DMARC Phased Rollout Worksheet

Use this worksheet to track your domain's move from monitoring (p=none) to full enforcement (p=reject). It pairs with the DMARC blog series: publish DMARC at p=none, read your aggregate reports, fix alignment issues, then tighten your policy in stages.

Domain: _____

Monitoring started (date): _____

Target enforcement date: _____

Owner: _____

Phase 1: Monitoring (p=none)

- ☐ SPF record published for the domain.
- ☐ DKIM signing enabled and the DKIM DNS record published.
- ☐ DMARC record published at p=none with an rua= address for aggregate reports.
  SPF and DKIM should be working for at least 48 hours before you publish the DMARC record.
- ☐ Aggregate reports are arriving and being reviewed regularly.
- ☐ Reviewed reports for at least 2–4 weeks to capture regular and periodic senders (e.g. monthly billing runs).

Sender inventory

List every source sending mail as your domain. For each one, note whether it passes SPF and DKIM with alignment, and whether/when you fixed it.

Source / System	SPF	DKIM	Fixed?	Date
Primary mail server				
Marketing platform				
CRM / helpdesk tool				
Billing / invoicing system				

Phase 2: Quarantine (p=quarantine)

- [ ] All legitimate senders pass SPF or DKIM with alignment, or have a documented plan to.
- [ ] No unexplained failures remain in recent reports.
- [ ] DMARC record updated to p=quarantine; pct=25.
  Date: _____
- [ ] Monitored for 1–2 weeks at pct=25 with no legitimate mail affected.
- [ ] Increased to pct=50.
  Date: _____
- [ ] Increased to pct=100 (full quarantine).
  Date: _____

Phase 3: Reject (p=reject)

- [ ] Reviewed reports at full quarantine and confirmed no legitimate mail is failing.
- [ ] DMARC record updated to p=reject; pct=25.
  Date: _____
- [ ] Monitored for 1–2 weeks at pct=25 with no legitimate mail affected.
- [ ] Increased to pct=50.
  Date: _____
- [ ] Increased to pct=100 (full reject).
  Date: _____
- [ ] Domain is now fully protected against direct-domain spoofing.

Notes