FLAGSHIP
STRATEGIC SERVICES, LLC

CHECKLIST

Triple Guard Security™
Best Practices Checklist

Our security experts have put together an advisory of security best practices to help protect businesses from the most common attacks they might experience. This guide aims to break down security into key categories that are easy to understand and easy to implement.

Use this checklist to ensure the highest levels of protection from all potential threats. Check in frequently to ensure practices are being enforced, passwords are being updated and security remains top of mind!

ACCOUNT SECURITY

□ Set password requirements to prevent users from choosing easily guessable passwords

- We recommend looooong vs complex passwords/passphrases
- Choose a password expiration policy that is long enough that users don't resort to writing down or reusing similar passwords frequently
- Discourage users from using unsafe passwords by enforcing the "compromised password" policy

□ Implement account lockouts when the wrong password is entered too many times

□ Purchase licenses for a password manager (like LastPass) for your employees

□ Enable and customize Suspicious Login Alerts to users and admins

□ Turn on 2 Factor Authentication (2FA) everywhere possible and implement a hardware token where possible

□ Restrict access to your company resources based on IP's (for example, limit it to ranges and countries you know your users will connect from)

Tip: *Encourage the use of passphrases instead of passwords. They are longer, more complex and may be easier to remember.*

Need some help suggesting a passphrase? Ask these questions:

- If you walked outside, what is the first thing you would see?
- Close your eyes. I say the word "awesome" - what's the first thing you think of?
- What would be included in your last meal?
- What makes up your ideal vacation?

ENDPOINT SECURITY

□ Encourage or enforce the use of VPN for remote users (with 2FA)

□ Invest in Mobile Device Management (MDM)

□ Encourage users to enable automatic updates of apps and mobile OS

□ Encourage the use of secure file sharing and backup that can be monitored by an administrator and that includes additional protection against ransomware attacks

□ Remove Admin rights from standard user accounts

□ Limit use of rooted phones or installation of applications from non-standard App stores

EMAIL SECURITY

□ Review your email security settings and options on a regular basis

□ Enable tagging or identification of external emails to help employees focus on potential external threats

□ Enable ActiveSync or other mobile synchronization policies to better protect data stored on mobile devices and consider further full Mobile Device Management (MDM)

□ Impose delivery restrictions on email distribution lists that do not need to receive messages from external senders

□ Enable an email archiving solution that is independent from your primary email mailbox

Tip: *Set up an annual review of all account security settings to keep security top of mind*

HUMAN SECURITY

□ Encourage employees to call their personal mobile phone providers, and turn-on extra security verification steps, like a PIN

□ Encourage employees to NEVER re-use the same password to their email with any other systems or applications they use

□ Discourage users from storing passwords in their browser

□ Mandate all employees take security training (ex: https://www.knowbe4.com/products/enterprise-security-awareness-training/)

□ Begin once a month/quarter live phishing exercises (ex: https://www.knowbe4.com/)

Tip: *Reward users for reporting anything suspect, this will make them more likely to come forward if they do fall for a phishing or other malicious attack*

TRIPLE GUARD SECURITY™

Is your business data secure? As cyberattacks become more sophisticated and hackers more aggressive, business communications such as telephone calls, voicemails, text messages, video meetings and file sharing are increasingly under attack. Triple Guard Security eliminates the complexity of securing your communications while giving you peace of mind that your business data is protected.

When it comes to security, not all cloud communications solutions are created equal. As a service provider we place the highest priority on security and have invested heavily in our security staff and security technologies to stay ahead of increasingly sophisticated cybercriminals. Triple Guard Security takes a multipronged approach to protecting your business data with technologies that address three potential points of vulnerability – protecting user access, securing applications, and defending the cloud infrastructure. Our cloud communications tools give small and medium-sized businesses the kind of reliability and security enjoyed by the biggest Fortune 500 companies.

QUESTIONS? CONTACT US TODAY!

Flagship Strategic Services, LLC

888-578-3088

support@Flagshipis.com
www.flagshipis.com