Including Salsa Labs Sender Policy In Your SPF Records

What is SPF?
- SPF stands for Sender Policy Framework.
- SPF is an open standard, defined in IETF RFC 4408, which provides domain owners a method for preventing sender address forgery by protecting an email message's envelope sender address, or return-path.
- The domain admin enters an SPF record as a TXT record into their DNS zone file specifying which machines are allowed to send mail from their domain.
- When a recipient mail server receives an email claiming, via its return-path, to come from your domain, it can verify this by checking the domain shown in the return-path against the policy published in your SPF record. If the message fails this check, i.e., if the envelope sender address does not fall within the scope specified in your SPF record, then it can be considered a forgery and dealt with accordingly.
- Since spam and forged email is caught by recipient spam filters that check SPF records, this enhances the reputation of your domain and improves the deliverability of your email.

Implementation
- Organizations that do not currently have an SPF record in their DNS should add one. The format varies somewhat between various DNS platforms – please consult your specific documentation for how to enter an SPF record as a TXT record – but it should look something like:

```
yourdomain.org. TXT "v=spf1 mx include:salsalabs.net ~all"
```

- Organizations which already have an SPF record in their DNS should insert `include:salsalabs.net` into their current configuration, just before the "all" mechanism. This tells the SPF record requestor to look up the record for salsalabs.net, and include that information in the organization's SPF response.

Syntax
- Below is a typical SPF record, and a breakdown of what each component of the SPF string does:

```
"v=spf1 mx include:salsalabs.net ~all"
```
  - `v=spf1` means SPFv1 or SPF Classic, the current version of SPF. This identifies the TXT record as an SPF string.
  - `mx` is a mechanism indicating that the incoming mail servers for your domain are also permitted to send mail.
  - `include:salsalabs.net` is a mechanism indicating any server permitted to send mail from "salsalabs.com" may also send mail from your domain.
  - `~all` means that all other mail not explicitly permitted by the rest of the SPF record can be accepted but will be marked for greater scrutiny.

Additional Resources
Should IT professionals reviewing this documentation have any additional questions, please email support@salsalabs.com and make sure to reference this document in your email.