Risk Checklist

December 2022

Protecting Your Data With Vendors

Preventing cybercrime and ensuring data compliance goes beyond your financial institution and accountholders. It's important to ensure that your vendors and subcontractors are adhering to data protection, security, and management best practices. Protect your data with these four due diligence checklists.

Allied Solutions

alliedsolutions.net

Vendor Data Storage & Access Checklist

ENSURE THAT YOUR VENDORS ARE STORING AND ACCESSING YOUR DATA WITH THESE BEST PRACTICES:

Visit our website for more risk education: ***alliedsolutions.net/resources***

- □ Data is being housed in a physically secure environment with 24/7 monitoring that restricts access to only authorized individuals and detects all access attempts.
- □ Systems and devices processing or holding your data remain protected by encryption, antivirus, and antispyware software.
- □ Access to all systems holding or processing data uniquely identifies each individual requiring access, to be able to trace fraudulent data access or use to an individual user, when needed.
- □ A list of locations and devices storing and processing your data is accessible to your institution, and any changes to this list are promptly communicated.
- □ A list of any third party vendors with which your data is being shared is known by your institution, and any changes to this list are promptly communicated.
- □ All data access is guarded by passwords that adhere to strong criteria, including complex character requirements and entry safeguards (i.e. password expiration, suspension, and reset protocols).
- □ Oversight of key functions and systems is split amongst multiple employees to reduce internal data exposure or theft.
- □ Regular reviews are performed to ensure access to data is limited to only those who have a business need.

Vendor Data Policies & Procedures Checklist

PROTECT YOUR DATA WITH STRONG POLICIES REQUIREMENTS FOR YOUR VENDORS:

- □ Written data management policies in place to identify safe, compliant practices for collecting, accessing, storing, disclosing, and destroying confidential information.
- □ Comprehensive written data access and security policies that outline safe, compliant practices for preventing unauthorized, unauthenticated, or unlawful use of data.
- □ Plans are established to regularly review and revitalize data security protections and procedures.
- □ A third-party risk management program is maintained to prevent data exposure that may originate from your vendors' vendors.
- □ A documented business continuity plan is in place that identifies processes for managing response activities and recovering operations without neglecting security or compliance.
- □ Plans are in place to immediately communicate data deficiencies or threats if at any point one is discovered.

Vendor Data Security Audits & Simulation Tests Checklist

ENSURE THAT YOUR VENDORS FOLLOW THESE DATA BEST PRACTICES:

- □ At least once a year, a comprehensive, independent risk audit (i.e. SOC2) is performed to identify and resolve any internal or external data security weaknesses or threats. High-level summaries of these audits should be sent to your institution, with the inclusion of any risk remediation plans.
- □ Simulations of business continuity plans are annually performed to confirm the appropriate planning and budgeting has been conducted.
- □ Breach simulation tests are performed to ensure all areas of the organization are prepared to quickly and effectively respond to any security incident that may occur.
- □ Cyberattack simulation tests, or penetration tests, are conducted to help discover weaknesses that may be exploited by a cybercriminal. High-level summaries of these tests should be sent to your institution, with the inclusion of any risk remediation plans.

Vendor Data Breach Preparation & Education Checklist

PREVENT OR RESPOND TO A BREACH BY IMPLEMENTING THESE:

□ Systems are in place 24/7/365 to monitor suspicious patterns and immediately alert of any unauthorized access attempts being made against any part of a vendor's network or servers, or anything else used to process or transport your data.

□ An incident response plan is built with your institution to collaboratively mitigate any potential exposure.

- This plan should establish required actions for responding rapidly and effectively to any confirmed security breach or potential data compromise.
- This plan should also include escalation procedures for both parties.

□ Training programs are provided to educate employees on data risks, vulnerabilities, and red flags.

□ Ensure that your bond solution offers broad protection.

To learn more about Allied Solutions' data protection practices visit our website: alliedsolutions.net/trust-center.