SNAPLEADS / LAB

Outbound Deliverability Preflight Checklist

1. Sender identity and authentication

BEFORE FIRST SEND

- [ ] **SPF is singular and intentional**

  Confirm the domain publishes one SPF policy and that every legitimate sender is represented without blindly stacking vendor records.

- [ ] **DKIM signs the message path you are actually testing**

  Inspect the DKIM-Signature header and selector; a DNS record existing somewhere is not the same as the message verifying.

- [ ] **DMARC exists and alignment is understood**

  For a monitoring rollout, p=none can be appropriate. Check alignment between the visible From domain and SPF or DKIM authentication.

- [ ] **Authoritative DNS is the source of truth**

  After nameserver or provider changes, query the authoritative path instead of trusting a stale dashboard screenshot.

- [ ] **TLS and reverse DNS are reviewed where applicable**

  If you operate sending infrastructure, confirm the transport and DNS requirements relevant to that path.

2026 DMARC note

RFC 9989 is the current DMARC base specification. Aggregate reporting is RFC 9990; failure reporting is RFC 9991. Older RFC 7489 is no longer the current base reference.

Outbound Deliverability Preflight Checklist

2. List hygiene and send envelope

CONTROL EXPOSURE

- [ ] **Normalize and deduplicate recipients**
  Trim whitespace, normalize addresses, and prevent the same lead from being assigned to multiple mailboxes.
- [ ] **Apply global hard-bounce suppression**
  A permanent failure belongs to recipient state, not to one campaign. Check suppression immediately before every send.
- [ ] **Record verification date and method**
  A list can become stale. Do not preserve only a permanent-looking verified=true flag.
- [ ] **Separate catch-all and role-address risk**
  Catch-all and shared inboxes are classifications, not confirmed person-level validity.
- [ ] **Use a planned envelope, not a magic limit**
  Track planned vs actual sends. Increase only after the prior step has stable authentication and recipient signals.
- [ ] **Spread work so state can update**
  Allow replies, bounces and suppressions to change the queue before later touches are emitted.

Illustrative ramp

A pattern such as 5 -> 9 -> 18 -> 31 -> 57 can be used as an operating example, but the exact counts are not provider guarantees. Health gates decide whether the next step happens.

SNAPLEADS / LAB

Outbound Deliverability Preflight Checklist

3. Replies, IMAP state and incident recovery

BEFORE FOLLOW-UP

- [ ] **Reply detection is idempotent**

  Reprocessing the same message must not create duplicate reply events or duplicate cancellations.

- [ ] **Unread state is preserved when required**

  For IMAP inspection that should not set Seen, use the appropriate BODY.PEEK behavior described in RFC 9051.

- [ ] **UID and UIDVALIDITY are stored for durable message state**

  Do not persist message sequence numbers as long-lived identifiers.

- [ ] **Out-of-office responses have their own class**

  Stop immediate follow-up without counting an automatic response as a positive human reply.

- [ ] **2.x.x, 4.x.x and 5.x.x outcomes are not blended**

  Permanent and transient delivery status classes should trigger different queue actions.

- [ ] **Incident changes are one-at-a-time**

  If authentication, list quality or volume becomes abnormal, freeze unrelated experiments and preserve the timeline.

Primary references

Google Gmail Email sender guidelines and FAQ; RFC 7208 (SPF); RFC 6376 (DKIM); RFC 9989/9990/9991 (DMARC); RFC 9051 (IMAP4rev2); RFC 3463 (enhanced status codes).