

Inbound Email Security & Acceptance Policy

Protecting customers, communications and data through enforceable authentication and attachment controls.

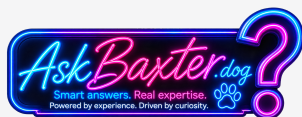
Check your email security configuration



Togethia MailCheck

Identify problems with your email system. You can choose to send the test results directly to Togethia for examination.

<https://togethia.tools/mailcheck/>



Ask Baxter — Video explanation

A straightforward explanation of SPF, DKIM and DMARC, and why correctly configured email authentication matters.

<https://askbaxter.dog/videos/dkim-spf-dmarc-explained/>

1. Our approach

Email remains a major route for phishing, impersonation, malware and fraud. First and Ten Productions adopts stringent inbound email controls and does not relax mandatory security checks simply to accommodate a sender's incorrect configuration. Delivery by another provider is not evidence that a message satisfies First and Ten Productions' acceptance criteria.

Responsibility for maintaining the sending service, published DNS records and authentication configuration rests with the sending organisation and its chosen provider. First and Ten Productions' requirements may exceed minimum interoperability standards and are an intentionally stricter local acceptance policy.

2. Sender Policy Framework (SPF)

When a sending domain publishes an SPF policy, First and Ten Productions evaluates the connecting IP address against the SPF identity used in the SMTP transaction (normally MAIL FROM; HELO where appropriate). An explicit SPF fail is a hard reject, regardless of the DKIM or DMARC result. An aligned DKIM pass does not override this local SPF rejection rule.

SPF softfail, neutral, none and permanent errors are evaluated under separate operational rules. Temporary DNS or evaluation errors may result in an SMTP 4xx deferral rather than a permanent rejection. SPF does not by itself authenticate the visible From header, and forwarding may cause legitimate mail to fail SPF; First and Ten Productions nevertheless chooses to enforce explicit fail results.

3. DomainKeys Identified Mail (DKIM)

When DKIM signing is present or required, First and Ten Productions requires at least one cryptographically valid DKIM signature aligned with the visible RFC5322.From domain. An invalid signature, or a signature that authenticates only an unrelated domain, does not satisfy the policy. Where no valid aligned signature is found, the message is rejected.

Multiple signatures are evaluated independently: one invalid signature does not negate a separate valid aligned signature. Temporary DNS failures may be deferred; missing keys or cryptographic failures are permanent failures when no acceptable signature remains. Alignment is evaluated using the applicable organisational-domain rules unless a stricter requirement is specifically imposed.

For example, mail visibly sent from `excellect.co.uk` but signed only with `excellect.onmicrosoft.com` is not DKIM-aligned. Microsoft 365 can retain the initial `onmicrosoft.com` DKIM signing configuration until custom-domain signing is enabled. First and Ten Productions considers that configuration unacceptable for such correspondence.

4. Domain-based Message Authentication, Reporting and Conformance (DMARC)

DMARC is evaluated as an additional authentication and reporting signal, but it is advisory for First and Ten Productions' independent acceptance decisions. DMARC allows either aligned SPF or aligned DKIM to pass; First and Ten Productions' stricter policy may reject a message despite a DMARC pass if SPF explicitly fails or the message lacks an acceptable DKIM signature where required. A published DMARC `p=none` does not waive First and Ten Productions' controls.

5. Sending-server identity and reputation

First and Ten Productions may require forward-confirmed reverse DNS (FCrDNS): a connecting IP must resolve to a hostname whose forward DNS resolves back to that IP. Missing or inconsistent records may justify rejection. First and Ten Productions also checks selected DNS blocklists and reputation sources. A listing on any blocklist that First and Ten Productions enforces is grounds for immediate rejection. Inclusion in an arbitrary list not used by First and Ten Productions is not automatically disqualifying.

6. Attachment restrictions

First and Ten Productions rejects file types or packaging that create unacceptable execution, deception or inspection risks. These restrictions apply even if the email itself is otherwise authenticated.

Absolute prohibition: Microsoft Word `.docx` and Microsoft Excel `.xlsx` attachments are rejected without exception. Other legacy Office document types, including `.doc` and `.xls`, may also be rejected.

Executables and scripts: executable files, installers, script files and similar active content are prohibited, including when concealed within archives or renamed.

Encrypted archives: password-protected ZIP files and other encrypted attachments are rejected where their contents cannot be inspected. Passwords supplied separately do not create an automatic exception.

Legacy encapsulation: TNEF, winmail.dat, and DAT attachments used for opaque or proprietary mail encapsulation are rejected where policy applies. Unverifiable or misleading content types may also be rejected.

Double extensions: attachments with misleading or suspicious multiple extensions, such as document.docx.pdf, invoice.pdf.exe, statement.xlsx.scr or report.pdf.js, may be stripped or the message rejected. File content inspection is not limited to the visible extension.

Senders should use a safe, inspectable format acceptable to the intended recipient. Where a prohibited document format is essential to a business process, the parties should use a suitably secured alternative transfer method rather than attempting to bypass mail filtering.

7. Rejection, silent disposal and backscatter

Where feasible, First and Ten Productions rejects unacceptable mail during the SMTP transaction, returning a relevant 5xx permanent failure or 4xx temporary deferral. This gives the connected sending system responsibility for reporting delivery failure to its sender. First and Ten Productions seeks to avoid accepting a message and subsequently generating a non-delivery report to an address that could have been forged.

Backscatter explained: an attacker may forge an innocent person's address as the apparent sender of unwanted mail. If a recipient system first accepts that message and later bounces it, the non-delivery notice is delivered to the innocent person instead of the attacker. This misdirected bounce traffic is known as backscatter.

When a message has already been accepted and is subsequently determined to be dangerous or unacceptable, First and Ten Productions may quarantine or silently discard it without generating a backscatter-producing notice, where legally and operationally appropriate. Silent disposal may leave the purported sender unaware of non-delivery. It is distinct from rejecting an SMTP transaction; sending servers receiving a 5xx reply should ordinarily report failure to their own sender.

8. No automatic exceptions

Commercial importance, urgency or the fact that other providers deliver a message does not exempt it from First and Ten Productions' security controls. First and Ten Productions does not routinely whitelist senders or disable mandatory authentication checks to accommodate configuration mistakes. Where a message is rejected, the sending organisation or its mail administrator should correct the underlying fault. Any discretionary operational exceptions remain subject to First and Ten Productions' security assessment, but the .docx and .xlsx attachment prohibition has no exceptions.

9. Reporting and remediation

For rejected email, provide the full SMTP response, sending domain, approximate UTC time, recipient domain and the sending server's IP address where available. Avoid forwarding suspicious attachments as part of an investigation. Further information on SPF, DKIM and DMARC is available in First and Ten Productions' introductory video:

DKIM, SPF and DMARC explained - <https://askbaxter.dog/videos/dkim-spf-dmarc-explained/>

10. Standards and technical references

The following standards describe baseline mechanisms and behaviours; the stricter decisions in this policy are First and Ten Productions' local acceptance requirements, not claims that every RFC mandates rejection.

RFC 7208 §8.4 - SPF fail and SMTP rejection - <https://www.rfc-editor.org/rfc/rfc7208.html#section-8.4>

RFC 7208 - Sender Policy Framework - <https://www.rfc-editor.org/rfc/rfc7208.html>

RFC 6376 - DKIM signatures, verification, multiple signatures and SMTP handling - <https://www.rfc-editor.org/rfc/rfc6376.html>

RFC 7489 - DMARC alignment and policy - <https://www.rfc-editor.org/rfc/rfc7489.html>

RFC 5321 - SMTP delivery and reply semantics - <https://www.rfc-editor.org/rfc/rfc5321.html>

Microsoft documentation - DKIM configuration for custom domains - <https://learn.microsoft.com/en-us/defender-office-365/email-authentication-dkim-configure>

Policy interpretation: The term "reject" describes refusal of a message, preferably at SMTP time. "Strip" describes removal of an attachment while handling the message; "silent disposal" applies only after acceptance. Nothing in this policy guarantees delivery of an otherwise compliant message.