Account Lockout Policy

The standard lockout policy is the following:

*Account lockout duration – 30 minutes
* Account lockout threshold – 3 invalid attempts
* Reset account lockout counter after – 30 minutes

I have changed it to the following:

*Account lockout duration – 35 minutes
* Account lockout threshold – 4 invalid attempts
* Reset account lockout counter after – 35 minutes

This gives users a greater chance to avoid accidental lockouts since the system now accepts 4 invalid attempts instead of 3 invalid attempts. I am assuming that this is a small business with IT on site. If the business were huge and IT wasn't readily available, I'd probably follow the Windows 10/15/15 recommendation (10 bad attempts, 15 minute lockout duration, 15 minute counter reset.) The account policy I created will probably prevent intrusion just as much as the standard lockout policy. Setting the lockout duration to a reasonable value will also reduce helpdesk calls. If the lockout duration is 0 (indefinite, which it's not), this can be a crippling account. To assist with the account lockout policy, I would recommend IT to review account lockout policies on the web, especially sites like the following:

https://blog.netwrix.com/2017/03/09/top-5-free-tools-for-account-lockout-troubleshooting/

There is no single account lockout configuration that works for all organizations. After several months of operation, I would probably "fine-tune" the account lockout policy so that it would better prevent accidental lockouts, denial of service attacks, and intrusion.