

Chapter 20: The Inbox Is Infrastructure

Table Reference

Every table from this chapter, with what it's for and how to actually use it.

Email Authentication Setup Record

Field	Value
SPF Record Location	DNS TXT record at root domain
DKIM Selector(s)	
DMARC Policy	☐ p=none ☐ p=quarantine ☐ p=reject
DMARC Reporting Email	
DMARC Report Tool	e.g. Postmaster Tools, dmarcian, Valimail
Last Reviewed	
Current Status	☐ Not Configured ☐ SPF/DKIM Only ☐ DMARC p=none ☐ DMARC p=reject

Description: A worksheet for documenting your actual SPF, DKIM, and DMARC configuration alongside the field definitions.

How to use it: Fill in with your own domain's real authentication records – this becomes your single source of truth when troubleshooting deliverability issues or briefing IT/Security.

Reputation Monitoring Tools

Tool / Source	What It Measures	How Often to Check
Google Postmaster Tools	Domain reputation, spam rate, authentication pass rates for Gmail recipients	Weekly
Microsoft SNDS	IP reputation, complaint rates, trap hits for Outlook / Hotmail recipients	Weekly
Validity / 250ok /	Inbox placement rate across ISPs, blacklist	Per major send

Tool / Source	What It Measures	How Often to Check
Everest	monitoring, engagement data	
Litmus / Email on Acid	Rendering previews, spam filter testing, inbox placement simulation	Before each campaign
MXToolbox / Blacklist Check	Blacklist status across major RBLs (CBL, Spamhaus, SORBS)	Monthly or on deliverability drop

Description: The specific tools (Google Postmaster, Microsoft SNDS, Validity/250ok, and others) for monitoring sender reputation, with what each measures and how often to check it.

How to use it: Use as a setup checklist to confirm you're actually monitoring reputation through every major mailbox provider, not just the one you happen to check.

Reputation Alert Thresholds

Metric	Healthy Target	Alert Threshold	Action if Breached
Spam complaint rate (Gmail)	< 0.10%	>= 0.10%	Pause sends; audit recent list segments and suppression
Spam complaint rate (overall)	< 0.08%	>= 0.08%	Review content, frequency, and consent recency
Hard bounce rate	< 2%	>= 2%	Audit list quality; run enrichment or validation
Soft bounce rate	< 5%	>= 8%	Check sending volume, IP reputation, and content triggers
Inbox placement rate	>= 90%	< 80%	Run spam filter audit; check authentication and content
Unsubscribe rate per send	< 0.2%	>= 0.5%	Review send frequency, relevance, and list segmentation
DMARC pass rate	>= 98%	< 95%	Audit sending services; check for unauthorized senders

Description: Real target and alert thresholds for the metrics that actually predict deliverability trouble (spam complaint rate, hard bounce rate, and others), with the specific action to take if breached.

How to use it: Use as a build spec for automated deliverability alerting, so a reputation problem triggers action at the threshold, not after inbox placement has already collapsed.

Bounce & Suppression Policy

Type	Definition	Required Action	Suppression Scope
Hard Bounce	Permanent failure – invalid address, domain does not exist, or recipient rejected	Suppress immediately and permanently; flag in CRM for data hygiene	All marketing sends
Soft Bounce (3+ consecutive)	Temporary failure (mailbox full, server busy) persisting across 3+ attempts	Suppress from active sends; re-validate address before reactivating	Active campaign sends
Global Unsubscribe	Contact opted out via unsubscribe link or preference center	Suppress from all non-transactional sends; honor within 10 business days; sync MAP and CRM	All marketing sends globally
Spam Complaint	Contact marked email as spam via ISP feedback loop	Suppress immediately; do not re-engage without explicit re-opt-in; flag in CRM	All sends; flag for data review
Competitive / DNC	Known competitor employee or company-level DNC	Suppress from all outbound marketing and paid retargeting	All sends and paid audiences
Manual Admin Suppress	Legal hold, contractual restriction, or executive DNC request	Log request with reason and requester; apply in MAP suppression list	All sends; audit annually

Description: Defines each bounce/suppression type (hard bounce, soft bounce, global unsubscribe, and others) with the required action and how broadly it applies.

How to use it: Use as a build spec for your MAP's suppression logic, so every bounce type is handled consistently instead of case-by-case.

Engagement Tier Definitions

Engagement Tier	Definition	Recommended Frequency	MarkOps Action
Highly Engaged	Opened or clicked in last 30 days	Full frequency – all relevant programs	No action; prioritize in targeting
Engaged	Opened or clicked in last 31-90 days	Full frequency	Monitor for downward trend

Engagement Tier	Definition	Recommended Frequency	MarkOps Action
Lapsing	No open or click in 91-180 days	Reduced – 1-2 sends/month max	Enroll in re-engagement sequence; flag for content review
Dormant	No open or click in 181-365 days	Re-engagement sequence only	Send win-back sequence (max 3 emails); suppress if no response
Sunset	No engagement in 12+ months; no win-back response	Suppress from all marketing	Move to suppression list; retain record in CRM with suppression flag

Description: Defines each engagement tier (Highly Engaged through Lapsing) with its recommended send frequency and the action MarkOps should take.

How to use it: Use as a segmentation framework for your own send-frequency rules, tying actual list health to how often someone gets emailed.

Quarterly List Health Tracker

Health Metric	Q1	Q2	Q3	Q4 / Notes
Total active database size				
Highly Engaged (%)				Target: >= 30%
Lapsing (%)				Alert: >= 25%
Dormant (%)				Alert: >= 20%
Sunset / suppressed (total)				
Hard bounce rate (last 90 days)				Target: < 2%
Unsubscribe rate (last 90 days)				Target: < 0.2%
Spam complaint rate (last 90 days)				Target: < 0.10%
Re-engagement sequence response rate				Benchmark: 5-10%

Description: A blank quarterly tracker for logging list health metrics against the targets and alert thresholds defined earlier in this chapter.

How to use it: Populate each quarter to catch list health degrading gradually, well before it becomes a deliverability crisis.

IP Warmup Schedule

Week	Daily Send Volume	Audience Segment	Notes
Week 1	250-500/day	Highest-engagement contacts (opened last 30 days)	Monitor complaint and bounce rates daily; pause if either exceeds alert threshold
Week 2	500-1,000/day	Engaged contacts (opened last 60 days)	Check inbox placement rate before increasing volume
Week 3	1,000-5,000/day	Active database (opened last 90 days)	Ensure DMARC pass rate >= 98% before proceeding
Week 4	5,000-10,000/day	Full active + lapsing segments	Run seed list test to confirm inbox placement across major ISPs
Week 5+	Ramp to full volume	Full sendable database	Do not exceed 20% volume increase per week once at scale; monitor weekly

Description: A real, worked warmup schedule showing how to ramp send volume gradually on a new sending IP or domain.

How to use it: Use as the literal schedule when warming up a new IP or domain, adjusting volumes based on your own list size and engagement data.
