In this article:

About DMARC Records

DMARC stands for Domain-based Message Authentication, Reporting, and Conformance - it is a DNS TXT Record that can be published for a domain to control what happens if a message fails authentication, meaning if the recipient server can't verify that the message's sender is who they say they are.

Why use DMARC Records?

A published DMARC record essentially serves two purposes:

- Tell the recipient's server to quarantine the message, reject the message, or allow the message to continue delivery into the recipient's inbox.
- Sends reports to an email address or addresses with data about all the messages seen from the domain .

Implementing DMARC is the best way to protect your email traffic against phishing and other fraudulent activity. It empowers you to ensure legitimate email is properly authenticating and that fraudulent activity appearing to come from domains under your company's control is blocked before it reaches your customers. Microsoft is looking for DMARC and gives inbox priority if it is associated wth the sending domain. This results in higher inbox placement.

Info needed to implement a DMARC record via Ascent360 and an explanation below:

Type:	TXT
Host/Name:	_DMARC.example.com
Value:	v=DMARC1; p=none; pct=100; rua=mailto:dmarc_agg@vali.email;

Host/Name = Your domain will replace the above example.com portion.
Value = For this field include the entire line, **do not omit anything**.

We have included an email address "dmarc_agg@vali.email" that utilizes a tool we have for monitoring of the records.
Please let us know at support@ascent360.com if you are adding or changing your DMARC records so we can ensure it is also set up for monitori

We recommend using a search engine to fully verify how your web host implements DMARC records.