Misc infrastructure - Feature # 212: Publish a DKIM record for bitfolk.com and sign emails with it

Status:	New	**Priority:**	Low
Author:	admin	**Category:**	
Created:	2023-06-12	**Assigned to:**	
Updated:	2023-06-17	**Due date:**	
Subject:	Publish a DKIM record for bitfolk.com and sign emails with it		
Description:	DKIM records have been published and used for rt.bitfolk.com and mailman.bitfolk.com for a long time, since most human-to-human emails sent by BitFolk use those domains. BitFolk's transactional emails, however, such as invoices, reminders, alerts, etc. tend to come from @bitfolk.com addresses, which currently do not have a DKIM record. This should be remedied, and those emails signed. This has become more important because there was a recent phishing attack that forged bitfolk.com email addresses. At the time there was no DKIM record on bitfolk.com, and the SPF record was an ~all (SOFTFAIL) so there was no strong automated means to tell that the emails were not genuine. The SPF record has since been tightened up to -all, though this is on the one hand not enough and on the other hand provides no way to tell if a legitimate email has simply been forwarded. A valid DKIM signature would give another way for recipients to allowlist genuine emails.		

History

2023-06-12 00:28 - admin

- Subject changed from Publish a DKIm record for bitfolk.com and sign emails with it to Publish a DKIM record for bitfolk.com and sign emails with it

2023-06-15 11:22 - admin

bitfolk.com has had a _domainkey record published for some time, and the main outbound mail relay has been signing emails, but no DMARC policy was published.

Now publishing a "none" policy to see if there are any notable failures. There are going to be a bunch of VMs sending email as @bitfolk.com that aren't going through the main mail relay.

After these are caught and cleaned up the DMARC policy will be tightened ("reject").

2023-06-15 11:28 - admin

Amusingly this redmine VM sends email as redmine@bitfolk.com so that will need to be fixed. See issue #213

2023-06-17 08:51 - admin

Aggregate reports show that the Icinga host is sending mail as monitoring-bounces@bitfolk.com without DKIM signature, though SPF is already covered.
DKIM signatures added for this now.