DMARC policy

The question

DMARC needs a rollout owner

A published policy can request monitoring, quarantine or rejection. The right next step depends on evidence from legitimate mail.

01 Understand

02 Observe

03 Verify

A practical briefing for the people who own your domain.

DMARC policy

The mechanism

Connect the visible domain

DMARC needs a successful SPF or DKIM result aligned with the domain in the From address. Either mechanism can satisfy it.

01 Visible From domain

↓

02 Aligned SPF or DKIM pass

↓

03 DMARC result and policy

Either aligned SPF or aligned DKIM can satisfy DMARC. Both mechanisms do not have to pass.

DMARC policy

The evidence

We measure published policy

> The check uses bounded DNS discovery and selected policy settings. Message alignment, report review and recipient enforcement need separate evidence.

PUT THE OBSERVATION IN CONTEXT

- **Public signal**
- **Service context**
- **Operational validation**

Use the finding to start an owned review.

DMARC policy

The handoff

Validate before tightening

Inventory senders and review message results. Let email and DNS owners agree a staged change with delivery monitoring.

BRING THE RIGHT OWNERS TOGETHER

01 Email operations and business service owners

02 Email security owner with DNS administrator

DMARC policy

Your checklist

Use the DMARC review checklist

- ✓ Confirm senders and indirect flows
- ✓ Review current guidance
- ✓ Check subdomain policy
- ✓ Document recovery

> Read the full explainer before changing enforcement.
>
> **/learn/dmarc**