Vendor Management Policy

Reveal relies on vendors to perform a range of services, some of which are critical for operations.

Reveal aims to manage its relationship with vendors and minimize the risk associated with engaging third parties to perform services. This policy provides a framework for managing the lifecycle of vendor relationships.

Vendor Risk Assessment

For each potential vendor, conduct an initial risk analysis, assigning the vendor a “low,” “medium,” or “high” rating based on the highest risk level attributable to the contract.

	Low	**Medium**	**High**
Business impact	Nominal impact, could get along without it. Does not connect to any piece of #company infrastructure.	Significant but non-critical business impact	Mission critical
Customer facing?	No	Indirect	Direct
Access to customer data	No access	Access to often public but personally-identifiable information (e.g. email addresses)	Access to non-public personally-identifiable information (e.g. email content)

The rating indicates the level of due diligence Reveal requires for each vendor:

- **Low-risk** vendors typically require little analysis
- **Medium-risk** vendors should be evaluated to determine the appropriate level of due diligence required
- **High-risk** vendors require extensive review

Vendor Assessment Process

Risk assessments should be conducted before doing business with a new vendor and revisited when the relationship with the vendor changes significantly, including contract renewals. All vendors are required to be reassessed annually.

An assessment of the proposed vendor is initiated when a Vendor Sponsor (anyone at Reveal looking to do business with a vendor) submits a review request to the Security Team.

The Vendor Sponsor may wish to sign a mutual Non-Disclosure Agreement (mNDA) with the proposed vendor. The proposed vendor and the Vendor Sponsor should sign the mNDA before the Vendor Sponsor:

- discloses Reveal information to determine company/vendor fit
- accepts a completed Vendor Assessment Questionnaire (VAQ), which contains the vendor's operating information.

The Vendor Sponsor should then submit the mNDA (if applicable), VAQ, and other relevant collateral to the Security Team for review.

The Security Team will complete the review in a timely manner and communicate next steps to the Vendor Sponsor. All reviews should be documented in [output documents of the vendor management process], for security, legal, and audit.

When the Security Team approves the vendor, the Reveal Vendor Sponsor may move forward with contract negotiations.

The Security Team must provide documented approvals to the Vendor Sponsor.

The Vendor Sponsor may set the vendor up for payment. The Vendor Sponsor will be responsible for ensuring the Security Team’s documented their signoff.

Vendor Assessment Due Diligence

Due diligence entails making a reasonable inquiry into a vendor’s ability to meet the requirements for the proposed service. Reveal first sends the proposed vendor a Vendor Assessment Questionnaire. Once the VAQ is completed, the Security Team reviews the responses and either clears the vendor, rejects the vendor, or requests further information.

A due diligence review might include further discussions regarding the following topics:

- **Regulatory**: Can the vendor create regulatory risk for Reveal?
- **Reputation**: How might the vendor impact Reveal’s reputation?
- **Financial**: Can the vendor impact Reveal or its customers financially?

- **Access to customer data**: To what extent will the vendor handle sensitive Reveal data?
- **Operational effectiveness**: How might Reveal be affected if the vendor experienced downtime? If the vendor ceased operations suddenly? Are there other potential vendors that Reveal could work with in such cases?
- **Compensating controls:** Does the vendor offer multi-factor authentication on its service? Can that be enforced such that all Reveal users must turn on MFA to use the service?

Vendor Compliance Considerations

If the vendor has a SOC 2, ISO27001/2, or other relevant collateral, it should be collected, reviewed by the Security Team, and documented in Reveal records.

Managing Vendors

Vendor Supervision

Each vendor will be assigned a Vendor Sponsor who will act as a liaison between the vendor and Reveal.

Vendor List

The CTO maintains a complete list of all vendors, associated risk rankings, the Vendor Relationship Manager, and the date of the most recent evaluation.

Vendor Configuration

Multi-factor authentication should be enabled on all accounts for all vendors.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Reveal management will determine how serious an employee's offense is and take the appropriate action:

- For minor violations, employees may only receive verbal reprimands.
- For more serious violations (e.g. onboarding a vendor without appropriate review and due diligence), employees may face severe disciplinary actions up to and including termination.

Responsibility

The Reveal Vendor Sponsor is responsible for ensuring prospective vendors enter the vendor review process.

The CTO is responsible for ensuring this policy is followed.

Last updated: 2021-10-07