EAA Policy for Accepting and Handling Credit and Debit Card Payments (“Policy”)

Background

Due to increased threat of identity theft, fraudulent credit card activity and other instances where cardholder information has been compromised, five members of the Payment Card Industry (PCI), Visa, Master Card, American Express, Discover and JCB, banded together to develop security standards for any organization that accepts, captures, stores, transmits and/or processes credit card information either manually or through an automated system. This set of standards is referred to as the Payment Card Industry’s Data Security Standard (“PCI-DSS”).

PCI-DSS is enforced through the contracts that Experimental Aircraft Association, Inc. (“EAA”), as a merchant account holder, has with our merchant bank, i.e., the financial institution that serves as a liaison between EAA merchants and the payment card companies. Each merchant will receive a compliance certificate once they have completed and passed the following requirements:

- The completion of an annual questionnaire that provides a means for assessing an organization’s compliance to PCI-DSS.
- Remote network vulnerability scans of all outward facing IP addresses (quarterly).

Penalties for non-compliance can include increased credit card transaction fees, a suspension of credit card privileges, and fines in cases where an account is compromised.

For additional information about PCI-DSS, please visit the PCI’s Web site at: https://www.pcisecuritystandards.org.

Purpose

This document describes EAA’s policy and procedures for the proper handling of credit and debit card transactions processed through automated systems and/or manual procedures. It is intended for:

Any employee, contractor, or volunteer (“individual”), who accepts, captures, stores, transmits and/or processes credit or debit card payments received in the course of business with EAA.

Any individual who supports any EAA effort to accept, capture, store, transmit and/or process credit card information. (e.g. such as a technical support staff member whose role gives him or her access to computer hardware and software holding credit card information, individuals tasked with shredding credit card information, etc.

This policy and procedures are intended to ensure that credit and debit card information is handled and disposed of in a manner that satisfies EAA's obligation to protect such information to the level that meets or exceeds that required by PCI-DSS.

Since any unauthorized exposure of credit or debit card information could subject EAA to reputational damage and significant penalties, failure to comply with the policy contained within this document will be considered a serious matter.

Principles

EAA is committed to complying fully with the expectations specified by the PCI-DSS. Compliance by EAA requires that:

- PCI-DSS compliance is mandatory for any department that accepts, captures, stores, transmits and/or processes credit or debit card information.

- Only authorized and properly trained individuals may accept and/or access credit or debit card information.

- Credit and debit card payments may only be accepted using methods approved by Senior Leadership Team and Controller.

- Each person who has access to credit or debit card information is responsible for protecting and destroying the information.

- Each department that handles credit and/or debit card information must have documented procedures and controls for complying with this policy and PCI-DSS.

- Suspected theft of credit or debit card information must be reported immediately to a member of the Senior Leadership Team and the Controller.

Failure to comply with these principles, as implemented in this Policy, may result in the revocation of the ability to process credit and debit card transactions and/or could lead to disciplinary action.

The following section defines the EAA's standard procedures in support of the above principles.

Procedures to Implement the EAA's Credit and Debit Card Principles

1. **PCI-DSS Compliance is Mandatory for any Department that Accepts, Captures, Stores, Transmits and/or Processes Credit or Debit Card Information.**

   Any EAA department that accepts credit and/or debit cards must comply with PCI-DSS to ensure the security of cardholder information. Compliance with the requirements of this policy (as updated or amended) satisfies the elements of compliance with PCI-DSS.

2. Only Authorized and Properly Trained Individuals May Accept and/or Access Credit or Debit Card Information

No individual is authorized to accept, access or support systems housing credit or debit card information until the following requirements are satisfied:

- The individual must be authorized by the Controller and Human Resources department.
- The individual must be trained in the proper handling of credit and debit card information.
- Individuals who are new to the role must be trained prior to taking on their credit or debit card handling duties. Individuals whose credit or debit card handling responsibilities preceded the implementation of this policy should receive training as soon as possible. The content of the training program must be reviewed and approved by the Controller and the Human Resources department to ensure that EAA objectives are met.
- The individual must acknowledge his or her understanding of this policy and must confirm his or her commitment to comply with all related EAA policies and procedures before he or she assumes credit and/or debit card handling duties and on an as needed basis thereafter. This requirement is satisfied by the individual physically signing the “Credit and Debit Card Security and Ethics Agreement” in Appendix A of this document.
- An individual is authorized to access lists, reports and/or storage areas where credit or debit card information is stored in electronic, magnetic, optical and/or physical (e.g., paper) form, or to support computer systems that store or process credit or debit card information if the following additional requirements are satisfied:

  - ✓ The individual must be an employee of EAA.
  - ✓ The Human Resources Department has performed a criminal background check to include a potential credit check, character reference, etc. on any prospective individual who may have access to such data.
  - ✓ In cases where a background check returns outstanding issues, the Controller, Human Resources department and Legal Counsel will review those issues to determine whether or not the individual should be permitted to handle credit card information.

3. Credit and Debit Card Payments May Only Be Accepted using Methods Approved by the Controller

Credit and debit card payments may only be accepted in the following manner, as approved:

- in person

- via telephone,
- via FAX,
- via physical mail (not e-mail),
- through a PCI-DSS-compliant automated system that is entirely hosted by a PCI-DSS-compliant third party organization approved the Director of IT and Controller,
- through an automated system that is hosted in the EAA data center that does not accept, capture, store, transmit or process credit or debit card information itself, but refers the customer to a PCI-DSS-compliant system hosted by a third party organization, approved by the Director of IT and Controller, which handles credit and debit card payments on our behalf. The third party system must not return credit card numbers, expiration dates or verification values to the EAA-based system.

Note – In cases where the use of a PCI-DSS-compliant third party for the capture, storage, transmission and/or processing of credit card payments is not feasible, an exception may be requested for an automated system that handles credit or debit card information on a EAA-based system, but only if the system can satisfy all PCI-DSS requirements. Exceptions require written approval the Director of IT and Controller.

Any department that uses a third party organization to accept, store and/or process credit or debit card information on its behalf, must receive from the vendor, on an annual basis, and keep on file documentation indicating that the vendor's system and procedures have been found to be in compliance with PCI-DSS. This documentation must be completed by a firm that has been authorized by the PCI to make such an assessment. A copy of this documentation should be submitted to the Controller.

4. Each Person Who Has Access to Credit or Debit Card Information is Responsible for Protecting and Destroying the Information

Individuals who have access to credit or debit card information are responsible for properly safeguarding the data to protect the integrity and privacy of such information.

The following pieces of information are considered "confidential" and must be protected appropriately from initial capture through destruction regardless of the storage mechanisms used (e.g., on computers, on electronic, magnetic or optical media, on paper, etc.):

- Credit or debit card number
- Credit or debit card expiration date
- Cardholder Verification Value (CVV2) – the 3- or 4-digit code number generally located on the back of the credit or debit card.
- Personal identification number (PIN)
- Cardholder's name, address and/or phone number when used in conjunction with the above fields

Special note: ***The use of Social Security Numbers in conjunction with credit or debit card information is strictly prohibited.*** *The use of Social Security Numbers is highly restricted. As such, Social Security Numbers never should be used.*

Neither the three- or four-digit credit or debit card validation codes (CVV2) nor Personal Identification Numbers (PIN) may ever be stored in conjunction with credit or debit card information in any form.

Point-of-sale devices must be configured to print only the last four characters of the credit or debit card number on both the customer and the merchant receipts, and on any reports that may be produced by the device.

Physical documents, such as customer receipts, merchant duplicate receipts, reports, etc., that contain credit or debit card information should be retained only as long as there is a valid business reason to do so, and no longer than 90 days. After the 90 days or earlier, all documents containing credit or debit card information should be forwarded to the EAA Finance Department for secure storage. Based on sales tax payment information or other regulatory standards the documents will be kept for 4 years.

All physical documents that are no longer necessary must be cross-cut shredded using a commercially available shredding device.

In cases where the Director of IT and Controller has granted an exception that allows EAA's system to accept, capture, store, transmit and/or process credit card information, the approved individual or department must ensure that computer-based data that is no longer necessary is destroyed in the manner described in Appendix B of this document.

While the documents are retained, they must be stored in locked cabinets in secured areas with access restricted to authorized individuals on a need-to-know basis. Keys that allow access to such containers must be immediately collected from any individual who leaves EAA or whose responsibilities no longer require them to access such documents. When combination locks are used, the combination must be changed when an individual who knows the combination leaves EAA or no longer requires access to perform assigned work.

For any physical documents that contain credit or debit card information, it is strongly recommended that all but the last four digits of the credit or debit card number be physically cut out of the document. Overwriting the credit or debit card number with a marker is not acceptable since the number can still be viewed in certain circumstances.

No lists should be maintained that include entire credit or debit card numbers.

Credit or debit card information may be shared only with individuals who have been authorized to access such data by the Controller.

In cases where the Director of IT and Controller have granted an exception that allows an EAA's system to accept, capture, store, transmit and/or process credit card information, the approved individual or department must ensure that the design of and all procedures associated with the application comply with the requirements listed in Appendix B of this document.

5. **Each Department that Handles Credit and/or Debit Card Information Must Have Documented Procedures and Controls for Complying with this Policy and PCI-DSS.**

Each department that handles credit and debit card information must have written procedures tailored to its specific department that is consistent with this policy and PCI-DSS. Departmental procedures should be reviewed, signed and dated by the Department supervisor on an as needed basis indicating compliance with the EAA's Policy. These procedures also must be submitted to and approved by the Controller.

These departmental procedures will include, but are not limited to, the following:

- Segregation of duties
- Deposits
- Reconciliation procedures
- Physical security
- Disposal
- Cash register procedures (if applicable)

Note - For assistance in developing departmental procedures, contact the Controller.

Exceptions to Required Procedures

It is understood that a unique situation within an individual department may require a permanent or short-term exception to one or more of the above procedures. Such an exception must satisfy ALL of the following conditions:

- It must comply with all applicable PCI-DSS requirements.
- It must be approved by the Controller.
- In the case of a permanent exception, it must be included in a department's written procedures.
- In the case of a short-term exception, it must be restricted to specific dates or events and documented in writing.

Revision History

This policy is subject to revisions.
1. Issuance date: 09/19/2013

Appendix A
Credit and Debit Card Security and Ethics Certification Form

The following page is a statement of understanding and intent to comply with the EAA Policy for Accepting and Handling Credit and Debit Card Payments.

Anyone who has access to credit or debit card information must sign the form and submit it to his or her Department supervisor on an annual basis.

Credit and Debit Card Security and Ethics Agreement

Many EAA departments and activities accept credit/debit card information, such as credit/debit card numbers, expiration dates and card verification codes, from donors, purchasers of EAA products and services, etc.

I recognize that this information is sensitive and valuable and that the EAA is contractually obligated to protect this information against unauthorized use or disclosure in the manner defined by the Payment Card Industry's Data Security Standard, and should such information be disclosed to an unauthorized individual, EAA could be subject to fines, increased credit and debit card transaction fees and/or the suspension of our credit and debit card privileges.

As an individual whose role includes the acceptance, capture, storage, transmission and/or processing of credit and/or debit card information, I agree with the following statements:

- I have read the requirements stated in the EAA's Policy for Accepting and Handling Credit and Debit Card Information ("Policy").
- I understand that I may only accept credit and debit card payments using methods approved in this Policy.
- I understand that, as an individual who has access to credit and debit card information, I am responsible for protecting the information in the manner specified within the Policy. Further, I understand that I am also responsible for effectively protecting the credentials (IDs and passwords) and the computers that I may use to process credit or debit card transactions.
- I understand that I must destroy credit and debit card information as soon as it is no longer necessary using methods prescribed by the Policy.
- I understand that in cases where I suspect that a breach of credit or debit card information has occurred, I must immediately report the breach to my immediate supervisor, Controller and/or the Human Resources department.
- If I manage an area that handles credit card information, I understand that I must have appropriate checks and balances in the handling of credit and debit card information, and that I am responsible for having documented procedures in place for complying with Policy.
- I commit to comply with the Policy and its documented procedure, and understand that failure to comply with the above requirements may subject me to a loss of credit card handling privileges and other disciplinary measures; up to and including termination of employment.
- I understand any fraudulent or other inappropriate use of credit or debit card information may result in criminal charges.

Signature: ____ Date:_________________________

Print Name:____

Appendix B

Procedures for In-House Application Systems that have been Granted an Exception to Handle Credit or Debit Card Transactions

In cases where a Department is granted an exception that allows a system to accept, capture, store, transmit and/or process credit card information, the Department supervisor must ensure that the design of the application and all procedures associated with the application complies with the following additional requirements:

- System and network controls, approved by the Director of IT and Controller, <u>must</u> be implemented to restrict access to authorized individuals and only on a need-to-know basis. The Department Manager is responsible for ensuring that access is immediately revoked for any individual who leaves EAA or whose responsibilities no longer require him or her to access such information.
- The three- or four-digit credit or debit card validation code (CVV2) <u>must</u> never be captured in any form.
- Credit or debit card information that is transmitted across a network <u>must</u> be encrypted using a method approved by the Director of IT and Controller.
- <u>No</u> reports should be maintained that list entire credit or debit card numbers without the approval of the Director of IT and Controller.
- It is <u>strongly</u> recommended that only the last four characters of the credit or debit card number may be retained in a database or computer file. Retaining the entire credit or debit card number in such circumstances requires the approval of the Director of IT and Controller. If such approval is granted, the following requirements apply:
  - Credit or debit card information held on EAA computer hard drives or on removable storage media (diskettes, CDs, DVDs, USB storage devices, etc.) must be encrypted using a method approved by the Director of IT and Controller.
  - Any file containing credit or debit card information stored on electronic or magnetic media (computer hard drives, diskettes, USB storage devices, etc.) that is no longer needed must be electronically “shredded” or wiped using a commercial tool and method approved by the Director of IT and Controller. Merely deleting the files is not sufficient, as common computer operating systems typically leave deleted information on such media intact.
  - No computer that has hosted a software application that accepts, captures, stores, transmits or processes credit or debit card information may be repurposed, donated, sold or sent to surplus until all of the hard drives on that system have been removed from the system and physically destroyed using a method approved by the Director of IT and Controller.
  - The Department supervisor is responsible for establishing procedures confirming that the required hard drive removal has taken place, and that all removed hard drives are protected against theft and unauthorized access through their destruction.
  - Any piece of non-magnetic/non-electronic media (e.g., CDs, DVDs) that has been used to store credit or debit card information must be cross-cut shredded before being discarded using a shredding device approved by the Controller.