workiva

Workiva Platform Security: Enabling Partners in the Sales Process

Security Team
Cybersecurity and Compliance - Workiva

This presentation is internal to Partners and not meant to be shared with your clients or prospects.

workiva

Partner's Success through Security

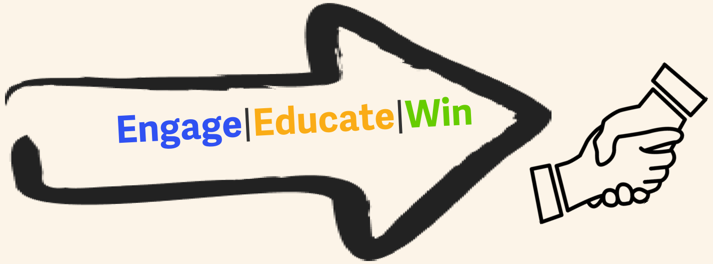
Signing NDA: Get **NDA signed** early with your prospect

Engaging security (Security@workiva.com) team **early** in sales cycle to avoid any potential road blocks on Security.

Educating the Prospect : Workiva platform is **FedRAMP** authorised and undergoes **SOC 1, SOC 2, ISO 27001** audits annually. Reports can be shared upon **NDA** for new prospects.

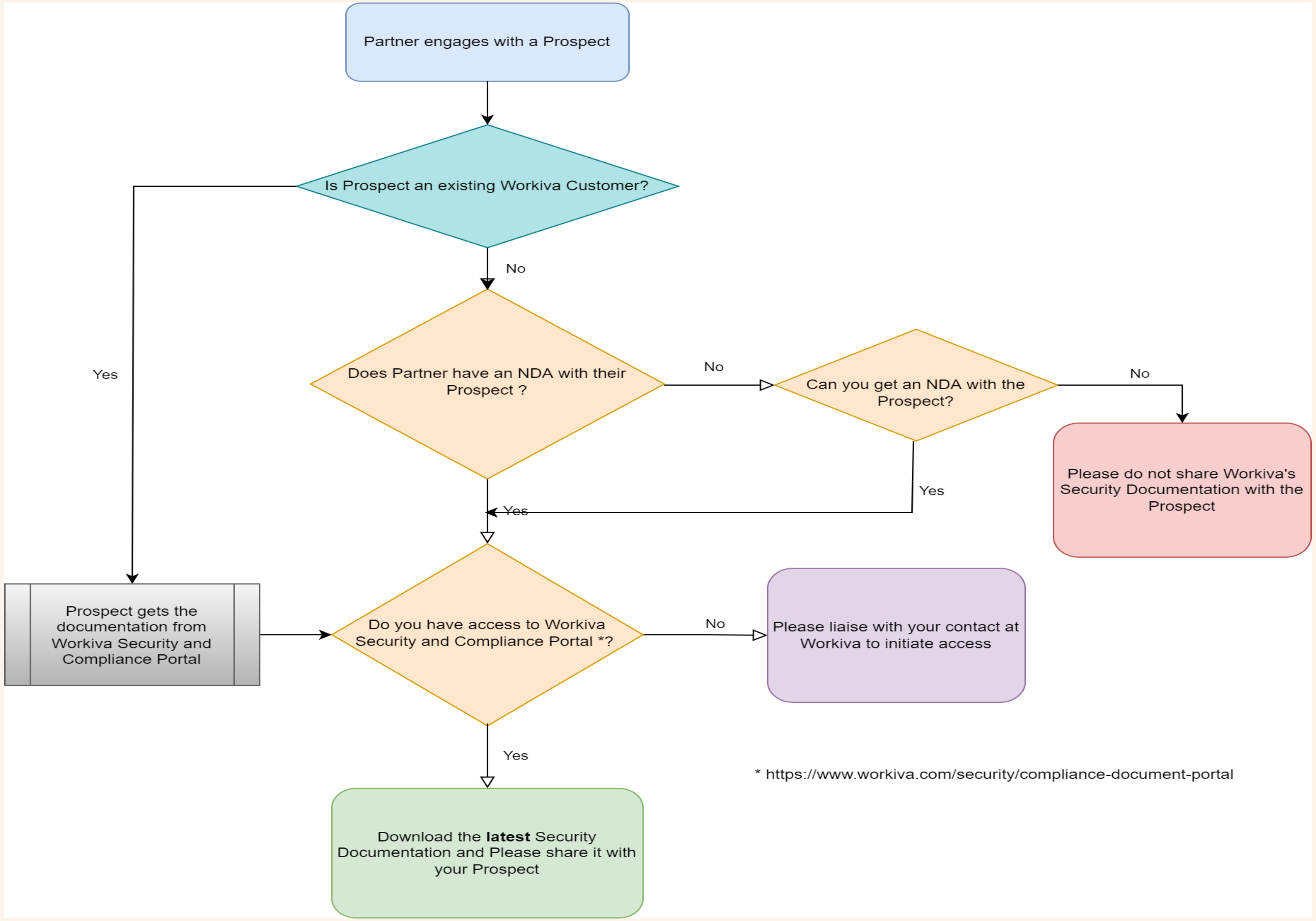
Know where and how to send security documentation with the prospect: Security documentation via **Security Compliance Portal**

Please do not share Workiva's Security documentation with your prospect without a signed NDA in place. When sharing the information, please make sure to download the latest security documentation from the Security Compliance Portal.



Engage|Educate|Win

Partner Enablement Security Process


Partner engages with a Prospect
Is Prospect an existing Workiva Customer?
Yes
No
Does Partner have an NDA with their Prospect ?
No
Can you get an NDA with the Prospect?
No
Please do not share Workiva's Security Documentation with the Prospect
Yes
Yes
Prospect gets the documentation from Workiva Security and Compliance Portal
Do you have access to Workiva Security and Compliance Portal *?
No
Please liaise with your contact at Workiva to initiate access
Yes
Download the **latest** Security Documentation and Please share it with your Prospect

* https://www.workiva.com/security/compliance-document-portal

Partner Enablement Security Information

Security at Workiva - https://www.workiva.com/security

- Workiva focuses on several aspects of security that are critical to business customers:
  - Application and security architecture – Our applications are designed and developed with careful consideration given to customer data security, reliability, and integrity.
  - Data security – Customer data is stored in secure facilities, on secure servers, and within secure applications.
  - Data privacy – Confidential information is kept private.
  - Organizational and operational security – Policies and procedures ensure security at every phase of design, deployment, and ongoing operations.

- Workiva provides extensive controls to combat hacking attempts, so you can be confident that we are always working to keep your data secure.
- Workiva requires Okta authentication for access to all our internal systems, with multi-factor authentication.
- Our customers are able to configure IP address allow lists that prevent anyone - even those with correct credentials - from connecting unless they originate from a known-good network.
- Workiva uses cutting-edge malware detection and response capabilities on our endpoints to identify any unauthorized access or malware on our employees' laptops.
- Outbound traffic on Workiva employee laptops is also controlled with DNS filtering to prevent access to phishing, malware, and command & control domains.
- No single Workiva employee has access to all our customer data. Access is granted as needed, to what is needed, and only after additional training has been successfully completed.

workiva

Security Resource Pool

Workiva Website

Workiva utilizes numerous measures to ensure the utmost in data security and privacy. More information available at https://www.workiva.com/security

Compliance Portal

On-Demand Access

Simply navigate to the Portal, and sign in with your Workiva account.

https://www.workiva.com/security/compliance-document-portal

Getting Started for IT

Easy steps for Information Technology teams to follow in order to easily onboard the platform.

- Network Settings
- System Requirements
- 'How-to' Links to Configure Company Policy

https://support.workiva.com/hc/en-us/articles/360043119131-Getting-Started-with-Workiva-for-IT

Policies

Privacy Policy: https://www.workiva.com/legal/privacy-policy

Cookies: https://www.workiva.com/legal/cookies

Code of Conduct: https://s21.q4cdn.com/997645077/files/doc_downloads/2022/05/WLife-Code-of-Conduct_April2022.pdf

GDPR: https://www.workiva.com/resources/general-data-protection-regulation-gdpr-and-wdesk

BYOK (if applicable)

With Bring Your Own Key (BYOK), customers can bring their own encryption keys for complete flexibility, control, and visibility of access to their data https://www.workiva.com/security/byok

Key Management: https://support.workiva.com/hc/en-us/articles/360041584231-Managing-Encryption-Keys

FAQs

Q: Does Workiva store Customer information on their internal network?
No, customer data is only ever stored in Workiva's Platform. Workiva does not maintain any local infrastructure. Customer data is stored in secure facilities, on secure servers, and within secure applications.

Q: How is Workivas' platform accessed by Customers?
All access is via web browser, over TLS 1.2+, Port 443.

Q:Does Workiva require access to my network or physical locations?
No, access is not required.

Q: What data types are in scope?
Workiva's Platform stores confidential company information used for either internal or external reporting, including compliance management, risk, management and audit reporting. Workiva does not access data put into its system, and all data is input by customer employees. We do not store PII subject to GLBA (Gramm-Leach-Bliley Act), or PCI data. PHI data is allowed for SOX customers, but is generally also out of scope.

Q:Where can I find more due diligence documentation or a specific document?
If you are unable to find a document on our compliance portal here please email Security@workiva.com

Q: Where can I find more information on Workiva's APIs?
Our API documentation is posted for review here

Q: What is required from IT teams?
The Workiva platform requires very little support from IT. The only required action is to ensure DNS whitelisting is completed. We have a **getting started guide** for Customer IT Departments available at https://support.workiva.com/hc/en-us/articles/360043119131

Q: Where can I find Workiva's Financials?
Workiva is a publicly traded company under ticker WK on the NYSE. Filings can be found on the SEC's website here

Q:Does Workiva comply with GDPR/CCPA and other privacy laws?
Workiva stores business contact information (Employee First Name, Last Name, Business email address, and IP Address) for account creation, incident monitoring, and audit logging. Workiva has a published privacy policy with a Truste and Privacy Shield Certification https://www.workiva.com/legal/privacy-policy. More information on GDPR compliance can be found here

Q: Does Workiva maintain documentation on the Platform?
Yes, Workiva maintains help articles and configuration guidance on our help site, which can be accessed at success.workiva.com. T access most of this information, no account is required.

Q:Is there an NDA required to share security pack documentation?
Yes, as we have NDA protected information contained within Workiva's Security Pack.

Q: Do you perform penetration testing and can these reports be accessible?
Yes, Workiva performs its own penetration testing as well as working with external companies to provide penetration testing. Workiva will provide our Third Party Penetration and Vulnerability Summary Report completed semi-annually, as tested in our SOC reports.

workiva

Useful Links

Workiva Security : https://www.workiva.com/security (most of the security related information available here)

Workiva is **ISO/IEC 27001:2013** certified. Download Certificate.

Cloud Security Alliance **CAIQ-Lite** available here https://www.workiva.com/resources/caiq-lite-security-assessment-responses

Workiva **Status Page**: https://status.workiva.com/

Service Level Commitment: https://www.workiva.com/legal/service-level-commitment

System Requirements: https://support.workiva.com/hc/en-us/articles/360036001691

Security Recommendations

Recommended settings to implement to secure your organization and workspaces.

- Single Sign-On
- Two-Factor Authentication
- Password Policy

Getting Started with Workiva Platform for IT

Easy steps for Information Technology teams to follow in order to easily onboard the platform.

- Network Settings
- System Requirements
- 'How-to' Links to Configure Company Policy

https://support.workiva.com/hc/en-us/articles/360043119131-Get-started-with-Workiva-for-IT

BYOK (Bring Your Own Key): With BYOK, customers can bring their own encryption keys for complete flexibility, control, and visibility of access to their data https://www.workiva.com/security/byok

Release Notes

- New Features and Functionality within the Workiva Platform

https://support.workiva.com/hc/en-us/sections/4404206165268-Release-Notes

Security Bulletins

- https://support.workiva.com/hc/en-us/sections/4405094352660-Security-Bulletins-

workiva

Key Takeaways

Get NDA signed early with your client

Please access the Security Compliance Portal with your Wdesk login or work with your Account Admin to obtain it

Email all your security related requests (queries, request for document, etc.) to **security@workiva.com**

Please make sure to share the latest downloaded information from Security Compliance Portal

workiva

We're here to Help!

If you have any questions, please reach out to security@workiva.com