

**Request for Comments (RFC) Instructions:
RFC for Currently Published
PCI Data Security Standard (PCI DSS v4.0.1)
3 June – 20 July 2026**



Thank You in Advance!

First and foremost, the PCI Security Standards Council (PCI SSC) would like to thank you for taking time to review and provide feedback on the current Payment Card Industry Data Security Standard (PCI DSS), v4.0.1

- Your feedback is fundamental to the ongoing evolution of our standards. The following slides will guide your review.
- If you have any questions or issues regarding this RFC, please do not hesitate to contact us directly at RFC@pcisecuritystandards.org.

Before You Begin

Please read these instructions and guidance in their entirety.

Plan your reviews ahead of time and ensure your feedback is submitted before the RFC period **closes at 11:59 pm Eastern Time on July 20, 2026.**

Refer to the [What to Know Before Participating in a PCI SSC Request for Comment](#) flyer for more information.

Purpose & Scope of this RFC

- PCI SSC is conducting this RFC period to gather industry feedback on PCI DSS v4.0.1, the currently-published version of the standard.
- The purpose of this RFC is to help determine whether to revise, and what type of revisions are needed for, PCI DSS v4.0.1.
- Feedback received during this RFC period will be reviewed and considered in the planning for a potential revision effort.

Types of RFC Feedback Requested

PCI SSC is seeking feedback on the whole standard, including the introductory section, security requirements, testing procedures, guidance, and appendices.

Examples of the types of feedback items requested include:

- PCI DSS concepts, principles, terms, definitions, requirements, and/or guidance that would benefit from additional clarification and/or improvement.
- New security requirements and testing procedures that should be considered for inclusion in a revision.
- Security risks or other related issues that are not effectively addressed in the currently-published standard.
- Areas where implementation experience since the publication of v4.0.1 suggests revision, refinement, or additional supporting guidance would be beneficial.

Additional Questions & Considerations

In addition to feedback on the current version of PCI DSS, PCI SSC would also like your feedback on the following broader considerations:

- Are there areas where PCI DSS can better align with other PCI SSC standards, and if so, how?
- Are there specific PCI DSS requirements that need to be addressed, considering the impact of AI and mobile?

If you provide answers, note them under the Category of '**Other**'.

RFC Timelines

The RFC period will run from 3 June to 20 July 2026.

Feedback must be submitted before 11:59 PM ET on 20 July 2026 to be considered.

Late feedback will not be accepted.

Note: PCI SSC can only accept feedback that is received via the Portal during the RFC period. Late feedback and feedback submitted via any other channel will not be accepted.

RFC Feedback Instructions

PCI DSS v4.0.1



Accessing the RFC Document

Log in to the PCI SSC Portal with your username and password: <https://programs.pcissc.org/>

- If you don't know your password, click "Forgot your password" to create a new password. If you do not have a username, please contact RFC@pcisecuritystandards.org for assistance.
- Click on RFC – PCI Data Security Standard (PCI DSS v4.0.1).
- Accept the Non-Disclosure Agreement (NDA).
- Click to download the RFC document.

Note: Only your company's primary contact may log into the portal and download the RFC document. If you do not know who your company's primary contact is, please contact RFC@pcisecuritystandards.org for assistance.

Entering Your Feedback

- In the Document field, select the following option from the drop-down:
 - Payment Card Industry Data Security Standard (PCI DSS), v4.0.1
- In the Section field, select the appropriate document section that is the subject of your feedback (as applicable).
- In the Sub-section field, select or specify the appropriate document sub-section or Requirement (for example, Requirement X.X.X) that is the subject of your feedback (as applicable).
- Specify the Page Number containing the content to which your feedback refers.
- Select the appropriate Category of feedback from the drop-down menu.
- Provide your Comments and a Suggested Solution for each item of feedback.

Note: Further details describing the subject of your feedback, such as the specific section or requirement referenced, should be specified in the Comments and/or Suggested Solution field(s).

Maximizing Your Feedback

- In the Comment field, explain the reason for your feedback.
- In the Suggested Solution field, provide a recommended approach for addressing your feedback.
- Be as detailed as possible with your comments and suggested solutions.
- If you do not have a Suggested Solution, please leave the Suggested Solution field blank. It is not helpful to duplicate the same information in both fields.
- Do not submit the same feedback item more than once.
- Do not include company sensitive information and remember to keep your comments professional and collaborative.
- **Each company is limited to 50 feedback entries in total, so consolidate your organization's submissions before entering them in the Portal.**
- Please contact RFC@pcisecuritystandards.org with any questions or concerns.

Other Feedback Reminders

- Ensure your work is saved after each entry and before you exit the portal - select “Save Draft Comments.”
- You can come back later to finish entering feedback; you do not need to enter all feedback in the same session.
- When all your feedback is complete, select “Submit Feedback” and then select “Ok” to confirm your submission is complete.
- A confirmation email will be sent after you submit your feedback.
- Once you select “Ok” to submit your feedback, you will not be able to edit it.
- **Your feedback, including your organization’s name, and how PCI SSC actioned your feedback, will be made available for review by RFC participants through the PCI SSC Portal. Please ensure your feedback is appropriate for public viewing.**

After Submitting Your Feedback

- All RFC feedback will be reviewed and considered by PCI SSC.
- Your feedback, including your organization's name, and how PCI SSC actioned your feedback will be made available for review by RFC participants through the PCI SSC Portal.
- Refer to the [PCI SSC RFC Process Guide](#) for more information.

Thank You!