Oregon

Kate Brown, Governor

Department of Administrative Services
Enterprise Information Services (EIS)
155 Cottage St NE, 4th Floor
Salem, OR 97301
PHONE: 503-378-3175
FAX: 503-378-3795

MEMORANDUM

To: All Agency Directors and Agency CIOs

From: Katy Coba, DAS Director and Chief Operating Officer
Terrence Woods, State Chief Information Officer

Date: August 13, 2020

Subject: Use of Personal Devices and Statewide Policy 05.050.01 – "Working Remotely"

As the State of Oregon pivots toward normalization of working remotely, the Department of Administrative Services (DAS) and Enterprise Information Services' (EIS) have partnered to enable the business of state government while ensuring the security of the state network and protection of data entrusted to us by the people of Oregon—particularly, in these uncertain times when bad actors are seeking to exploit the state's vulnerabilities.

With the update and release of statewide policy 50.050.01 – "Working Remotely," there have been a number of questions regarding the State's long-standing prohibition against the use of personal devices to conduct state business or "Bring Your Own Device" (BYOD).[1] More specifically, the applicability of Section 7(b), which states that, *"Employees will not conduct state business on the following personal equipment: phones, computers, laptops or other information storing devices."*

There have also been calls for the establishment of an exception process to address specific use cases given the exigent circumstances our state agency partners are facing, including the use of personal printers and scanners and personal cell phones for the following: voice and text, to enable Multi-Factor Authentication (MFA,) and for use with Virtualized Remote Desktop Infrastructure (VDI). This memo is intended to address these questions and reiterate the position of DAS on the use of personal devices.

- **Use of personal computers, printers and scanners:** ***No exceptions will be granted regarding the use of personal computers, printers or scanners.***

- **Use of personal cell phones for voice and text:** From a technical and security perspective, the use of personal cell phones to conduct state business using voice and text poses little risk to the

[1] *The use state-owned device to conduct state business was also required pursuant to the preceding telework policy and has remained in effect throughout the accelerated migration of Enterprise Email customers to Microsoft 365 (M365) and deployment of deployment of Multi-Factor Authentication (MFA). The EIS policy decision to* ***require all agencies to disable Outlook Web Access (OWA) unless they have MFA in place*** *was announced on March 12, 2020 and Enterprise Email customers were given until April 2, 2020 to achieve compliance with the MFA requirement.*

state network. However, it is important to recognize that any records generated in conducting state business would be subject to public records law, any related public records requests or associated retention requirements. Furthermore, in the event of litigation, the personal device would be subject to discovery and a potential legal hold. Given current circumstances and the challenges associated with acquiring and deploying state-issued cell phones for new remote workers*, **DAS and EIS are providing a temporary exception to the prohibition against the use of personal cell phones for voice and text only.***

- **<u>Multi-Factor Authentication (MFA):</u>** Absent mobile device management and applicable security standards (e.g., device type, operating system), the use of personal devices to authenticate someone's identity is a fundamentally insecure way to grant access to state resources and increases the state's risk exposure to cyber-attacks. ***No exceptions will be granted regarding the use of any personal devices for MFA.***

- **<u>Virtual Desktop Infrastructure (VDI):</u>** While the use of Virtual Desktop Infrastructure (VDI) on state-owned equipment is an acceptable method of providing remote user access to on-premises hosted applications, the use of VDI with personal devices comes with substantial security risks given that it provides a direct connection via the internet to state-owned assets (*i.e*., without a virtual private network or VPN). Risks associated with using VDI on personal devices include threats to the VDI infrastructure itself due to lack of anti-malware or use of an insecure internet connection (e.g., ransomware, file-less attacks, browser based attacks, credential stealing malware, key loggers DNS spoofing, Man-in-the-Middle attacks, session hijacking, Denial of Service). Additionally, risks include threats related to the configuration of the guest operating system on the personal device and its susceptibility to particular attack vectors (remote control software, Trojan, Man-in-the-Middle). Furthermore, there are potential threats associated with VDI-user interactions, including but not limited to, absence of MFA enforcement, lack of local encryption, and lack of general posture-checking (patching and encryption validation and verification of up-to-date anti-malware) among others. From a technical and security perspective, these risks are unacceptable and ***no exceptions will be granted regarding the use of any personal devices to access VDI.***

It is important to recognize that use of personal devices for conducting state business has implications beyond current technical and security challenges: data privacy, disclosure, public records and legal compliance, human resource management and labor relations must be taken into consideration and managed appropriately. As we navigate these and other challenges together, we look forward to continuing to partner with you to enable a culture of working remotely.