Third Party Security Review (TSR)

FAQ for Third Parties

Questions

What is the purpose of doing the Third Party Security Review (TSR)?

PG&E completes a detailed risk assessment or Third Party Security Review (TSR) to ensure third parties who collect, store, use, or disclose PG&E's covered and other sensitive information have proper business agreements with PG&E and are capable of protecting those data assets from unauthorized access, use, modification, destruction, or disclosure. PG&E is also responsible for ensuring the aforementioned third parties are in compliance and remain in compliance with the same internal and external regulatory requirements to which PG&E is subject.

The purpose of the TSR program is to provide PG&E with a standardized method for evaluating the risk of conducting business with any third parties and ensuring PG&E data assets are protected in compliance with PG&E information security standards and appropriate regulatory requirements.

Why do we need to participate in a TSR?

PG&E has determined that you are, or will be, receiving protected data assets.

What happens if we choose not to participate?

PG&E will not provide you with any protected data assets until a TSR has determined that you are eligible to receive that protected data.

What if we have already done a TSR?

Even if your organization has already done a TSR, you may need to go through the process again. Usually this is because TSRs expire. A TSR is good for one year and then the TSR will need to be renewed.

Changes in the information being shared, network connectivity, and/or the size and complexity of your organization can also influence whether or not a new, or revised, TSR is required.

If you have a currently valid and applicable TSR, PG&E will not require a new TSR unless/until you need to renew your current TSR.

Who decides what constitutes protected data assets?

PG&E makes this decision based off of careful consideration of our policies and legal and regulatory requirements.

"PG&E" refers to Pacific Gas and Electric Company, a subsidiary of PG&E Corporation. © 2015 Pacific Gas and Electric Company. All rights reserved.

FAQ for Third Parties

How will the TSR be conducted?

PG&E's Cybersecurity/Security team will contact your organization by email. This email will include an assessment questionnaire and instructions for how to complete it and submit it back to PG&E.

Your organization will complete the assessment questionnaire and return it to the Cybersecurity/Security team.

The Cybersecurity/Security team will evaluate your compliance with PG&E's data protection requirements. This completes the assessment part of the TSR.

If your organization does not fully comply with our data protection requirements, PG&E will contact you about what mitigating alternatives and/or remediation measures would have to be in place for the transfer of protected data assets.

The TSR process is not complete until all of the mitigation and/or remediation measures are in place.

Note: under certain specific conditions, it may be possible that your organization has an existing certification or audit that satisfies PG&E's requirements without completing our questionnaire. These conditions, and what to do if you meet them, will be specifically covered in the initial email you receive.

What if we do not need the protected data assets, do we still need to participate?

If your company doesn't need any protected data assets, you may not need to participate once you no longer have them.

Some companies are only required to have TSRs because they have protected data assets. If this is the case, then eliminating the protected data will eliminate the need for a TSR.

Other companies may require a TSR for other reasons, such as access to PG&E networks. In these cases, the companies will still require a TSR, whether they have access to protected data assets or not.

If you believe you want to change your data requirements to avoid receiving protected data assets in the first place, please discuss this with your PG&E point(s) of contact.

Who will pay for the TSR assessment?

While PG&E will not charge you for any of the work we do as part of the TSR process, including work done by PG&E on your assessment, PG&E will not be accountable for any costs incurred by your organization associated with the TSR assessment.

FAQ for Third Parties

If corrective actions are identified as part of the TSR, what are the next steps and who will pay for these?

If gaps are identified during the TSR, PG&E will give you details of those gaps and work with you to make sure your remediation and/or mitigation plans are consistent with PG&E's data protection requirements.

PG&E will then review your completion of the remediation and/or mitigation plans to make sure they meet PG&E's data protection requirements.

Your organization is responsible for implementation of any remediation and/or mitigation plans, and PG&E will not be accountable for any costs incurred by your organization associated with this responsibility.

What if our organization cannot afford to remediate a security risk? What's the impact?

PG&E may attempt to work with you to find alternate methods to mitigate risks.

PG&E cannot transfer protected data assets until all specified risks have been either remediated or mitigated by an alternate method.

Who should participate in the TSR (from our organization)?

The review should be addressed by someone at your company who is knowledgeable about your information security practices, policies and controls.

Generally, these individuals include your Information Security Officer, IT Network Specialists, Security Administrators, System Administrators, Disaster Recovery and Business Continuity Experts, etc.

How long do TSRs last?

A TSR is good for one year. If your organization will still have protected data assets after one year, the TSR will need to be renewed.

Note: the TSR is good for one year from the date of the completion of the assessment, **not** one year from the date of the completion of any remediation. This is another reason you will want to complete any remediation efforts as quickly as possible.

If we have additional questions, who do we contact?

Please wait till after you have received the email from Cybersecurity/Security with the assessment questionnaire. If you still have follow up questions after you have thoroughly reviewed that email, use the contact information in that email for follow up.