SUPERIOR COURT OF CALIFORNIA
CONTRA COSTA COUNTY

Disaster Recovery & Business Continuity Statement of Work

The Superior Court of California, County of Contra Costa (the Court) received all the following questions concerning the Phase 1 of the definition, author, and implementation of the Business Continuity/Disaster Recovery ("BC/DR") Plan of the Court's network from qualified vendors prior to the June 19, 2023, submission deadline.

Please see all questions and responses below provided by the Court's IT Infrastructure Manager:

1. Do you currently have a Business Continuity in place now that we would be updating or are we creating a BCP from scratch?
    a. *No, we do not have a Business Continuity in place.*

2. Do you have a Disaster Recovery plan in place now?
    a. *Yes, only for operational purposes.*

3. Do you have a documented incident response plan?
    a. *No, we do not have an incident response plan.*

4. Do you have a documented cyber security policy?
    a. *No, we do not have a cybersecurity policy.*

5. Do you have a documented communication plan?
    a. *No, we do not have a documented communication plan.*

6. Do you have an updated IT asset inventory?
    a. *Yes, we have an updated IT asset inventory in Solarwind.*

7. How many servers are involved?
    a. *There are 195 servers, and most are virtualized.*

8. How many ends points?
    a. *There are approximately 700 endpoints.*

9. How many critical applications are in scope?
    a. *The mission-critical applications are: Tyler Odyssey (Enterprise Justice), Tyler Odyssey (Enterprise Justice) public portal, Thomson Reuters C-Track, Thomson Reuters C-Track Portal and the Jury Duty System.*

10. How many applications are SaaS vs how many are hosted on prem?
    a. *Most applications are hosted on premises and less than 10 are SaaS.*

11. How many locations, offices and facilities do you have outside of the 5 listed in the RFP?
    a. *There are 9 locations: 5 in Martinez (Taylor, Bray, Spinetta, Annex, and Juvenile Hall), Walnut Creek, Richmond, Pittsburg, and Concord.*

12. How many remote workers do you have?
    a. *We have some (< 20) remote workers.*

13. Where are the Data Centers?
    a. *There are 2 data centers.*

Disaster Recovery & Business Continuity Statement of Work

14. Do you run vulnerability scans and penetration tests?
    a. *No, we currently do not run penetration tests. We run Endpoints scans regularly with a hosted application.*

15. How often do you run vulnerability scans and penetration tests?
    a. *No, we currently do not run penetration tests. We run Endpoints scans daily with a hosted application.*

16. Do you have an incident response plan and communication plan?
    a. *No, we do not have an incident response plan and communication plan.*

17. Have you completed a Business Impact Analysis that ranks your applications?
    a. *We have not completed any BIA's ranking our applications.*

18. Do you have recovery time objective (RTO) and recovery point objective (RPO) defined for applications?
    a. *No, we do not have RTO or RPO defined for applications.*

19. Is there existing documentation on application dependencies?
    a. *No, we do not have documentation on application dependencies.*

20. What regulatory or compliance requirements do you adhere to?
    a. *We adhere to the policies & procedures of the California Judicial Council.*

21. What is the current recovery strategy?
    a. *We currently use a local backup appliance with SaaS backup as our recovery strategy.*

22. Do you run DR tests? How often?
    a. *No, we currently do not run DR tests.*

23. Do you test backup restores? How often?
    a. *No, we currently do not test backup restores methodology.*

24. Do you have any step by step guides (runbooks) that are used during DR failure testing or would we be developing from scratch?
    a. *No, we currently do not have any DR runbooks.*