NATIONAL MORTGAGE SERVICING ASSOCIATION

BEST PRACTICES FOR DATA SECURITY REGARDING "WORK FROM HOME"

WHAT COMPANIES CAN DO:

- **Business Continuity & Disaster Recovery Plans, Work From Home Information Security, Privacy, Communication Policies**
  - » Perform regular testing to ensure that Business Continuity & Disaster Recovery Plans plans are effective.
  - » Incorporate secure work-arounds or redundancy into business continuity planning, to allow stakeholders to gain access in the event of a system or network failure, and the company's IT team has thoroughly tested all backup systems.
  - » Establish and implement well defined Security Awareness Training Programs for employees to mitigate risks of data security breaches
    - Bring security awareness to employees on an on-going basis regardless of the location in which they reside.
  - » Establish and implement well defined Communications Matrix/Workflows to enable consistent lines of communications/operations across the organization to mitigate disruption to the business.

- **Leverage newer Infrastructure services such Desktop As A Service (DaaS) to securely connect and scale remote workforces without business disruptions.**
  - » One example is Amazon Workspaces that has encryption protocols to encrypt client based traffic in transit and at rest.

- **Invest in Security Services to protect Employees , Customers, Clients, and Corporate Data Use a VPN (aka Virtual Private Network) on workplace/business machines to ensure that employees are able to work inside the company's secure network, and the VPN should be used when available.**
  - » Implement a Secure Mail Protocol (e.g. Mimecast) to enable employees to securely communicate with external parties.
  - » Implement an "Identify Access Management" service (e.g. OKTA) to add additional layers to identify users' access rights to corporate networks.
  - » Implement a third party Managed Detection Response Security Vendor where a 24x7x365 Security Operations Center monitors all network entry points, internal and external facing, for threats, viruses, malicious network intrusion and unusual activities.
  - » Implement a 3rd party identity provider (e.g. BitGlass) to increase control and authentication, and to prevent data leakage from mobile devices such as iOS and Android cell phones and tablets.

PROPOSED EMPLOYEE GUIDELINES TO ENSURE THAT DATA SECURITY REMAINS STRONG AND EFFECTIVE:

- **Maintain regular working hours, including planned breaks**
  - » Planning working hours and penciling in suitable breaks allows employees to focus on what needs to be done and when.
  - » Regular breaks from a computer screen are essential to avoid fatigue, strain or headaches from excessive use. All these factors may increase the chances of human error and, therefore, the chance of a data security breach.

- **If sharing your home with others, designate a workspace and ground rules for interacting with others**
  - » Be clear from the outset as to where your working space is, and the hours you'll be working.
  - » Lock your machine at all times in the event you take a break or leave your workstation.
  - » Do not write notes or sensitive information on paper; instead use technology tools such as (O365) Microsoft Word, Microsoft Teams, Onenote.
  - » Be aware of your surroundings and the activities occurring around you.
  - » Go paperless, leverage technology and tools to eliminate manual printing of documents.

- **Take precautions around web security at home**
  - » For example, ensure your home router is secure, does not use a generic default password, is using encryption, and has its firewall switched on. All these measures will help to secure your home network for personal as well as work use and increase the likelihood of being able to work safely and securely without compromise.
  - » This is even more critical in the age of connected devices. Today, TVs, baby monitors, smart speakers, doorbells, and even lightbulbs can be connected to your network, presenting potential routes into your home network to compromise your more secure work devices and web security. Two-factor authentication, a password, your router, and your firewall may be all that keep them secure. Ensure that all your devices have been changed from their default passwords and that any available security measures are enabled.

- **Resist the temptation to use unfamiliar WiFi for work or private browsing**
  - » It might be tempting to connect to a neighbor's or public unsecured WiFi if the signal appears stronger and your connection appears to be very slow, but it's critical not to do this for private or work-related purposes because it is impossible to discern whether you're inadvertently giving away your credentials to a tech-savvy attacker.

- **Use Multi-factor/two-factor (MFA/2FA) authentication whenever possible**
  - » This extra layer of web security may prevent compromise of work applications.

- **Supplemental encryption with a VPN**
  - » For an external layer of web security and encryption, always use a VPN.

- **Be aware of increased phishing and other forms of cyber attacks through electronic communication.**
  - » Do not click links or attachments in any unsolicited communications offering help or advice, particularly relating to COVID-19 (or really any other significant global events that may be occurring). Stay up to date using reputable news providers and trustworthy government websites for informed and credible updates.