Exchange Server 2019 Enterprise Migration	
PRO	CON
Perpetual license	City will have to migrate again once support ends Oct 2025 for Exchange 2019
Provides additional logging access and server control beyond what M365 would provide	City will have to manage virtual server for Exchange 2019 (patching, logging, monitoring, etc.)
Lower upfront cost than Exchange Online migration	Additional memory resources needed for servers
	Upgrade of backup appliance with larger mail server required
	Limits our capabilities for increased productivity and collaboration internally and externally
	City will need to interface with a consulting firm to assist with e-mail migration
	Could be impacted by another zero-day vulnerability at any point in the future

Exchange Online Migration (M365)	
PRO	CON
Fully supported with no end-date published	Cost associated with annual subscription (M365) per user
Handles server hardware/software updates without any added costs	No direct access to servers since it is Software as a Service (SaaS)
Enhancements to City software included with M365 subscription (SharePoint, Teams, Teams Phone, One-Drive, Booking, DLP, Always-On VPN, Device Management, PowerBI, MFA, Threat Analytics, Access Reviews, and many others)	Cost associated with annual subscription for Cloud Backup Service (although backup cost is lower than Exchange Server 2019)
Most City data is stored centrally and will provide visibility into how that data is managed.	Would involve costs for standing up other required services
Ability to authenticate with 3rd party services (Brightly, NeoGov, ClearGov, etc.) to use one user password across several systems.	
City may enter an Enterprise Agreement (EA) with Microsoft to keep pricing level on a per user basis over a three (3) year time period before entering an EA with updated pricing.	
Larger mailbox size limits (100GB user / 50GB shared mailboxes) than what could be attained with an on-premises Exchange Server	
Detonation Chamber feature to safeguard us from malware or ransomware that may originate through a phishing e-mail with an attachment.	
Was not impacted by the zero-day vulnerability in 2021.	