Department of Information Technology

MEMORANDUM

DATE: September 26, 2023

TO: Mayor and City Council

THROUGH: Doug Thornley, City Manager Approved Electronically

FROM: Craig Franden, Director of Information Technology

SUBJECT: Microsoft M365 Migration and Multifactor Authentication

---

The Department of Information Technology (DoIT) is working on two significant projects aimed at improving security as well as improved integration and efficiencies citywide.

Microsoft 365

Microsoft 365 will replace Google Enterprise Suite. The Microsoft 365 project replaces email, document types, document storage, meetings, collaboration spaces and chat that we currently use in Google. This transition is required to support improved integrations with software and technology programs used across the city and provides a more robust suite of services to meet the growing needs of the organization. Examples of two major Integrations are outlined below to illustrate the impact of this transition.

OnBase and Microsoft Outlook Integration:

The Outlook integration with OnBase allows importing and retrieving documents in Outlook while still allowing for indexing and using workflows correctly. This will greatly enhance the effectiveness of users that work with the OnBase product on a regular basis.

OneMeeting Agenda Management and Office 365 Integration:

Users of OneMeeting will be able to seamlessly integrate with Word documents, track changes and collaborate in real time without the need to download staff reports, make changes and re-upload to OneMeeting. In addition, other staff will now be able to see the changes in real time and collaborate on documents throughout the process, limiting the opportunity for errors throughout agenda development and reducing the amount of time required to work around the current limitations created by using tools with no integration between systems.

The Liaison team will be trained and available for support to assigned Council Members throughout the transition. Account history will transition to the new system to ensure continuity of service and access to previous emails and calendar information. Transition to Office 365 for Council Members will be October 3, 2023.

Multi-Factor Authentication – A Necessary Layer of Cybersecurity

Multi-factor Authentication (MFA) is being added to enhance security to all systems and augment passwords. All security is comprised of three things: Something a person knows (such as a password), something a person has (such as a physical key), or something physically unique to the person (such as a fingerprint or retina scan). Passwords are becoming increasingly easier to obtain by malware attacks and large data breaches. When a password is stolen in a data third party breach, the probability that a staff member is also reusing that same password for their City password is incredibly high. Adding MFA protects against stolen and reused passwords by requiring an attacker to also gain access or intercept a physical device that is your second factor.

MFA is a mandatory requirement for obtaining and maintaining cybersecurity insurance coverage through risk management. Disabling MFA for any staff can result in immediate denial of a potential insurance claim in the event of an attack for violation of the contract. It is also a requirement the City is mandated to follow to maintain security requirements of the Federal Bureau of Investigation for compliance with the Criminal Justice Information Services (CJIS) and the National Crime Information Center (NCIC) which are both critical to public safety operations.

When an agency is compromised it can greatly impact the government's ability to provide emergency services and all other facets of work with businesses and citizens. Many local governments that have been affected by ransomware or other attacks have led to downtime to citizens for weeks to months. Implementing MFA will help in protecting the City of Reno ability to provide critical infrastructure/services along with its' citizens trust in protecting their data.