attached to computer resources. Peripherals do not include removable media such as thumb drives, cameras or smartphones. For more information about removable media, see PPM 030.13, *Removable Media and Encryption of Data.*

Personally identifiable information – For the purposes of this policy, see the definition in Policy No. 030.06, *Records Management and Access to Records*.

Software – A set of instructions used by a computer to perform specified tasks.

Support Team – IT Division staff, under direct supervision of an IT Division manager(s), who have been assigned the responsibility to provide computer resources or programming activities in support of another division as specified by the director of that division.

Forms: None

Policy and Procedure:

I. Requests to Purchase Computer Resources

A. Tablet Computers: A request for a tablet computer must be submitted through the Service Request System. The Service Request must be approved by the employee's supervisor, office director/district engineer and division director.

B. For all other computer resource purchases, see Policy No. 010.01, *Equipment Procurement*.

II. Acceptable Use of Computer Resources

A. General guidelines for acceptable use of computer resources include the following:

1. Employees must:

a. Access and use information technology only for authorized purposes and in accordance with the DOT's Policies and Procedures.

b. Protect their userids and accounts from unauthorized use.

c. Protect confidential and personally identifiable information from unauthorized access by locking or otherwise securing computer resources whenever employees are away from their devices. To assist employees in maintaining IT resources security, computer resources connected to the DOT's network will lock after 15

minutes of inactivity. Additionally, all employees who use mobile devices must make sure they are configured to automatically deactivate (time out) after a maximum of 15 minutes of inactivity even when not connected to the DOT's network, at which time a four-or-more character password is required to reactivate the device. For more information about mobile device security, see PPM 030.13, *Removable Media and Encryption of Data,* and PPM 030.12, *Laptop Encryption.*

d. Access only files and data that they are authorized to access or are publicly available.

e. Use only legal versions of copyrighted software in compliance with vendor license requirements.

f. Allow IT Division support teams access to computer resources to install software, monitor inappropriate activity, diagnose problems and retrieve inventory information.

2. Employees must NOT:

a. Use another person's computer resource, files or data without permission.

b. Use another person's individual userid and password for any reason other than official DOT business without obtaining prior authorization.

Users must change their password immediately after completion of the work allowing another person to use it to access the employee's account.

c. Use computer programs to decode passwords or modify control information.

d. Attempt to circumvent or subvert security measures, including by not participating in required DOT information security training initiatives.

e. Engage in any activity that might be harmful to systems or to any information stored on them such as creating or propagating viruses, disrupting services, or damaging files.

f. Use the DOT's information technology for commercial or political purposes, such as using e-mail to circulate advertising for products or for political candidates.

g. Make, use or store illegal copies of copyrighted software.

h. Use the DOT's information technology resources for games, or non-business chatter in the form of jokes, chain letters, or the routing of large non-business attachments, such as video and audio files.

i. Use e-mail or messaging services to harass, intimidate or annoy another person. However, this does not include unsolicited business-related messages or e-mail, such as retirement or catastrophic leave announcements.

j. Waste computing or network resources. Examples include intentionally placing a program in an endless loop, by allowing real-time update of data via constant

connection to an external site, or by allowing downloading of media for non-business usage.

k. Create security breach or system vulnerability by acting as an unauthorized gateway for external access.

l. Use the DOT's information technology resources for personal gain or engage in any other activity that does not comply with the general guidelines presented above in section II.A.1.

B. Employees in work status shall only use their computer resources for DOT business.

C. The computer resource may be used for personal use provided:

1. The use is limited to non-worktime, which is defined as before or after work and during lunch breaks.

   An exception to this provision applies in the event of a weather or other emergency, at which time usage must be restricted to responding to or monitoring the emergency.

2. The use is incidental and there is no additional, easily quantifiable cost to the DOT.

3. The use is consistent with all other requirements of this policy.

D. Employees are responsible for the safety of their computer resources and data.

E. Portable equipment shall not be left in an unsecured location under any circumstances or checked as baggage when flying on commercial airliners unless required by law or airline policy. See section VIII of this policy for International travel.

F. The DOT reserves the right to monitor, copy and examine any files, network traffic, information technology usage or information resident on any system used to conduct the DOT business. If the DOT believes illegal or improper behavior is taking place, or if a user's actions are affecting the integrity or the reliability of the DOT's services, the DOT reserves the right to suspend services and/or access privileges until the user has been notified and the DOT has conducted an investigation.

III. Use of Software

A. The DOT secures licenses for the use of computer resource software from a variety of vendors. The DOT may not, unless authorized by the software vendor, reproduce or copy any licensed software or documentation either electronically or manually.

B. Software use must be in compliance with the license agreement.

C. The division directors or designees shall approve all software used on computer resources within their division. The IT Division shall coordinate with the division directors or designees to establish, as much as is practicable, a DOT-wide standard to warrant and approve the installation of each authorized software package. Installation standards shall be followed by support team staff. The IT Division shall remove any unauthorized software found on a DOT computer resource.

D. The support team shall install all software. An exception would be free mobile applications for mobile computing devices that aid an employee in his or her work. Contact the Service Desk at 515-239-1075 with questions or requests.

E. The following actions are prohibited:

1. Duplication of licensed software, except as permitted by the license agreement, is a violation of the federal Copyright Act.

   Under the federal Copyright Act, anyone involved in the misuse of copyrighted material, such as the illegal reproduction of software or documentation, may be subject to civil damages and criminal penalties including fines and imprisonment.

2. Employees shall not copy, alter or remove licensed software without the permission of the IT Division.

3. Employees shall not install software licensed by the DOT on the employee's personal home computer or any other computer unless specifically authorized by the DOT.

F. Pursuant to Iowa Code subsection 721.2(5), it is a serious misdemeanor to use state property for private purposes or personal gain. Software developed by DOT employees is the property of the DOT. Employees shall not provide DOT-owned software or copies to persons outside the DOT without specific authorization from the IT Division Director.

IV. Data Availability

A. It is the responsibility of the employee to store critical DOT data on appropriate networked storage devices. Networked storage is available to multiple users and is routinely backed up by the IT Division. Local drives such as desktops, laptops, or mobile devices available only to single users, are not backed up by the IT Division.

B. If non-critical data is stored on a computer resource, it is the employee's responsibility to create a backup copy of the non-critical data.

C. It is the employee's responsibility to copy non-critical data from the computer resource to another media when the support team is going to replace the resource. The employee may copy the non-critical data from the media back onto the resource after installation.

V. Installation, Support, and Disposal of Computer Resources

A. The IT Division shall install and support all computer resources. The IT Division shall approve all peripheral equipment.

1. Only DOT equipment shall be attached to the DOT's networks, unless authorized by the IT Division. As explained in PPM 010.18, *Cellular Telephones and Smartphones,* a wireless exception to network connections exists:

   Wireless Exceptions: 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 do not allow unauthorized

devices (such as personal devices) access to secured networking resources. When an unauthorized device connects to "IADOT_Employees_Only," it is granted access only to the Internet.

At DOT facilities that offer Wi-Fi access, an employee in work status shall secure supervisor approval to connect a personal device to the "IADOT_Employees_Only" network. Connecting personal devices must never interfere with an employee's work duties.

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.

2. Employees who believe they have a justifiable business need for connection of non-DOT devices to secured DOT networks shall first discuss the need with their supervisor and then contact the Service Desk, 515-239-1075, for instructions.

B. Computer resources that are replaced shall be turned into the support team for reassignment or disposal. The resource shall be prepared for disposal in accordance with Policy No. 010.02, *Equipment Transfers.*

C. Used computer resources may be reinstalled if it is deemed usable by the receiving cost center. It shall be the responsibility of the IT Division to reinstall the resource.

VI. Broken/Malfunctioning Equipment

A. The employee shall report equipment problems to the Service Desk: 515-239-1075. The Service Desk shall document all equipment problems.

B. In the event of equipment failure, the IT Division shall verify the condition of the equipment and recommend, based on cost, age and use, whether to have it repaired or replaced.

1. If the equipment is repaired based on the IT Division recommendation, the IT Division shall contact the vendor and pay for the repairs.

2. If it is mutually agreed between the IT Division and the cost center owner the equipment should be replaced, the replacement equipment shall be submitted as an IP plan amendment and purchased in accordance with Policy No. 010.01, "*Equipment Procurement."*

VII. Lost or Stolen Equipment

If a computer resource is lost or stolen, specific procedures must be followed. See Policy No. 010.11, "*Equipment—Security, Inventory and Reporting of Loss or Damage"* for guidance.

VIII. International Travel

Mobile technologies vary among nations, providers, and device brands; therefore, an employee who travels internationally and requires use of a DOT mobile or portable

computer resource to conduct DOT business shall contact the IT Division's Service Desk, 515-239-1075, at least two weeks prior to scheduled travel. The IT Division will then determine the best method for ensuring international connectivity at the most reasonable cost.

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 [redacted] COUNTY, IOWA

This Agreement is made and entered into this [redacted] day of [redacted], 2017, by and between [redacted] 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 antic-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 [redacted] IOWA

Security Awareness Training

The Key to Crisis Prevention

Importance of Security Awareness

- Protects staff and the public from improper use of personal information
- Protects against illegal and fraudulent activities

Responsibility For Security

- Every computer and every desk is a potential point of entry for someone that wants to improperly obtain information.
- All licensing personnel must be vigilant and involved to protect ourselves and the public.

Areas Requiring Security

- Internal Resources
  - Passwords
  - Internet/Intranet
  - Procedural/reference materials
- Physical Security
  - Keys/Access cards and awareness
- Documents
  - Personal information/documents
- Equipment
  - Computers and office equipment

Password Protection

- **Don't:**
  - Share your passwords
  - Store them in computer files
  - Write them down
  - Allow programs to "remember" your password.
    - » Remember, the system logs all actions (such as deleting files, sending malicious e-mails, or browsing to inappropriate sites) under user access/passwords.
- **Do:**
  - Use strong passwords containing at least eight characters consisting of combinations of upper and lowercase letters , numbers and special characters.
    - People may guess passwords based on family, hobbies, and interests, and password-breaking programs can crack passwords
    - Passwords aren't much use if you cannot remember them, so use a pass-phrase instead. It gives you the opportunity to use something that you can remember, but is still tough for someone to crack. For instance, an Iowa State fan should not use "cyclones," but could use "Iluv2root4st8." Another good suggestion is to intentionally misspell words. For instance, an Iowa fan should not use "hawkeyes," but could use "hwkIzRdabest"

Internal Resources

- Internet/Intranet
  - PPM 030.09
  - Any personal reference materials should be e-filed
    - Memos

Maintaining Physical Security

PPM 020.05

- Don't share keys or access cards.
- Don't defeat security by propping open secure doors, copying keys or letting people follow anyone into secure areas.
- Report lost access cards or keys immediately.
- Report suspicious activity.
- If someone looks out of place in a secured area, ask them if you can help them and try to find out who they are. If you are not comfortable doing so, report them to someone who can.
- Supervisor will discuss physical security information pertinent to your facility.

Maintaining Document Security

PPM 030.06

Don't:

- Print unnecessary copies of confidential documents
- Leave confidential documents on the copier or fax machine
- Leave confidential documents in places where they can be seen or taken by the public
- Take confidential documents out of the office without the approval of your supervisor
- Copy confidential information onto unencrypted disks, flash drives, etc PPM 030.13

Maintaining Document Security

Do:

- Practice a clean desk policy – don't leave confidential documents on your desk or work station overnight.
- Lock confidential work documents in a secure storage area overnight or when not accessing them for work purposes.
- Shred confidential documents/credentials as directed
- Make sure secure files and rooms remain locked when unattended.

Maintaining Equipment Security

- Secure and protect Department equipment **PPM 010.11**
  - Computers
  - Digital Photo equipment/Site Server Security Key (Dongle)
  - Fax
  - Printers
  - Document authenticator
  - Vehicles
- Immediately report missing, stolen or damaged equipment
- Maintain inventory and accountability of assigned Department equipment

Maintaining Workstation Security

PPM 030.02

Security Awareness Doesn't End At Log-On

- Logout when leaving your workstation for:
  - Break
  - Lunch
  - Drive Tests
  - Change in assignment (rotation)
  - End of shift
- Lock your workstation when stepping away from it. (In some offices locking the workstation may be preferred over logging out, your supervisor will provide direction.)
- Position your monitor so it can't be seen by unauthorized persons – don't allow people to peek over your shoulder.

Social Engineering

- Guard against con artists gaining your confidence or playing on your natural instinct to help people.
  - Follow protocol - know the proper procedure and adhere to it.
  - Ask questions –find out who the person is, what information they want, and why they want it, so you can make a good decision as to whether they are entitled to the information.
  - Don't release information unless the person provides all necessary documentation. If you are not sure ask for help.
    - PPM 030.06
    - Driver Privacy Protection Act,
    - Acknowledgement of Release of Confidentiality of Records
    - Acknowledgement of Work Rules and Policies and Procedures
  - Trust your instincts – if something feels wrong to you, ask for help.

Resources

- PPM 010.11 Department Equipment - Security, Inventory and Reporting of Loss or Damage
- PPM 010.12 Inventories at Field Locations
- PPM 010.17 Personal Data Assistant and Accessories
- PPM 020.05 Building Security--Ames Central Complex and Motor Vehicle Division Facilities in Ankeny and Des Moines
- PPM 030.02 Computer Workstations
- PPM 030.03 DOT Policies and Procedures Manual
- PPM 030.05 Records
- PPM 030.06 Records Management
- PPM 030.09 Internet and Intranet Services
- PPM 030.11 Information Resources Security
- PPM 030.12 Laptop Encryption
- PPM 030.13 Removable Media Encryption
- Release and Confidentiality of Records Acknowledgment
- Work Rules
- DPPA Policy

State of Iowa

Motor Vehicle Division

Security Awareness Training

ACKNOWLEDGMENT

I, _____, an employee of the:

☐ Iowa Department of Transportation, Motor Vehicle Division,

☐ _____County Treasurer's Office,

hereby acknowledge that I have completed the security awareness training module and viewed the ICE video "Do The Right Thing"..

_____ _____

Employee's Signature Date

_____ _____

Supervisor's Signature Date

Revised 2/11/2010