POLICY

PCI DSS compliance policy

Version 2.1

June 2022

Variation
This document replaces the previous PCI DSS compliance policy v*ersion 2.0*
The following areas have been updated in this version:

- For further information and guidance, change of contact.

This policy/procedure is applicable to ICAEW employees in the *UK only* and does not include staff in our non-UK offices.

CONTENTS

THE POLICY

ICAEW processes tens of millions of pounds in card payments annually. Application of this policy is critical to maintaining our business operations.

This policy has been drafted and approved in agreement with the PCI Compliance Group. It describes the principles of compliance that ICAEW follow and establishes a policy that:

- facilitates ongoing compliance with the Payment Card Industry Data Security Standards (PCI DSS).
- enables ICAEW to continue to have the facility to accept card payments in support of delivering our business.
- is appropriate and fit for purpose for the service provision within ICAEW.
- endeavours to balance the need for effective governance with agile process.

The PCI policy shall:

- be documented and available on the ICAEW intranet for all staff.
- be communicated within the organisation.
- be managed and maintained effectively in accordance with company process.
- be signed-off as acknowledged and understood by all staff on joining ICAEW and then at least annually.
- be available to interested parties, as appropriate.

Failure to comply with this policy

Failure to comply by one part of ICAEW could result in our bank withdrawing permission for the whole of ICAEW to take card payments. Individuals who do not comply with this policy may be subject to disciplinary action.

Detailed procedural requirements are contained in various policy and procedure documents across ICAEW. Finance and ITD must give prior approval to any new or proposed changes to existing policies, systems, procedures, and processes that might affect payments using payment cards, or our payment gateways to ensure that the changes do not undermine compliance with this standard.

The Finance department is responsible for completing an annual self-assessment for PCI DSS compliance. The ITD department is responsible for completing quarterly penetrations tests and the Finance department upload these to the PCI Maintenance portals for First Data and Worldpay each quarter.

When does this policy apply?

This policy applies to all ICAEW staff, at all times (including the use of personal card details relating to expense claims and corporate credit cards). It also applies to contractors, subcontractors or temporary staff working on behalf of ICAEW in the delivery of facilities, catering, events, or other services.

What is covered by this policy?

Any/all processes or operations relating to taking, storing, processing and securely destroying data relating to card payments.

Policy Statement

This policy states ICAEW's commitment to compliance and good practice with the Payment Card Industry Data Security Standards (PCI DSS).

All staff will read and sign this policy on joining ICAEW and then confirm annually that they will adhere to ongoing compliance with PCI DSS in support of delivering our business objectives.

To implement this statement, all staff should ensure:

We limit the range of IT systems that contain payment card data in order to limit the risk in relation to PCI DSS compliance requirements.

a. We do not record payment card details in any of our core systems such as Pro, Nav, dynamics D365, Enquiry Management D365 (CRM), NICE, Ungerboeck and Outlook etc.
b. We do not store any 16-digit string numbers on any documents or files stored on our systems, including personal or company credit cards.
c. We do not record payment card details from 3rd parties on any documents or files stored on our computers or file servers.
d. We only retain card details in physical documents where it is necessary and then only for the necessary period.
e. When we scan forms and other documents to retain them in our document management systems, we ensure that the payment card details are masked and unreadable.
f. We use PCI DSS compliant hosted payment services to take payment card payments for self-service transactions through the web, payments via the secure payment line and for payments taken by staff.
g. Any providers selected to process payment information must be PCI compliant.
h. Access to systems should not be granted to any 3rd party without prior approval from ITD.

We maintain strong systems controls

a. We comply with the IT Security User Guide (held on the intranet).
b. We protect our network and systems in accordance with PCI DSS requirements. These include:
    - Maintaining an effective firewall and router configuration.
    - Not using vendor supplied defaults for system parameters and other security parameters.
    - Providing effective data-retention and disposal policies.
    - Encrypting transmission of card holder data across open, public networks.
    - Maintaining anti-virus software.
    - Maintaining secure systems and applications.

- Restricting access to card holder data to only staff whose jobs require it.
- Ensuring appropriate access controls and monitoring systems are in place.
- Assigning a unique ID to each person with computer access.
- Regularly testing security systems and processes.
- Maintaining an information security policy (held on the intranet).
- Ensuring all ICAEW corporate card holders have read, understood and agree to adhere to the ICAEW One Card Holders Policy Statement prior to delivery of the card.

We restrict the ways that payment card information comes into or out of ICAEW so that we can ensure it is safe.

a. We do not use email to send any payment card details. Emails containing payment information are restricted to a secure inbox and receipt is subject to strict protocols.
b. We insist that all card payments coming into ICAEW by post or phone must follow one of the specified routes.
c. We provide approved and PCI DSS compliant means for members and customers to make online payments and payments via the automated phone line.
d. We will not accept images of cards for payments, and endeavour to limit use of screen shots, photos, scanned pdfs, or any digitised image in the business that may contain card numbers.

We protect card data within ICAEW as if it were cash.

a. We keep all payment card details secured when in ICAEW premises or staff possession. Specific data that is secured includes the primary account number (PAN), card holder name and expiration date. We never write down the 3-digit security code (or CVV) from a card.
b. We do not send card details between ICAEW locations by internal mail or email.
c. We operate additional policies in those areas that routinely handle payment cards to restrict the exposure of card information. These include:
    - No payment card details are left on unattended desks.
    - Mobile phones and smart devices capable of capturing image, video, audio, or Optical Character Readers (OCR) are kept out of sight and must not be used in the designated PCI Compliant areas.
d. We comply with the card payment handset (PDQ) guidelines to protect card data.
e. We limit physical access to any retained card data, eg, till-rolls, microfiche, call recordings, etc. We only allow staff who need access for their role to access the data.
f. We record and monitor all access to retained card data and maintain an audit trail of access.

We only keep payment card data for as long as necessary for business and legal reasons.

a. We comply with the ICAEW Document retention and destruction policy (held on the intranet) and destroy documents as soon as they are no longer needed.
    - We do not retain card payment details once the payment has been processed.

- We only retain PDQ merchant copy receipts for as long as necessary. This is defined in the PDQ machine guidelines.

b. We comply with the Data Retention policy (held on the intranet) and destroy data as soon as it is no longer needed.

Remote / home working

Extra challenges are experienced when employees are working remotely but these risks can be mitigated by reminding staff:

a. Any unauthorised copying, moving, sharing, or storing of payment card data in remote environments is prohibited.
b. Remote staff should also be aware of their physical surroundings, for example taking care to prevent sensitive information from being viewed by unauthorised persons.
c. Beware of potential phishing calls. Remote staff should know how to confirm that a person who phones, claiming to be from IT Support is legitimate before providing any information.
d. Remote workers should be provided with and only use company approved hardware devices e.g. mobile phone, laptops, desktops etc. as this ensures ICAEW can maintain control of systems and technology supporting the processing of telephone-based payments.
e. Such hardware should:
   Have firewalls installed and operational.
   Have the latest version of the approved virus protection software.
   Have the latest approved security patches installed.
   Be configured to prevent users from disabling security controls.

Further information and guidance

For further information please contact the Financial Controller, or any member of the PCI Compliance Group Connect - Search (sharepoint.com)

More about PCI DSS https://www.pcisecuritystandards.org/pci_security/how

Document control

Date: June 2022
Expiry: June 2024
Confidentiality: ICAEW use only
Version: 2.1
Owner: Financial Controller
Drafted by: Andrew Hopkinson
Approved by: PCI Compliance Group
Next review date: May 2024
Linked documents: PCI DSS Card Payment (PDQ) Handsets Procedure