Technology Resources - Admin Tips & Tools

- AD and email policies
- AD/E-mail Meeting Notes
- City of Milwaukee Website and Application Shortcut URLs
- **Network and Security**
- Outlook Web App for Office 365

Network and Security

2018 City of Milwaukee Network Security Platform Upgrade

In 2018, ITMD will be deploying an updated Next-Generation Security Platform. This system will be deployed in phases to different departments throughout the year to avoid impacts to each department during their busy or critical times.

In addition to refreshing the systems that are currently in place, the new security platform provides much greater functionality to support the City of Milwaukee's operations in a secure manner. Some new functionality includes:

- Redundant systems to reduce down-time during scheduled maintenance and unexpected events.
- The ability to allow access to systems by user ID, as well as by device. Currently, access to restricted systems was controlled on a per-device basis. Going forward, the primary means to verify access will be by user ID, meaning a user can access those systems from any device to which they are logged in, not just their primary device.
- The ability to inspect traffic and block based on anti-virus, anti-spyware, and vulnerability protection profiles.
- The ability to block or allow categories of websites, including secure (HTTPS) sites. The City allows Internet access for business use and incidental personal use. General Internet access is open, except for those categories that pose a security, financial, or legal risk to the City. Those categories that are blocked include:
    1. **Command and Control** - URLs and domains used by malware and/or compromised systems to surreptitiously communicate with an attacker's remote server to receive malicious commands or exfiltrate data.
    2. **Copyright Infringement** - Web pages and services that are dedicated to illegally offer videos, movies or other media for download infringing copyrights of others. Should not include sites that provide peer-to-peer file exchange services or general streaming media.
    3. **Dynamic DNS** - Sites that provide and/or utilize dynamic DNS services to associate domain names to dynamic IP addresses. Dynamic DNS is often used by attackers for command-and-control communication and other malicious purposes.
    4. **Excessive Bandwidth** - Sites that utilize a large amount of bandwidth for non-business purposes. This includes sites that provide streaming media and live gaming content. This does not include web conferencing or training/tutorial video. (Please note, certain applications not needed for business use but popular for personal use may be temporarily disabled on occasion if required due to limited available bandwidth.)
    5. **Hacking** - Sites relating to the illegal or questionable access to or the use of communications equipment/software. Development and distribution of programs, how-to-advice and/or tips that may result in the compromise of networks and systems. Also includes sites that facilitate the bypass of licensing and digital rights systems.
    6. **Malware** - Sites containing malicious content, executables, scripts, viruses, trojans, and code.
    7. **Phishing** - Seemingly reputable sites that harvest personal information from its users via phishing or pharming.
    8. **Proxy Avoidance and Anonymizers** - Proxy servers and other methods that bypass URL filtering or monitoring.
- The ability to restrict downloading of files that are considered "high risk". We are currently using the manufacturer default settings for "basic file blocking". These settings block the following file types:
    1. 7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf.
- A new remote VPN access solution that includes support for Windows 10 and other current operating systems.

When deploying new features, we will make every effort to verify they function as expected and do not restrict or impede current City operations. In any instances where problems may occur, please report them via RITS or x2777 and we will work to make changes as soon as possible. In the support request, please include your user ID, the time the trouble occurred, and the specific nature of the trouble.

- If you have problems with a website, please note which web browser you are using, the website you are going to, and any error messages that appear (a screenshot would help, if available).
- If you have problems downloading a file, please note the type and name of the file (is it a PDF, Word, Excel, EXE program, etc.) and the software used to download the file.
- If you have problems with a specific application, please note the application being used.

Special Note for Web Conferencing

One application that is a unique challenge to anticipate and support is web conferencing. We've found multiple vendors which each have unique implementations. The following providers have been tested and are confirmed to work under the limited testing performed to date:

- GoToMeeting
- WebEx
- Zoom.us
- Skype
- LogMeIn

The following vendors have not been tested or are known not to be supported at this time:

- UberConference
- join.me
- Any other web conferencing provider

Because support for web conferencing is time-critical and difficult to test outside of those scheduled sessions, please contact David Henke at 286-3248 or david.henke@milwaukee.gov prior to any scheduled web conference after the change has been implemented or if you intend to use a new web conferencing tool to verify a successful web conference connection 10-15 minutes prior to the start of the actual meeting.

Thank you for your support and understanding in enhancing the City's computing environment to make it as secure and functional as possible.