VAIXUS
Technologies

REM-2026-001

Remediation Plan

Full Infrastructure Authentication Alignment

Prepared for: [Sample Organization] (Synthetic Engagement)
Prepared by: Vaixus Technologies
Publication Date: July 02, 2026
Document Version: 1.0
Classification: Confidential Sample Deliverable

LABORATORY-ENGINEERED CONSULTING SIMULATION

This report is a fictional, laboratory-generated case study prepared for portfolio and methodology-demonstration purposes. It does not describe a real client, a real organization, or an actual engagement.

Synthetic Demonstration Notice

This report is a representative demonstration of the Vaixus remediation methodology. Organization names, domains, identifiers, and execution timelines have been synthesized to illustrate a typical enterprise engagement. Representative evidence shown throughout this document does not originate from an actual client. The remediation process, rollback logic, and technical instructions reflect the exact standards used during production consulting engagements.

Document Control

Field	Value
Document Title	REM-2026-001 — Remediation Plan
Document Version	1.0
Publication Date	July 02, 2026
Prepared By	Vaixus Technologies
Review Status	Final — Approved for Publication
Classification	Confidential Sample Deliverable
Engagement Type	Laboratory-Engineered Consulting Simulation

Revision History

Version	Date	Author	Summary of Changes
1.0	July 02, 2026	Soorya S V	Final release of remediation strategy.

Table of Contents

Synthetic Demonstration Notice 2
Document Control 2
Table of Contents 3
1. Remediation Objectives 4
2. Current State Summary 4
3. Environment Inventory 4
4. Remediation Scope 4
5. Dependency Mapping 5
6. Change Register 5
7. Implementation Phases 6
8. Rollback Procedures 7
9. Validation Plan 7
10. Consultant Conclusion 7

1. Remediation Objectives

Objective	Description	Type
SPF Optimization	Restructure SPF records to eliminate RFC 7208 PermError by reducing lookups below 10.	Primary
DKIM Alignment	Provision and activate DKIM cryptographic signing for the Salesforce CRM environment.	Primary
DMARC Escalation	Escalate root domain DMARC policy from p=none to p=quarantine.	Primary
MTA-STS Deployment	Deploy strict TLS transit encryption via an MTA-STS policy.	Secondary

SCOPE NOTE — This Remediation Plan focuses strictly on DNS, protocol, and authentication engineering. It does not include inbox placement guarantees, penetration testing, or marketing strategy.

2. Current State Summary

Based on the Infrastructure Assessment (ASR-2026-001), the primary domain currently exceeds the RFC 7208 SPF lookup limit (11/10) due to nested third-party includes, creating severe deliverability volatility. Furthermore, Salesforce CRM traffic is unsigned, and the root DMARC policy is stalled at monitoring (p=none), leaving the domain vulnerable to exact-domain spoofing. This plan outlines the exact technical steps required to seal these vulnerabilities and achieve strict authentication alignment.

3. Environment Inventory

Domain	DNS Provider	Mail Platform	Third-Party Platforms	Auth Status	Risk
[Demonstration Domain]	Cloudflare	Google Workspace	Salesforce, SendGrid	Misaligned	High

4. Remediation Scope

In Scope

- SPF record restructuring and macro-flattening deployment
- DKIM selector configuration within Salesforce and Cloudflare
- DMARC policy escalation and aggregate reporting setup

- Monitoring setup and post-implementation validation

Out of Scope

- Email content review and CRM data hygiene
- Deliverability guarantees for third-party blacklists

5. Dependency Mapping

Dependency	System	Owner	Impact if Incorrect	Risk
DNS Admin Access	Cloudflare	Client IT	Inability to deploy records	High
Salesforce Admin	CRM Portal	Sales Ops	Unable to generate DKIM keys	High

6. Change Register

CHANGE CONTROL — All changes require explicit client authorisation before implementation. No production changes will be made without confirmed approval from an authorised contact.

Change ID	Description	Affected Domain	Risk Level	Status
C-001	Deploy Flattened SPF Record	[Demonstration Domain]	High	Planned
C-002	Publish Salesforce DKIM CNAMEs	[Demonstration Domain]	Medium	Planned
C-003	Update DMARC to p=quarantine	[Demonstration Domain]	High	Planned

6.1 Pre-Implementation Checklist

- [✓] DNS administrative access confirmed
- [✓] Current BIND zone file backup exported
- [✓] Rollback procedures documented
- [ ] Client approval received for Change Window

6.2 Proposed Change Window

Field	Value
Implementation Date	July 05, 2026
Change Window	22:00 IST - 00:00 IST

Field	Value
Time Zone	Indian Standard Time (UTC+5:30)
Downtime Tolerance	Zero downtime expected. Changes are propagation-dependent.

7. Implementation Phases

Phase	Owner	Estimated Duration	Exit Criteria
Phase 1: Preparation	Vaixus	24 Hours prior	TTL lowered, backups secured
Phase 2: Execution	Vaixus	2 Hours	Records deployed in Cloudflare
Phase 3: Validation	Vaixus	24-48 Hours	Propagation complete, tests passed

Phase 1 – Preparation

Field	Value
Objectives	Reduce TTL to minimize rollback time. Secure current configurations.
Changes	Lower SPF and DMARC TXT record TTL to 300 seconds (5 minutes).
Success Criteria	Zone file successfully backed up to secure local storage.

Phase 2 – Execution (Authentication Changes)

Field	Value
Objectives	Deploy new records to eliminate PermError and sign CRM mail.
C-001 Actions	Replace existing SPF record. Deploy optimized SPF authorization structure for SendGrid/Mailchimp.
C-002 Actions	Provision DKIM key pair in Salesforce. Publish CNAMEs in Cloudflare. Activate.
C-003 Actions	Modify _dmarc TXT record from p=none to p=quarantine; pct=100.

Phase 3 – Monitoring and Validation

Field	Value
Objectives	Confirm cryptographic alignment and successful mail routing.
Activities	Send test triggers from Google Workspace and Salesforce CRM.
Success Criteria	Raw headers indicate SPF=Pass, DKIM=Pass, DMARC=Pass.

8. Rollback Procedures

ROLLBACK — If critical mail flow disruption is detected, immediate rollback protocol is initiated. TTL reduction in Phase 1 ensures 5-minute recovery.

Change ID	Rollback Trigger	Rollback Steps	Owner
C-001 (SPF)	Legitimate internal mail hard-bouncing	Restore legacy SPF TXT record via BIND import	Vaixus
C-003 (DMARC)	Mass quarantine of valid CRM mail	Revert _dmarc TXT to p=none	Vaixus

9. Validation Plan

Validation Category	Verification Method	Evidence Required
SPF Validation	CLI `dig TXT` command	Terminal output showing < 10 lookups
DKIM Validation	Salesforce UI Status + Header Auth	Screenshot of Active status + Headers
DMARC Validation	RUA XML Log Parsing	JSON excerpt showing DMARC=Pass

10. Consultant Conclusion

This remediation plan surgically addresses the critical vulnerabilities identified during the assessment phase. The planned implementation is designed to minimize operational disruption during the designated off-peak window. Temporary propagation delays may occur depending on DNS behavior, ultimately resulting in an immediate upgrade to strict DMARC enforcement and improved inbox placement for CRM communications.

RECOMMENDATION — Proceed with Remediation. Implementation Subject to Customer Approval.