A blue and black logo

Description automatically generated

**VENDOR DATA SECURITY QUESTIONNAIRE**

## GENERAL INFORMATION

Name of Vendor:Click or tap here to enter text.

­­­­­­Vendor is a(an): Individual Corporation  Partnership Other ­­­­­­­­­­­­­­­Click or tap here to enter text.

## SAFEGAURDS ON LACERA CONFIDENTIAL INFORMATION

1. Does / will the vendor hold LACERA Confidential or LACERA member PII information? Yes No

­If yes, please provide details. Response: Click or tap here to enter text.

1. Is LACERA information physically or virtually segregated from the vendor and its vendor’s other clients? Yes No

­If yes, please provide details. Response: Click or tap here to enter text.

1. Provide brief description on the type of connection (encryption and authentication) for information exchange between LACERA and the vendor organization. Response: Click or tap here to enter text.
2. Is LACERA information encrypted at rest? Yes No
3. Describe the teams within vendor’s organization that have access to the LACERA information:

Response: Click or tap here to enter text.

1. Are vendor’s production and test/development areas separated? Yes No

­If yes, please provide brief details. Response: Click or tap here to enter text.

## VENDOR Security and INCIDENT RESPONSE PROGRAM

1. Provide documentation on vendor Information Security Policy and Incident Response programs.

Response: Click or tap here to enter text.

1. Provide confirmation and/or attestation to a 72-hour breach notification.

Response: Click or tap here to enter text.

1. Vendor agrees to a periodic review for compliance to LACERA policies and security requirements. Yes No

Response: Click or tap here to enter text.

## VENDOR PENETRATION TEST AND SOC2 REPORTS

1. Has the vendor completed a Penetration test? Yes No Provide summary report of the latest Penetration Test. Response: Click or tap here to enter text.
2. Has the vendor completed an Independent Service Auditors compliance exam such as SOC 2? Yes No

If yes, please provide the latest audit report and proceed to the last section of this questionnaire sign and date the document. Response: Click or tap here to enter text.

If compliance report has not been completed, please proceed to the next sections.

## EMAIL SECURITY CONTROLS

If the answer to any question in this section is “No”, please provide additional details in the “Additional Comments” section.

1. Do you tag external emails to alert employees that the message originated from outside the organization? Yes No
2. Do you pre-screen emails for potentially malicious attachments and links? Yes No

If “Yes”, complete the following:

Provide your email security provider. Response: Click or tap here to enter text.

Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine

if they are malicious. Yes No

1. Have you implemented any of the following to protect against phishing messages? (check all that apply):

Sender Policy Framework (SPF)

DomainKeys Identified Mail (DKIM)

Domain-based Message Authentication, Reporting & Conformance (DMARC)

None of the above

1. Can your users access email through a web application or a non-corporate device? Yes No

If “Yes”, do you enforce Multi-Factor Authentication (MFA)? Yes No

1. Do you use Office 365 in your organization? Yes No

If “Yes”, do you use the Office 365 Advanced Threat Protection add-on? Yes No

ADDITIONAL COMMENTS (Use this space to explain any “No” answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)

Response: Click or tap here to enter text.

## INTERNAL SECURITY

If the answer to any question in this section is “No”, please provide additional details in the “Additional Comments” section.

1. Do you use a cloud provider to store data or host applications? Yes No

If “Yes”, provide the name of the cloud provider. Response: Click or tap here to enter text.

1. Do you use MFA to secure all cloud provider services that you utilize (e.g. Microsoft Azure)? Yes No
2. Do you encrypt all sensitive and confidential information? Yes No

If “No”, are the following compensating controls in place:

1. Segregation of servers that store sensitive and confidential information? Yes No
2. Access control with role-based assignments? Yes No
3. Do you allow remote access to your network? Yes No

If “Yes”, do you use MFA to secure all remote access to your network? Yes No

1. Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise? Yes No

If “Yes”, provide name of your NGAV provider. Response: Click or tap here to enter text.

1. Do you use an endpoint detection and response (EDR) tool that includes monitoring and logging? Yes No

If “Yes”, provide name of your EDR provider. Response: Click or tap here to enter text.

1. Do you manage privileged accounts using privileged account management software (PAM) Yes No

If “Yes”, provide name of your PAM provider. Response: Click or tap here to enter text.

1. Do you roll out a hardened baseline configuration across servers, laptops, desktops? Yes No
2. Do you record and track all software and hardware assets deployed across your organization? Yes No
3. How frequently do you install critical and high severity patches across your enterprise? Yes No
4. Do you use a protective DNS service (PDNS) to block access to known malicious websites? Yes No
5. Do you implement PowerShell best practices as outlined by Microsoft? Yes No
6. Do you utilize a Security Information and Event Management system (SIEM)? Yes No
7. Do you utilize a Security Operations Center (SOC)? Yes No

If “Yes”, complete the following:

Is your SOC monitored 24 hours a day, 7 days a week? Yes No

If your SOC is outsourced, provide name of your SOC provider. Response: Click or tap here to enter text.

1. Do you have an established Third Party Risk Management Program (TPRM)? Yes No

ADDITIONAL COMMENTS (Use this space to explain any “No” answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)

Response: Click or tap here to enter text.

## PHISHING CONTROLS

1. Do all employees at your company complete mandatory cybersecurity training? Yes No

If “Yes”, does such training include phishing simulation? Yes No

## BACKUP AND RECOVERY

If the answer to any question in this section is “No”, please provide additional details in the “Additional Comments” section.

Do you use a data backup solution? Yes No

If “Yes”:

1. Which best describes your data backup solution?

Backups are kept locally but separate from your network (offline/air-gapped backup solution).

Backups are kept in a dedicated cloud backup service.

You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive).

1. Check all that apply:

Your backups are encrypted

You have immutable backups

Your backups are secured with different access credentials from other administrator credentials

You utilize MFA for both internal and external access to your backups

You have tested the successful restoration and recovery of key server configurations and data from backups

You are able to test the integrity of backups prior to restoration to ensure that they are free of malware

1. Estimated amount of time it will take to restore essential functions using backups in the event of a widespread malware or ransomware attack within your network.

0-24 hours 1-3 days 4-6 days 1 week or longer

1. Has the vendor completed Disaster Recovery testing? Yes No

If yes, please provide RTO/RPO objectives (Recovery Time Objective or Recovery Point Objectives).

Response: Click or tap here to enter text.

ADDITIONAL COMMENTS (Use this space to explain any “No” answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)

Response: Click or tap here to enter text.

## INCIDENTS

1. Has the vendor received any complaints or written demands or been a **subject in litigation** involving matters of privacy injury, breach of private information, network security, defamation, content infringement, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks or the ability of third parties to rely on the vendor’s network? Yes No
2. Has the vendor been the subject of any government action, investigation, or other proceedings regarding any alleged violation of privacy law or regulation? Yes No
3. Has the vendor notified customers, clients or any third party of any security breach or privacy breach? Yes No

ADDITIONAL COMMENTS (Use this space to explain any “Yes” answers in the above section.)

Response: Click or tap here to enter text.

## CERTIFICATION, CONSENT AND SIGNATURE

The vendor has read the foregoing and understands that completion of this questionnaire does not bind LACERA to procure vendor’s products or services. I hereby declare that, after inquiry, the above statements and particulars are true, and I have not suppressed or misstated any material fact.

Print or Type Vendor’s Name: Click or tap here to enter text. Title of Signee: Click or tap here to enter text.

Signature of Signee: Click or tap here to enter text. Date signed: Click or tap here to enter text.