

[Your Company Letterhead]

[Date]

[Recipient Name]

[Recipient Title]

[Recipient Company]

[Recipient Address]

[City, State, Zip Code]

Subject: Guidance for DKIM Deployment

Dear [Recipient Name],

I hope this message finds you well. As we move forward with enhancing our email security and deliverability, I am writing to provide guidance on the deployment of DomainKeys Identified Mail (DKIM) across our domains.

****1. DKIM Overview****

DKIM is a method that allows us to sign our emails digitally, ensuring integrity and authenticity. This helps authenticate the sender's identity and protects our emails from being altered in transit.

****2. Implementation Steps****

- ****Key Generation:**** Generate a DKIM key pair (public and private keys).
- ****DNS Configuration:**** Publish the public key in our DNS records as a TXT record.
- ****Email Server Configuration:**** Configure our email server to sign outgoing messages with the private key.

****3. Record Example****

To publish the DKIM public key, the TXT record should look like this:

```\n

```
selector._domainkey.yourdomain.com. IN TXT "v=DKIM1; k=rsa;\n p=yourpublickey"\n```\n
```

**\*\*4. Testing and Validation\*\***

After deployment, utilize tools such as DKIM Validator or MXToolbox to verify the DKIM signing and ensure emails are being properly authenticated.

**\*\*5. Monitoring and Maintenance\*\***

Regularly monitor our DKIM implementation and update keys as necessary to maintain security levels.

Please feel free to reach out if you have any questions or require further clarification on any of the steps mentioned.

Thank you for your attention to this important matter.

Sincerely,

[Your Name]

[Your Title]

[Your Company]

[Your Phone Number]

[Your Email Address]