DMARC None or Ignore Policy

DMARC None Policy ("**p=none**")

Though they are often confused, there is a difference between a None policy and Ignore policy in DMARC. Each has a different implication and use-case.

The "**p=none**" policy within DMARC instructs receiving email servers to take no action based on the DMARC policy. It means that the DMARC policy is set to *monitor and report mode* only. Emails that fail DMARC authentication are not subjected to any specific enforcement actions such as quarantining or rejecting. Instead, domain owners receive **aggregate (RUA)** and **forensic (RUF)** reports about email authentication results. This policy is typically used for monitoring and analysis purposes during the initial deployment or testing phase of DMARC implementation.

This policy is ideal for organizations in the initial stages of DMARC implementation, allowing them to understand their email ecosystem before transitioning to more stringent policies like "**p=quarantine**" or "**p=reject**".

DMARC Ignore Policy ("**p=ignore**")

In DMARC, there is no official "**p=ignore**" policy. However, it's possible that some may use this term informally to describe a scenario where the DMARC policy is effectively ignored by the receiving email server. This could happen if there are errors in the DMARC policy syntax or if the receiving server does not properly interpret the DMARC record. In such cases, the receiving server may default to its usual email handling procedures without considering the DMARC policy.

In summary, "**p=none**" is an official DMARC policy setting that instructs receiving servers to take no action based on the DMARC policy, whereas "**p=ignore**" is not an official DMARC policy and may refer to situations where the DMARC policy is not effectively enforced, or is being verbally discussed for various reasons.

Related Topics:

- What is DMARC?
- DMARC Policy Selectors & Tags Quick Reference
- DMARC Quarantine Policy
- DMARC Reject Policy
- DMARC Policy Percentages
- DMARC RUA Reporting - Aggregate Reports (rua)
- DMARC RUF Reporting - Forensic Reports (ruf)
- DMARC Subdomain Policy (sp)
- DMARC DKIM Alignment (adkim)
- DMARC SPF Alignment (aspf)
- What is BIMI?
- What is a VMC?
- DMARC, DKIM, SPF and BIMI Info

Don't have the time or energy to learn, setup, monitor and maintain DMARC? What if you had a team of DMARC experts to do this for you?

Let us do the DMARC for you. Check out Managed DMARC Services by GlowHost.