

## **ICADV CREDIT CARD SECURITY POLICY**

### **Summary**

The Payment Card Industry Data Security Standard (PCI DSS), a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis. PCI DSS compliance is mandatory for any organization that collects, processes, or stores credit card information.

### **Purpose**

The purpose of this policy is to establish requirements for collecting, storing, processing and transmitting credit card data to facilitate compliance with the PCI DSS requirements.

### **Groups Covered**

This policy applies to all ICADV staff, volunteers and any other persons who collect, process, transmit or store credit card information physically or electronically. Any other entity or individual using ICADV servers or the ICADV network must also abide by this policy. Hereinafter, all applicable persons will be referred to as "Department" for the purposes of this policy.

To help protect against exposure and possible theft of sensitive credit card data and to comply with the PCI DSS requirements, Departments must follow the policies and procedures outlined in this document.

### **Policy Requirements**

ICADV is required to establish, publish, maintain and disseminate a security policy that addresses all PCI DSS requirements. Each of the 6 goals and 12 requirements as outlined in the PCI DSS are addressed in this document.

#### **Section 1 - Build and Maintain a Secure Network**

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

#### **Section 2 - Protect Cardholder Data**

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

#### **Section 3 - Maintain a Vulnerability Management Program**

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

#### **Section 4 - Implement Strong Access Control Measures**

Requirement 7: Restrict access to cardholder data by business need-to-know

[Type text]

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

#### **Section 5 - Regularly Monitor and Test Networks**

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

#### **Section 6 - Maintain an Information Security Policy**

Requirement 12: Maintain a policy that addresses information security

### **Policy Implementation**

#### **1. Build and Maintain a Secure Network**

*Requirement 1: Install and maintain a firewall configuration to protect cardholder data*

All systems used to transmit cardholder data will implement a firewall to guard against intrusion.

*Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters*

All system passwords must meet the requirements given in the ICADV Electronic Information Security Policy.

#### **2. Protect Cardholder Data**

*Requirement 3: Protect stored cardholder data*

##### **Web Based Requirements**

In most cases, Departments will be required to use a secure web based gateway or virtual terminal that is supplied by a PCI compliant service provider.

Credit card data is not entered into a server on the ICADV network.

The contracted service provider transmits and stores the cardholder data. Data is not retained on any server hosted by the ICADV network.

Departments will not record or store sensitive cardholder data.

Sensitive authentication data that is stored on gateway systems or virtual terminals is masked and only select information is viewable to designated ICADV Employees with business need-to-know.

The maximum cardholder data that may be viewed may include the following:

- o The type of payment card (Visa, MasterCard, Discover, American Express)
- o The first four and the last four digits of the primary account number
- o The expiration date

##### **Hard Copy Requirements**

If a Department must physically collect cardholder data for payment, all documents containing sensitive data must be hand-delivered to the ICADV office within three business days of collection.

[Type text]

If hard copy of credit card data is kept by the Department for any length of time before it is delivered to ICADV, it must be stored in a secure, locked location with restricted access.

Only ICADV employees and volunteers with business need-to-know are allowed to access and/or view the cardholder data.

Cardholder data will not be stored in the ICADV office. Departments are not allowed to permanently retain credit card data.

Once the credit card data is received, the transaction(s) are processed by ICADV's third party processor.

Any received hard copy of credit card data is stored in a secure and locked location restricted from unauthorized access and is entered, processed, and shredded within 30 days of receipt.

No credit card data will be retained for no more than two fiscal years. The data will be kept for the time period specified for the following purposes:

- o To meet the ICADV's audit requirements.
- o To validate a charge in the event of a cardholder dispute or notification of fraudulent use.
- o To process a credit transaction to the card using the original method of payment.

At the close of a Fiscal Year end, ICADV will dispose of any credit card data stored from the prior Fiscal Year according to ICADV Data Retention and Disposal procedures.

### **Additional Requirements**

It is prohibited to enter or store sensitive authentication data on devices including, but not limited to, office or personal computers, laptops, data storage devices, USB flash drives, DVD's or CD's.

Credit card data may not be collected or transmitted using unapproved online forms, email, fax or any other unsecured transmission method.

#### ***Requirement 4: Encrypt transmission of cardholder data across open, public networks***

No cardholder data shall be transmitted across any data network in plain text. The transmission of cardholder data will require the use of Secure Socket Layer (SSL).

### **3. Maintain a Vulnerability Management Program**

#### ***Requirement 5: Use and regularly update anti-virus software***

All computer systems used for handling credit card payments will have current anti-virus software, updated regularly.

#### ***Requirement 6: Develop and maintain secure systems and applications***

All computing systems on the ICADV network and users of computers on the ICADV network must follow and abide by the ICADV Information Security Policy.

[Type text]

#### 4. Implement Strong Access Control Measures

***Requirement 7: Restrict access to cardholder data by business need-to-know***

Access to physically stored cardholder data and/or any system used to process and store transaction data is restricted and available only to ICADV employees whose job requires access to such information.

Authorized employees who access cardholder data must have a valid business purpose for doing so.

Access rights for employees utilizing web-based systems for online transactions are restricted to least privileges necessary to perform job responsibilities.

The assignment of privileges is based on each employee's job classification and function.

***Requirement 8: Assign a unique ID to each person with computer access***

User ID's for all ICADV information systems and services are granted and revoked as per the ICADV Electronic Information Security Policy.

Creation, access delegation and deletion of user accounts for systems used exclusively for credit card payment purposes is maintained by a system administrator appointed by the ICADV PCI Compliance Team.

- o Users of such systems are assigned a unique ID and password that allows access to their pre-determined privileges.

- o The initial password that is provided is changed immediately after the first use.

- o Users are prompted and required by the system to change passwords at least every 90 days.

- o Users shall follow good security practices in the selection and use of passwords as per the ICADV Electronic Information Security Policy.

- o Access for terminated users is immediately revoked and the user ID is disabled.

***Requirement 9: Restrict physical access to cardholder data***

Hard copy of credit card data is stored in a separate, secure room within the ICADV office.

The office is accessible only to ICADV employees and other ICADV volunteers/interns who require entrance into the area in order to perform functions of their jobs.

All access doors to the Cashier area are locked when the office is vacant and entrance is granted by entering an authorization code into a keypad. Only employees of ICADV are provided with the pass code(s).

If a Department must keep hard copy of credit card data for any length of time, it must be stored in a secure, locked location such as a vault or a locked filing cabinet.

Only ICADV employees with business need-to-know are allowed to access and/or view the cardholder data.

When destroying physically stored credit card information, hard copy of cardholder data is cross-shredded by an ICADV employee before it is disposed so that data cannot be reconstructed.

[Type text]

## 5. Regularly Monitor and Test Networks

### *Requirement 10: Track and monitor all access to network resources and cardholder data*

The ICADV will employ network monitoring tools to audit the network activity of systems transmitting cardholder data within the ICADV network.

The ICADV will employ intrusion prevention and detection methods to protect the transmission of cardholder data within the ICADV network.

### *Requirement 11: Regularly test security systems and processes*

Vulnerability management will consist of periodic network scans to identify and eliminate security threats that make system and network compromise possible.

Processes engaging the network will be reviewed periodically and will be adjusted accordingly as production processes give way to better practices.

## 6. Maintain an Information Security Policy

### *Requirement 12: Maintain a policy that addresses information security*

The ICADV PCI Compliance Team was created to facilitate and maintain compliance with the PCI DSS. The PCI Compliance Team is responsible for the following:

- o Establish, document and distribute security policies and procedures.
- o Monitor and analyze security alerts and information, and distribute to appropriate personnel.
- o Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
- o Assign responsibility for administering user accounts, including additions, deletions and modifications.
- o Assign responsibility for monitoring and controlling all access to data.

All transactions that involve the collection and processing of credit card data at ICADV or on ICADV systems must be performed using methods or systems approved by the ICADV PCI Compliance Team.

Departments must obtain approval from the ICADV PCI Compliance Team through an application process before credit card or debit card payments may be accepted.

If a Department is approved to accept credit cards, anyone within that Department who will be handling credit card data will attend a mandatory training session that addresses security awareness.

- o Individuals will be required to acknowledge that they have read and understand ICADV's Credit Card Security Policy and Procedures.

As an aid to minimize the risk of attacks from internal sources, criminal background checks are performed on each person hired for a position of employment at ICADV as per the policies and procedures relating to criminal background checks for employees.

Each Department approved to accept credit cards as a form of payment is required to adhere to ICADV policy and procedures to help ensure that they are compliant with the PCI DSS requirements.

[Type text]

The ICADV PCI Compliance Team will monitor and review that the Department is following compliance policies and procedures on at least an annual basis or if non-compliance is suspected.

#### **Risk Assessment**

The PCI Data Security Standard Self Assessment Questionnaire will be completed at least annually to identify threats, vulnerabilities and results.

The ICADV Credit Card Security Policy will be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

#### **Risk of Non-Compliance**

The requirements in this policy and other ICADV Policies are not optional and will be strongly enforced.

Failure to comply with the policies and procedures may result in:

- o Significant fines assessed to the Department and/or ICADV.
- o Additional costs associated with remediation or legal fees.
- o Loss of the ability to accept credit cards as a form of payment.
- o Unfavorable publicity and loss of a positive reputation.

#### **Resources:**

PCI Security Standards Council

<https://www.pcisecuritystandards.org/>

ICADV Electronic Information Security Policy

*Adopted September 7, 2011*

[Type text]

## The ICADV of Iowa Credit Card Handling Policies and Procedures POLICY

### Policy Statement

The establishment of control measures for credit card transactions is necessary to maintain proper security over credit cardholder information. The ICADV credit card handling policy requires each unit be certified as a credit card processing merchant, and each method of processing credit transactions be approved by the ICADV CFO. A credit card merchant is defined as a department or other entity which processes credit transactions.

Requirements for credit card merchants include the following:

- Approval of the ICADV CFO before entering into any contracts or purchases of software and/or equipment. This requirement applies regardless of the transaction method or technology used (e.g. e-commerce, POS device).
- Approval of the ICADV Information Technology Security Office of all technology implementation, including approval of authorized payment gateways.
- Establish departmental procedures for safeguarding cardholder information and secure storage of data. This pertains to ALL transactions initiated via the telephone, over the counter, mail order, Internet, etc.
- Perform an annual security self-assessment and report the results to Treasury Operations to ensure compliance with this policy and associated procedures.
- Compliance with Payment Card Industry (PCI) Data Security Standards

Periodic reviews of safeguarding and storage of cardholder information will be conducted by Treasury Operations, and credit card handling procedures are always subject to audit by Internal Audit and external audit or charge card review firms. In addition, ICADV will periodically conduct an assessment of security controls in place to protect technology implementations, including but not limited to periodic network-based vulnerability scans. Departments not complying with approved safeguarding, storage and processing procedures may lose the privilege to serve as a credit card merchant.

[Type text]

### **Who Should Know This Policy**

Any official or administrator with responsibilities for managing ICADV credit card transactions, and those employees who are entrusted with handling credit cards and credit card information.

### **Responsibilities**

**Department or Unit Executive Officer** - Submit a request to establish a merchant account.

**Credit Card Handling Supervisor**- Design an adequate process and procedure to ensure the following standards are maintained:

- Keep secure and confidential all cardholder numbers and information. Credit card receipts should typically be treated the same as you would treat large sums of cash. The department will be responsible for any losses due to poor internal or inadequate controls.
  - o Sensitive cardholder data (i.e., full account number, type, expiration, and track (CVC2/CVV2) data), cannot be stored in any fashion on computers or networks.
  - o Credit card numbers must not be transmitted in an insecure manner, such as by e-mail, unsecured fax, or through US mail (unless a sealed envelopes is used).
  - o All documentation containing card account numbers must be maintained in a "secure" environment limited to dependable, trustworthy and accountable staff. Secure environments include locked drawers, file cabinets in locked offices, and safes.
  - o All documentation containing card account numbers must be destroyed in a manner that will render them unreadable after their useful life (18 months) has expired.
- Restrict access to credit card data and processing to appropriate and authorized personnel.
  - o Background checks must be performed prior to hiring of any positions with unrestricted access to cardholder information.
  - o Require all personnel involved in credit card handling to attend card security training at least every two years.
- Establish appropriate segregation of duties between credit card processing, the processing of refunds, and the reconciliation function. Supervisory approval of all card refunds is required.
- Perform an annual self assessment to ensure compliance with this policy and associated procedures, and report the results of this assessment to Treasury Operations.
- Notify the ICADV Information Technology Security Office prior to implementation of any technology changes affecting transactions processing associated with the merchant account.

[Type text]

**Credit Card Handlers and Processors-** Agree not to disclose or acquire any information concerning a cardholder's account without the cardholder's consent. Credit card authorizations must be kept for 18 months for response to copy requests and charge-backs. E-commerce and merchants using third-party software, including cash register systems, are prohibited from storing complete payment card numbers on ICADV computers at any time. Other (external) credit card merchants must securely store and transmit information using at least 128 bit encryption, and provide a letter to the merchant unit attesting to Payment Card Industry Data Security Standards compliance.

**CFO** - Review and approve the establishment of new merchant credit card processors.

**Treasury Operations** - Administer the process of obtaining new merchant numbers. Conduct periodic reviews of existing merchants regarding safeguarding and storage of cardholder information. Provide periodic training on the secure storage and disposal of all non-ecommerce credit card paper transaction records in conjunction with cash handling training. Provide an annual report to the ICADV Information Technology Security Office of all merchant accounts, associated transaction volumes, and security self assessment reports.

**Information Technology Security Office** - Review and approve implementation of any technology changes and payment gateways associated with credit card transactions processing. Conduct periodic reviews for compliance with Payment Card Industry Data Security Standards.

#### **PAYMENT CARD INDUSTRY GUIDELINES**

[Visa Merchants Card Management Guide:](#)

[Mastercard International Rules Manual](#)

[Payment Card Industry Data Security Standard:](#)