Oregon
Tina Kotek, Governor

Department of Administrative Services
Office of the Chief Operating Officer
155 Cottage Street NE
Salem, OR 97301
PHONE: 503-378-3104

MEMORANDUM

To: All Agency Directors and Agency CIOs

From: Berri Leslie, DAS Director and Chief Operating Officer
Terrence Woods, State Chief Information Officer

Date: May 18, 2023

Subject: Use of Personal Devices and Statewide Policy 50.050.01 – "Working Remotely"

Department of Administrative Services (DAS) and Enterprise Information Services (EIS) have partnered to enable the business of state government to include remote work, while ensuring the security of the state network and protection of data entrusted to us by the people of Oregon. This is particularly important in these uncertain times when bad actors are seeking to exploit the state's vulnerabilities.

Since the update and release of statewide "Working Remotely" policy 50.050.01 – questions have resurfaced 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, *"Employees will not conduct state business on the following personal equipment: phones, computers, laptops or other information storing devices."*

Some of the risks of introducing BYOD to the state enterprise are:

- **Security:** BYOD may not have the same level of security as state-managed devices, such as antivirus software, encryption or password protection. This can expose state data and networks to unauthorized access, malware or cyberattacks. Additionally, BYOD may be more prone to loss or theft, which can compromise the confidentiality and integrity of the data stored on them.

- **Compliance:** BYOD may not comply with state policies and standards, such as data retention, backup or disposal. This can create legal and regulatory issues for the state, especially if BYOD handle sensitive or personal information. Moreover, BYOD may not adhere to the state's ethical and professional codes of conduct, such as avoiding inappropriate or offensive content or communications.

- **Cost:** BYOD may incur additional costs for the state, such as providing technical support, training or reimbursement for the employees. These costs may outweigh the

savings from reducing the need to purchase and maintain state-managed devices. Furthermore, BYOD may create conflicts or disputes between the state and the employees over the ownership, responsibility or liability of the devices and the data on them.

There have also been calls for the establishment of an exception process to address specific use cases given the pressing 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 DAS' position on the use of personal devices.

- **Use of personal computers:** ***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 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.

- **Multi-Factor Authentication (MFA):** Absent mobile device management and applicable security standards (e.g., device type, operating system), the use of personal devices to authenticate a user'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.***

- **Virtual Desktop Infrastructure (VDI):** 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. This is because 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.

BYOD security introduces complexity and security challenges for state IT departments, such as:

- Monitoring, updating and supporting different BYOD hardware and software
- Enforcing a BYOD security policy that balances security and privacy
- Preventing unauthorized access, data leakage or malware infection from personal devices

While we have made significant strides in improving cybersecurity practices since the pandemic, there are still outstanding BYOD-specific security challenges. The state will need to implement BYOD security solutions to make the risk manageable:

- Identify and authenticate BYOD devices and users
- Encrypt and secure data in transit and at rest related to the devices
- Control and limit access to sensitive data and applications
- Detect and respond to suspicious or malicious activities that can be posed by unmanaged devices
- Educate and train employees on BYOD security best practices

As we navigate through these and other challenges together, we look forward to continuing to partner with you to enable a culture of working remotely with a reliable, secure framework.

[1] *The use of state-owned device to conduct state business was also required pursuant to the preceding telework policy and remained in effect throughout the accelerated migration of Enterprise Email customers to Microsoft 365 (M365) and 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 October 1, 2022 to achieve compliance with the MFA requirement.*