

**CITY OF FRANKLIN
TECHNOLOGY COMMISSION MEETING MINUTES
JULY 22, 2026**

- I. The July 22, 2026 Technology Commission Meeting was called to order at 6:02 p.m. in the Hearing Room of Franklin City Hall by Chair Greg Strowig.

IT Director Jim Matelski took roll call; a quorum was present. Members present were Strowig, Alderman Johnson, Wielebski, Rehberger, Smak, and McWilliams. Members Surana and Romanski were excused. Member Berg was absent. Also, in attendance was IT Director Jim Matelski.

- II. Citizen Comment Period – no citizens were present.

- III. Review and approval of the April 22, 2026 Meeting Minutes.

Motion made by Member Rehberger and seconded by Member Wielebski to approve the April 22, 2026 meeting minutes as submitted. Upon vote, Ayes-5, Abstain-1, motion carried.

- IV. Review of Proposals for 3PAR SAN Replacement Project and Selection of Vendor

IT Director Matelski presented this item to the Commission and further discussion was held.

Motion made by Member Wielebski and seconded by Alderman Johnson to extend the warranty with a fall back of processing the Hitachi 3PAR SAN if financing of the warranty cannot be incurred. Upon vote, Ayes-All, motion carried.

- V.a. Review of the 2025/2026 SCS External and Internal Penetration Test with Recommended Remediations and the Risk/Watch Matrix

Motion made by Alderman Johnson and seconded by Member McWilliams to enter closed session for this subject matter item pursuant to Wis. Stat. § 19.85(1)(d), to consider strategy for crime prevention, and the furtherance of a program and policy and tools therefore for crime prevention, i.e., cyberattack prevention and technological crimes in relation thereto, for the protection of the City's technical and information infrastructure and the City officials, employees and the public who use the system, and to reenter open session at the same place thereafter to act on such matters discussed therein as it deems appropriate. Upon vote, Ayes-All, motion carried.

No further action was taken on this item once back in open session.

- V.b. Review of the Pro Phoenix Account Segmentation Proposal and Elimination of the SQL SA Account

Motion made by Member McWilliams and seconded by Alderman Johnson to enter closed session for this subject matter item pursuant to Wis. Stat. § 19.85(1)(d),

Technology Commission Meeting Minutes

July 22, 2026

Page 2

to consider strategy for crime prevention, and the furtherance of a program and policy and tools therefore for crime prevention, i.e., cyberattack prevention and technological crimes in relation thereto, for the protection of the City's technical and information infrastructure and the City officials, employees and the public who use the system, and to reenter open session at the same place thereafter to act on such matters discussed therein as it deems appropriate. Upon vote, Ayes-All, motion carried.

No further action was taken on this item once back in open session.

VI. Technical Issues Review

- After the first round of penetration testing was finished, it was discovered that substantial lateral movement on the network is made possible by the absence of ZTA (zero trust architecture) and NAC (network access control) policies. The capital budget for 2027 included the Aruba Clearpass Policy Manager. It is acknowledged that the best option is an integrated vendor solution that works with all network switches and wireless access points, but this comes at a cost that will probably be rejected during the budgeting process. The budget proposal's goal was to fully illustrate what an Aruba-architected enterprise network would look like, as well as how the NAC and administrative technology (Aruba Central) can be used to completely secure the internal LAN. It is acknowledged that manually generated ACLs (access control lists) are insufficient to restrict network-wide access to VLANs. Writing conditional ACLs is challenging and error-prone due to the dynamic routing of BGP (border gateway protocol) between offices and the addition of SD-WAN for multiple ISP backup. It will be necessary to investigate a less costly technology that is backwards compatible with legacy switching. The basic security architecture must incorporate both ZTA and NAC.

VII. Director's Report on IT Operations

- The FRANKLINNT domain was formally deactivated on July 5, 2026. A few minor disruptions occurred after servers were turned off, when a non-Windows device used the outdated domain controllers to resolve DNS names. Outdated DNS servers prevented the device from performing DNS resolution. The network's security flaws were greatly diminished by the former domain's deactivation. We are wrapping up and closing this project.
- VoIP Hell - On Monday May 25th (Memorial Day), VoIP services started receiving extensive packet loss, up to the point where phone connections were unstable and communications garbled. Extensive troubleshooting was performed between the firewall vendor (TPx), phone provider (Ring Central), ISP/carriers (WiscNet and Spectrum), as well as bringing in additional supplemental engineering support from Cornerstone. All firewalls are at current patch levels and there is nothing within the firewall policies that we attribute to extensive packet loss. QoS policies are implemented on all switches, up to a point that a 10-year-old switch can actually

Technology Commission Meeting Minutes
July 22, 2026
Page 3

Packet loss is occurring either at the edge network (firewalls, WAN switches, ISP, phone provider, or Internet aggregation router). Ring Central and WiscNet packet loss reports indicate that packet reliability was at 99.5% prior to the outage and was reduced to 80.4% starting on 5/25/2026. After two months of troubleshooting and finger pointing, the core problem still has not been fully determined. The problem is not believed to be with the internal network, ISP, or phone firmware/application. The packet loss exists when using either WiscNet or Spectrum as the carriers. This problem is almost two months old and is still being worked on.

- Rapid 7 deployed, under its current implementation, requires a service account that has domain administrator level privileges in order to read logs and export these to the SIEM. The SCS post-penetration test security recommendations require that the administrator and high security privileged accounts be members of the "Protected Users" built-in global group. Membership within this group elevates security restrictions and makes it significantly more difficult to view account details or steal password hashes. Rapid 7 has to be redeployed using a different and more complex security implementation, where the dedicated service account is no longer a member of the Domain Admins global group. This will require reinstalling the application on the network. This change will allow the Domain Admins global group to be a member of the Protected Users group, thereby increasing the level of security on all linked accounts.

VIII. Future Agenda Items.

- IT Security Project—Johnson Controls, Inc.
- Failure Avoidance and Mitigation
- Website ADA Compliance – Project Closure

IX. Next Meeting Date: August 26, 2026 - 6 p.m.

X. Adjournment

Motion made by Alderman Johnson and seconded by Member Rehberger to adjourn the July 22, 2026 Technology Commission Meeting at 8:14 p.m. Upon vote, Ayes-All, motion carried.