

Steve Sisolak
Governor



Laura E. Freed
Director

Matthew Tuma
Deputy Director

Timothy Galluzi
Administrator

STATE OF NEVADA
DEPARTMENT OF ADMINISTRATION
Enterprise IT Services Division

100 N. Stewart Street, Suite 100 | Carson City, Nevada 89701
Phone: (775) 684-5800 | www.it.nv.gov | Fax: (775) 687-9097

MEMORANDUM

January 26, 2022

TO: All Agencies

FROM: Timothy Galluzi, Administrator

SUBJECT: **Enhancements to State Office 365 Tenant Functionality**

The Enterprise IT Services Division (EITS) is proud to announce two feature enhancements to the State Office 365 Tenant.

First, Microsoft announced in August that it would be adding unlimited dial-in capabilities for Microsoft Teams meetings across their enterprise, business, frontline, and government suites. This capability has been added to the state Office 365 tenant and ensures that users can join their Microsoft Teams meeting from virtually any device regardless of location. To utilize this functionality, simply schedule a Teams meeting in either Teams or Outlook – dial-in information will be automatically included. To verify call-in information is present, check the details of any Teams meeting you create.

Next, effective February 7, 2022, EITS will enable multi-factor authentication (MFA) for unlicensed users, guest accounts, and external user accounts accessing data in the state Office 365 tenant, including identity and authentication data, from outside SilverNet (the state's network). For example, when an external job candidate (a guest) receives a Teams videoconference meeting invitation through Outlook from a state agency, the candidate will need to use MFA, which requires a text or phone call in addition to a password when logging in. Agencies that frequently share OneDrive-hosted documents or host Teams-based meetings with partners not on the state's Office 365 tenant may want to communicate this upcoming change to those partners.

When a guest or other unlicensed user is currently invited to access Office 365 data hosted in the state tenant, they receive a welcome email message that includes information about the content they will be accessing and instructions on how to connect to tenant-hosted resources. Upon completion of this change, guests or other unlicensed users will be further instructed to configure and enable MFA for their Microsoft-hosted guest account before they will be permitted to access the shared data. This means they will need to use a secondary device, such as a mobile phone with the Microsoft Authenticator app, to approve their sign-in.

Microsoft's documentation for configuring MFA can be reviewed here:

<https://support.microsoft.com/en-us/account-billing/sign-in-to-your-work-or-school-account-using-your-two-step-verification-method-c7293464-ef5e-4705-a24b-c4a3ec0d6cf9>

Per State of Nevada Information Security Standard S.5.06.01§6.5(B), MFA is required for state employees and contractors when connecting from outside SilverNet to a cloud service that collects, processes, transmits, stores, or interconnects with state data. Additionally, devices that connect via a state-hosted virtual private network (VPN) connection, including the EITS-hosted VPN, meet this requirement. This means that when employees work remotely, they use MFA to authenticate their online session. New employees or users new to MFA who would like more information are encouraged to review these MFA frequently asked questions (available on the state's network and by VPN):

http://ess.nv.gov/uploadedFiles/nerdsnvgov/Content/Training/MFA-FAQ_Final.pdf

To adhere to this security standard, EITS has already enabled MFA for all state employees accessing the state Office 365 tenant from outside SilverNet. This enablement also currently applies to licensed state users accessing third-party systems that integrate with Office 365 for authentication and authorization purposes.

By enabling MFA for the additional group of users, all individuals who access data within the state Office 365 tenant, as well as any third-party systems that integrate with Office 365 for authentication and authorization, will be made to adhere to State of Nevada Information Security Standard S.5.06.01§6.5(B).