Published on *MTAS* (http://www.mtas.tennessee.edu) October 26, 2020

Information Technology

Dear Reader:

The following document was created from the MTAS website (mtas.tennessee.edu). This website is maintained daily by MTAS staff and seeks to represent the most current information regarding issues relative to Tennessee municipal government.

We hope this information will be useful to you; reference to it will assist you with many of the questions that will arise in your tenure with municipal government. However, the *Tennessee Code Annotated* and other relevant laws or regulations should always be consulted before any action is taken based upon the contents of this document.

Please feel free to contact us if you have questions or comments regarding this information or any other MTAS website material.

Sincerely,

The University of Tennessee
Municipal Technical Advisory Service
1610 University Avenue
Knoxville, TN 37921-6741
865-974-0411 phone
865-974-0423 fax
www.mtas.tennessee.edu

Table of Contents

Information Technology

Reference Number: MTAS-65

Click on the topics listed below in this section for more information.

Archival Policy for Electronic Information

Reference Number: MTAS-1075

This section is intended to provide guidance, especially to smaller cities, in the creation and implementation of a practical and cost-effective archiving policy for Electronically Stored Information (ESI). Various state and federal laws require cities to retain certain records and communications for differing amounts of time. The fact that such a document is in an electronic format in no way relieves such responsibility. In fact, amendments to the Federal Rules of Civil Procedure clearly stipulate that special procedures must be taken to protect electronic data. To ensure compliance with state and federal laws, every city should institute an ESI archiving policy, which at a minimum:

1. Determines whether manual or automatic archiving is preferable for the retention of ESI;

2. Appoints someone to oversee and ensure compliance with this policy; and

3. Ensures that the retention archives are consistent throughout the organization so that retrieval, when necessary, can be timely and thorough.

A well-reasoned and thoughtfully implemented retention policy conveys an image of transparency, which is a benefit to any city. Such a policy can also save large amounts of time and money in the context of a discovery request. A policy for ESI retention should exist in conjunction with a more exhaustive records retention schedule.

The Records Management for Municipal Government [1]section in this database provides a nearly comprehensive list of municipal records and the appropriate retention period for each class of records. Many of these classifications of records such as warrants and other court documents may not exist in electronic format. Other records however, such as employment correspondence, citizen complaints, and other vital information, are becoming increasingly common in an electronic form. The overriding principle here is that record retention is subject-based not medium-based. Hence a letter and an e-mail with the same content would require the same retention.

When managing your ESI, there are two basic archiving methods – automatic and manual. Deciding which method will suit the needs of your city is the first step in developing a sound ESI retention policy. Generally, automatic archiving systems are preferable for large organizations that generate large volumes of ESI. While these systems are very thorough, their expense may be cost-prohibitive to many cities. Despite its potential for human error, manual archiving will be the likely choice for most Tennessee cities.

The first method, automatic archiving, is an automated system that would be managed by your IT department. Many such systems, available through various vendors, will harvest, archive and delete your ESI based on the rules that are implemented in the software. The rules that you implement are established by your written policy. A list of a few of the products and vendors is included at the end of this page. The recommendation of a specific software product is outside the scope of this document.

The second method, manual archiving, is a manual process managed by the individual users in your municipality. This method is similar to the current approach with paper documents and can even mirror this process if you decide to print all ESI and file it away with your other documents. Each user would be responsible for all the ESI that is created and received by that user. However, the municipality has the responsibility of developing, training, maintaining and auditing this method. If you would like to maintain your ESI in electronic format, consult with your IT department because your capability to do so depends on the server resources and technologies available to you. Manual archiving will work even if you do not have an IT department or a server. One example of this method would be to create a filing structure that would mirror the subject guidelines established in the Records Management for Municipal Governments - Retention Schedules [2]. See figure below.

ARCHIVE EXAMPLE DIRECTORY

Animal Control

Activity Reports . . . . . 2-year retention
Adoption Contracts. . . . . 4-year retention
Annual Reports . . . . . .permanent retention

Cemeteries (City Operated)

Deed Books . . . . . .permanent retention
Internment . . . . . .permanent retention
Perpetual Care Records. . . . .permanent retention

Courts

Affidavit of Complaint . . . . .permanent retention
Appeal Dockets . . 10-year retention after last entry

Elections

Candidate Lists . . . .4-year retention after election

Engineering

Aerial Photographs . . . . . permanent record
Complaints . . . . . 5-year retention

Finance

Accounts Paid Files and Ledgers . . 7-year retention
Accounts Payable . . . . . .10-year retention

This structure can be established in your e-mail file, a file server drive, or on the system drive for your specific computer. Note that if you are keeping this data electronically for retention purposes, keep it in a location that is backed up to another form of media on a regular basis. In the example shown above, the retention period was added to the name of the folder to make management of the content easier for the user.

The following systems are a few that were identified and are provided as references only. This is not a complete list of products and is not an endorsement by MTAS.

Google Vault - adds archiving and e-Discovery to G Suite for Government [3]

Microsoft Exchange online Plan 2 or Office 365 (Plan E3) for government offer the Archiving and Legal hold capabilities [4]

Veritas Enterprise Vault [5]

EMC Archiving Software [6]

ZL Technologies Unified Archive [7]

Finally, it is important to note the distinction between ESI archiving and the use of backup software. While archiving makes content distinctions and saves ESI accordingly, backup software stores all ESI transmitted during a specified time frame. Backups can be very large, unwieldy databases, and due to technological limitations in retrieval, would not satisfy the requirements of an archive system. Backup systems are designed for disaster recovery situations – not record retention.
Make sure your city has an adequate archival system for its ESI. Waiting until you receive a Subpoena Duces Tecum will certainly be too late.

Cable TV/Telecommunications and Utility Franchises

Reference Number: MTAS-83

Municipal governments may grant franchises to privately owned utilities that use public rights of way. The majority of city charters contain procedures for granting franchises. Most franchises require the utility to pay a fee to reimburse the community for using its streets and rights of way. Municipalities may, upon request by a cable company, grant a cable franchise. T.C.A. §§ 7-59-101, *et seq.*

Cities under the general law modified city manager-council charter have authority to acquire, own, and operate cable TV systems. T.C.A. § 6-33-101. Under the 1992 Cable Television Consumer Protection Act, all cities may build and operate a cable system in competition with their existing franchise without granting themselves a franchise.

Municipally owned electric utility systems may construct and operate cable TV systems in their service areas. However, the cable operation may not be subsidized by the municipality or by the electric system, and it must pay tax equivalents using the same method prescribed for the electric system. T.C.A. §§ 7-52-401–407.

In addition to cable TV companies, cities have issued franchises to private companies providing gas, electric, water, steam, and public transportation. State law prohibits a company from acquiring the franchise or property of another company operating under a city franchise without the city's permission. T.C.A. § 6-54-109.

Municipalities probably do not have the authority to franchise a telephone/ telecommunications company or to collect a franchise fee based on the company's income. But, cities may require the firm to pay "police power" rent, i.e., a fee that covers the municipality's direct costs of the telephone/ telecommunications company's use of rights of way. T.C.A. § 65-21-103, T.C.A. § 65-21-203. (Also see *City of Chattanooga v. BellSouth Telecommunications*, (unreported) 2000 W.L. 122199 (Tenn. Ct. App. 2000).)

Statewide Cable and Video Service Franchising

Notwithstanding the above discussion about local cable franchising authority, cable and video service companies have the authority to bypass a local franchise and obtain a state franchise under the Competitive Cable and Video Services Act. T.C.A. §§ 7-59-301, *et seq.*

The act preserves local franchising but creates a new statewide franchise with immediate opt-in provision for incumbent franchise holders. An incumbent with an expired franchise can apply for a statewide franchise within 180 days of July 1, 2008. The award of a statewide franchise terminates any unexpired local franchise. Franchise fees, however, remain the same until the local franchise agreement would have expired, and the provider cannot reduce or terminate any services until another provider is providing services.

Statewide franchise applications are filed with Tennessee Regulatory Authority and forwarded to the affected local government. Providers then have 24 months to begin offering services. Statewide franchise fees are set at 5 percent of gross revenues. The application fee is $15,000. The state franchise has a 10- year term and is transferable. Local governments cannot request anything else of value from statewide franchise holders.

State franchises do not alter state law regarding local control of rights of way, local police power, or right to impose generally applicable taxes.

State franchise holders are subject to FCC customer service standards and are obligated to keep current PEG channels at no additional cost. New PEG channels are based on population levels.

Siting Telecommunications Towers

Reference Number: MTAS-752

With the widespread use of cellular telephones and similar wireless electronics, cities are receiving an increasing number of requests from telecommunications companies to place antennas and towers in their communities. Many of these towers are quite large and can pose safety risks for neighboring residents and businesses. Communications towers may conflict with the aesthetics of the neighborhood and generate concerns from residents when applications are received at city hall.

A modern city should have a strategy in place before it considers a request from a telecommunications service to erect a tower. The strategy should recognize the important role that telecommunications services play in the community and not unduly prohibit tower construction. At the same time, however, the policy should assure that citizens will be protected against shoddy construction and ensure against an unreasonable proliferation of such antennas in the community.

Federal Laws Affecting Tower Placement

Reference Number: MTAS-1452

Section 704 of the 1996 Telecommunications Act contains several key provisions affecting the authority of municipalities to regulate the placement of towers for cellular telephones, personal communications services, and other similar transmitters. Generally, the act preserves municipal zoning authority as it relates to radio towers and their siting, but it also creates three key protections for firms seeking to erect a tower:

- Local ordinances may not “unreasonably” discriminate among providers of functionally equivalent services. Tower siting policies must not favor one company, or one technology, over another;
- Local government may not impose a blanket prohibition against the placement of telecommunications towers; and
- Local ordinances may not impose more stringent “environmental effects” limits on radio frequency emissions than those adopted by the Federal Communications Commission (FCC).

A municipality would do well to encourage colocation of telecommunications facilities — essentially the sharing of a single tower by multiple telecommunications services. Such practices have the potential to reduce the proliferation of towers. Federal law encourages this practice and gives cities some leverage to assure that legitimate efforts are made to effect colocation. 47 U.S.C. 251(c)(1) and 47 U.S.C. 251(c)(6) discuss the “duty” of telecommunications service to negotiate in good faith for colocation opportunities. Municipal ordinances should reflect this obligation, and final tower approval should depend on an applicant’s demonstration of these efforts.

Federal law allows cities to deny construction permit applications for telecommunications towers. The denial, however, must be based on a reasoned approach, otherwise the FCC is authorized to pre-empt the local decision and grant the construction permit.

Without adopting a telecommunications tower policy, it is doubtful that a municipality’s denial of a construction permit will be seen as resulting from a reasoned approach.

State Laws Affecting Tower Placement

Reference Number: MTAS-1453

T.C.A. § 13-24-304 specifically authorizes municipalities that have adopted planning and zoning regulations to regulate the siting of telecommunications towers. However, T.C.A.§ 13-24-305 places limits on a city’s power to regulate minor alterations to pre-existing antennas.

T.C.A.§ 65-21-116 requires owners of telecommunications towers to submit information concerning tower location and ownership, a copy of the deed or lease for the property, and related information to the Tennessee comptroller of the treasury. The comptroller’s Web site provides forms that can be downloaded for this reporting.

Otherwise, there are no state laws concerning placement of telecommunications towers.

Laws of Nature Affecting Tower Placement

Reference Number: MTAS-1454

The physics of radio signal transmission cannot be altered by the mere adoption of man-made laws and ordinances. Radio signals obey the physical laws of the universe, and government can no more repeal or amend these laws than it can the law of gravity.

One of the physical laws governing the placement of telecommunications towers is that antennas that are placed high in the sky tend to transmit and receive much better than those placed low to the ground. Cities that (inadvertently or otherwise) limit the placement of antennas to low-lying areas may effectively be prohibiting telecommunications towers in their community and inviting legal challenge.

From the perspective of the telecommunications provider, the ideal locations for telecommunications towers include:

- The tops of hills and mountains;
- Atop high-rise office buildings, apartments, water towers, etc.; and
- On existing telecommunications towers, if space is available.

Placement in the downtown area of a community has unique advantages and disadvantages that the tower owner must consider. The obvious advantage is that the central business district is where the city's tallest buildings are likely to be located. They can be used to achieve the altitude needed for radio signal transmission and reception. On the downside, buildings in a downtown area can cause wave reflection that results in poor signal quality. Additionally, certain commercial and industrial activity in a downtown area can contribute to electromagnetic interference of radio signals.

When determining which areas of towns are suitable for the placement of telecommunications facilities, city planners would do well to include locations where the physical environment favors the transmission and reception of radio signals. Conversely, limiting telecommunications towers to areas where radio signal transmissions or reception is weak may invite legal challenge.

Laws of Economics Affecting Tower Placement

Reference Number: MTAS-1455

Tower construction may be divided into two general types:

- Guyed towers: Towers that depend on the attachment of guy wires to hold them in place and to protect against the forces of wind and ice.
- Self-supporting towers: Towers that are rigidly constructed and, once attached to a base anchored in the ground, need no additional support to withstand the forces of nature.

Guyed towers tend to use a latticework construction. Self-supporting towers can use latticework construction, but the more modern approach is the monopole — a tapered, rigidly built spike or pipe placed perpendicular to the ground.

Inch for inch, self-supporting tower structures generally are more expensive to construct than guyed towers.

Despite their relative lower cost of construction, guyed antennas may ultimately be more expensive for the telecommunications provider due to the amount of real estate needed for this type of construction. For example, a 200-foot tower, 80 percent of which is to be guyed, will require nearly two full acres of real estate to achieve the necessary rigidity. [1] In a community having high real estate values, installing a guyed tower may not be a viable option.

As a city plans for the placement of telecommunications towers, it must understand these economic realities.

---

[1] Roger L. Freeman, *Telecommunication Transmission Handbook*, Second edition. John Wiley & Sons, New York, 1981, *page* 242.

Goals for a Municipal Tower Policy

Reference Number: MTAS-753

Seven Factors to be Addressed by a Tower Siting Ordinance

A well-written tower ordinance will:

- Encourage a modern, nondiscriminatory and competitive telecommunications system within the community;
- Protect the health, safety and welfare of the citizens in the community;
- Discourage antenna or tower proliferation and protect against visual blight and damage to community aesthetics;
- Avoid interfering with other types of telecommunications (fire, police, and other emergency communications);
- Create a reasonable and efficient permit application and review process;
- Assure that the tower will be maintained throughout its lifespan; and
- Comply with the permit requirements of the Federal Communications Commission (FCC) and the Federal Aviation Administration (FAA).

General Siting Strategy

An antenna facilities ordinance should identify areas of the community where the placement of towers will be encouraged. Generally, these will be:

- Areas where local zoning favors the placement of antenna towers. Usually, these will include industrially zoned properties, agricultural land and other sparsely populated sections of town.
- Areas where antenna towers may be permitted by issuing a special use or conditional use permit. Issuing the special use permit is subject to geographic and topographic conditions, population density and the physical properties of the proposed tower. In these areas, towers might be permitted if it can be demonstrated that they will not pose a safety risk or damage neighborhood aesthetics. Commercial areas, public rights-of-way and similar areas are included in this group.
- Areas where antenna towers are forbidden. Low density residential neighborhoods and areas near airports, helipads and other highrisk facilities that could be threatened by placement of an antenna tower. The FCC is required to evaluate the impact of a proposed tower on historic sites, wilderness areas, wildlife preserves, Indian religious sites, flood plains and wet lands, and the city might consider linking its permit approval to the FCC's review.

Within zoning districts where tower placement might be acceptable, cities should establish priorities that favor tower construction techniques that minimize environmental and aesthetic concerns. A city's telecommunications ordinance may, for example, encourage antenna placement on existing radio towers or other tall structures or buildings and require applicants who propose to construct new towers to inventory such available sites in the community and to explain why they were not proposed for site approval.

Compliance with FCC and FAA Regulations

A proposed telecommunications tower with a height of 200 feet or more above grade at the site must be cleared by the FAA and registered with the FCC. Towers proposed for construction within 20,000 feet of an airport runway may be required to be similarly registered with the FCC, depending on topography and the length of the airport runway. The FCC maintains an interactive website that allows users to submit key information about antenna proposals to determine whether FCC registration is necessary. The website provides automatic and immediate notice to the user about the need to register the proposed tower. [2]

Exceptions are granted for proposed towers that will be “shielded” by existing, permanent structures or natural terrain of equal or greater height, in congested municipal areas where there is “no reasonable doubt” that the structure so shielded will not affect air navigation. The phrase “no reasonable doubt” is open to fairly broad interpretation. Any misjudgment in this area could have tragic consequences, and cities would do well to leave such decisions to the FCC and the FAA. Cities should also be aware that if such shielding is ever removed (i.e., building demolition), a previously unregistered tower must be registered with the FCC.

The Antenna Facilities Ordinance should stipulate that the city will not consider any tower construction permit unless and until the applicant has completed the FCC and FAA registration process, if required.

[2] http://wireless2.fcc.gov/UlsApp/AsrSearch/towairSearch.jsp;JSESSIONID_AS... [8]

Design Criteria

Reference Number: MTAS-756

Specific standards will vary from one city to the next, as geologic, topographic and other environmental factors change. The basic guideline is to adopt construction standards that address the following:

- **Unit strength:** The tower design, the materials with which it is constructed and the methods used in construction must be sufficient for the tower to support its own weight plus the weight of any antennas it may support. Care should be taken to assure that unit strength is adequate to support antennas that may be added to the structure after the initial construction is completed.
- **Foundation strength:** The engineering of the foundation must take into account geologic and seismic factors that may affect the stability of the structure.
- **Wind loads:** The structure should be of sufficient rigidity to withstand the highest wind velocities prevalent in the area. Standards may be more stringent in heavily populated areas than in rural setting, for taller structures than for shorter towers, etc.
- **Ice loads:** Telecommunications towers must be designed to withstand ice storms typical for the environment in which they are located.

The American National Standards Institute ANSI) and the Telecommunications Industry Association (TIA) have jointly developed nationally recognized design standards for telecommunications towers, published as “ANSI/TIA Standard 222 — Structural Standards for Antenna Supporting Structures and Antennas, Revision G.” Tennessee cities should procure a copy of these standards and include them by reference in their telecommunications ordinances.

The ANSI/TIA tower design standard contains a complicated mixture of engineering formulas and statistical analyses. For this reason, any review of a proposed tower construction is best left to a qualified and experienced structural engineer, one who can subject the proposed design to sophisticated computer analysis. Tennessee cities should require all tower plans to bear the stamp of a professional engineer registered in the state of Tennessee.

Telecommunications: Model Ordinances

Reference Number: MTAS-757

Cities needing to update their telecommunications ordinance should avoid the urge to simply adopt a model telecommunications ordinance or the ordinance and specifications currently in place in a neighboring community. While many of these ordinances are quite good, there are unique geographic, environmental, and political factors in every community that should be carefully considered before adopting an ordinance. Model ordinances should be used as a starting place for cities wanting to adopt a modern telecommunications ordinance, but such ordinances should be modified to reflect the local situation.

An example of telecommunications facilities ordinance: Model Wireless Telecommunications Facility Siting Ordinance; PCIA The Wireless Infrastructure Association, 2012 [9].

Issues Regarding Siting of Telecommunication Towers

Reference Number: MTAS-758

Specifics to be Decided by the City

In modifying any particular model ordinance, your city should make amendments that will answer the following questions, based on your community's needs and preferences:

1. What types of antennas will be affected by the ordinance?
Cities usually exempt certain types of antennas from their zoning regulations. These include television satellite (dish) antennas and "receiveonly" antennas, which can be as simple as a piece of wire stretched between trees to receive shortwave radio broadcasts.

Counties often exempt amateur (or "ham") radio towers from compliance with their antenna facilities ordinance, presumably on the grounds that such facilities are built in sparsely populated areas and will not affect neighboring properties. Cities, however, should carefully consider regulating amateur radio towers that are excessively high.

Some city ordinances require construction permits for amateur radio towers that exceed specific heights (for example, 45 feet for a ground-mounted antenna and 30 feet for one mounted on a building).

2. How shall we encourage colocation?
Out of a concern that their communities may one day be overrun with antenna towers, some cities require tower applicants to conduct studies to determine if other facilities in the area would be suitable for antenna placement. These might include space on an existing tower that could be leased by the applicant to place an antenna or space on buildings, water towers, bridges or other tall structures that might be leased for antenna placement.

If the applicant's tower proposal is otherwise acceptable, some cities require that the tower be built in such a way that it can accommodate other antennas in the future, thus reducing the need for more antennas in the area. In cases where a new tower is proposed, some cities require applicants to thoroughly inventory all colocation opportunities in the community and explain why such opportunities have been rejected by the applicant.

Colocation studies are expensive (the costs should be paid by the applicant) and may be controversial. Still, such investigations can prevent the creation of "antenna farms" in certain areas of town.

3. How do we protect the community if the tower is eventually abandoned?
A city may opt to require tower applicants to post a performance bond guaranteeing the safe demolition of a tower in the event it is ever abandoned. This can be valuable to the city in the aftermath of a tornado or an occurrence where the tower owner may not have the resources to repair or demolish the tower.

4. How can we protect the community against poor maintenance of the tower?
The city might consider a requirement that telecommunications towers are inspected periodically by a qualified professional engineer registered in the state of Tennessee, and that a copy of such inspection report be filed with the municipality's building inspector.

5. How do we recover the cost of evaluating the permit application?
Properly evaluating a permit application requires consulting with a variety of professionals whom the city may not regularly employ (i.e., structural engineers, telecommunications engineers, telecommunications lawyers, etc.). In developing its tower ordinance, the city should take care to see that the cost of hiring such consultants is recovered in the applicant's permit fee. Due to the expertise required, it is doubtful that a city's normal building inspection fees will be sufficient; a separate fee schedule should be considered with all such fees paid by the applicant prior to permit review.

6. Should the city permit the tower owner to add facilities or change the design?
The city should require the tower owner to secure an additional permit for each antenna proposed for placement on the tower. This will assure that (a) wind loading standards are not exceeded, and (b) police, fire and emergency radio communications are not degraded or disrupted. The original construction permit likely will not take these factors into account.

7. For how long should a tower construction permit be valid?
The city should set reasonable deadlines for a permitted tower construction to be completed. The permit should not be open ended. The ordinance should encourage prompt completion and allow the city to revoke permits that fail to meet deadlines.

8. How can the city minimize the confrontational aspects of the permit process?
The city can encourage the development of modern, state-of-the-art telecommunications by adopting and uniformly enforcing a clearly written tower construction ordinance. Additionally, the city might consider a two-stage application process. In the preliminary stage, the applicant is made aware of the city's construction standards before incurring the costs of developing final construction plans. This may help the applicant avoid expensive, "back-to-the-drawing-board" costs after presenting final plans to the city.

9. How can the community's aesthetics be protected?
To most people, a telecommunications tower will be seen as having a negative impact on the landscape of the community. There are a few ways such an impact can be mitigated. The city should consider adopting an ordinance that:

- Limits the number of towers in the line of sight of historic neighborhoods and other scenic resources;
- Encourages the planting of vegetative screening or construction of screening fences;
- Requires setbacks that minimize interference with scenic resources; and
- Requires the telecommunications facility to be painted colors that blend with the surrounding natural or architectural environment. Muted colors, earth tones and subdued hues should be encouraged.

10. How can we encourage the owner to keep the tower secure?
The city should consider a requirement that all telecommunications towers are fenced to discourage intruders. Additionally, cities can require the owner to include telemetry and alarms to alert when illegal entry occurs or when tower lights are not functioning.

Siting Telecommunication Tower Resources

Reference Number: MTAS-759

A good information source for siting telecommunications towers can be found at the website of the Federal Communications Commission [10].

The FCC's preliminary application to construct or alter a telecommunications tower (FCC Form 854 [11]).

Forms for notifying the FAA of a proposed tower construction or alteration (FAA Form 7460-1) are difficult to access via the Internet. Instead, prospective applicants should contact the FAA's regional office at 1701 Columbia Avenue, College Park, GA 30337 or call (404) 305-5685.

Forms [12] for registering telecommunications towers with the Tennessee comptroller of the treasury

Competitive Cable & Video Services Act

Reference Number: MTAS-1395

One of the most expensive lobbying efforts in Tennessee history resulted in passage of the Competitive Cable and Video Services Act, T.C.A. § 7-59-301 which took effect on July 1, 2008. Following is a brief summary of the salient points of the legislation with which city officials and employees should be familiar.

Current franchise holders — The current holder of a city franchise may apply for a state franchise, whether or not the local franchise agreement has expired.

Current franchise agreements — The terms of a current local franchise agreement may be adopted by any other cable company that wants to provide services in the city.

Notice — The applicant for a state franchise is required to provide notice of filing an application to the mayor of each city in the proposed service area.

City action required to preserve PEG channels — After receiving notice that an application has been filed, a city must notify the state of any public, educational, and government access channels provided by the incumbent cable company.

City action required to preserve free cable service — If an incumbent cable provider offers free cable service to schools or government offices, the city must provide a list of locations at which free service is provided to the incumbent cable company. If the cable company applies for a state franchise, any cable service provided free must continue until the termination date of the local agreement.

This legislation is part of the national trend to diminish or eliminate the franchising authority of cities by granting cable companies the right to provide services without negotiating agreements with local governments. In recent years, several cable companies operating in Tennessee permitted local franchise agreements to expire and refused to negotiate contracts with cities in anticipation that legislation would be adopted that would give cable companies great advantages in negotiating new agreements. This tactic has paid off, as this law essentially grants a statewide franchise to these companies. Current franchise holders may now terminate their local agreements and seek a state franchise. A city that has previously negotiated a franchise agreement with one cable provider may be forced to permit other cable companies to serve its area under the same terms and conditions of the existing agreement.

The Tennessee law is actually more favorable to cities than competitive cable laws passed in other states, thanks in large part to the efforts of the Tennessee Municipal League. Tennessee cities may receive public access channels through the state franchise, and may receive financial support for public access channels. Unlike similar legislation in other states, the Tennessee law requires that franchise fees be paid directly to cities rather than routing such funds through a state department. The 5 percent franchise fee cities will receive is much higher than fees set by legislation in other states, and it is higher than the fees most cities received under negotiated franchise agreements. Considering the numerous laws passed as a result of the nationwide effort by the telecommunication industry to eliminate local control over cable services, Tennessee cities actually fared better than their counterparts in other states.

State Franchise Authority: Application

Reference Number: MTAS-1396

Application Process

The Competitive Cable and Video Services Act permits cable companies and video service providers to apply for a state-issued certificate of franchise authority, issued by the Tennessee Public Utility Commission. Large companies need file only one application to obtain authority to operate in any area of the state. The application consists of an affidavit signed by an officer or partner of the company which, among other requirements, describes the area to be served and affirms that services will be provided within 24 months of the issuance of the state certificate. If the company fails to provide the services within 24 months of receiving a certificate, the certificate becomes null and void, although the company is permitted to provide an explanation of the reason for the delay. In addition, the application/ affidavit must describe the applicant's customer service complaint process and contact information for customers, but the Public Utility Commission will not review or evaluate the complaint process. Notice is required of the filing of the application for all local governments included in the proposed service area. The application must also include a minority-owned business participation plan.

After an application is filed, the Public Utility Commission will determine if the applicant has the management, financial, and technical qualifications to provide the cable or video services to the areas proposed. The Commission may require the applicant to file a plan for compliance, explaining how the company will meet the 24-month deadline for providing services. These service plans or plans for compliance are confidential and may not be obtained by the local governments included in the proposed service area.

Large telecommunications companies have a distinct advantage in the application process. Applications filed by large telecommunication providers, defined as companies with more than 1 million telecommunication access lines in the state, are not reviewed by the Public Utility Commission to determine whether they can provide services to the proposed areas. Rather, these companies are presumed to have the required capabilities. Large companies also have a shorter review period after an application is filed. The Public Utility Commission must act on an application filed by a large telecommunication provider within 45 days of filing, or the certificate will be granted automatically. For smaller companies, the time for the Commission to act on their applications is 180 days after receipt. The certificate issued when the time expires without action is temporary, pending final approval or rejection by the Public Utility Commission.

State Franchise Authority: Rights Granted

Reference Number: MTAS-1397

Rights Granted

The state-issued certificate of franchise authority provides authority to construct, maintain, and operate facilities within the public rights of way, subject to the police powers of local governments. No city can require a cable or video services provider to obtain a local franchise agreement, and no additional taxes or franchise fees may be levied by cities on the operations of these providers. The state-issued certificate is valid for 10 years, after which the provider must reapply.

Local ordinances governing utility pole attachment and construction activities in public rights of way remain effective, but not to the extent that permission to attach to utility poles or to use the rights of way may be denied to a company holding a state franchise. The holder of a state franchise must still provide required notice to a city before installing lines in its rights of way or attaching to poles and, further, must repair any pavement or property disturbed during installation. Permit fees also may still be collected by cities.

State Franchise Authority: Franchise Fees

Reference Number: MTAS-1398

Franchise Fees

The law requires the statewide certificate holder to pay a franchise fee equal to 5 percent of the holder's gross revenues derived from subscribers located within cities and counties, advertising services, and commissions for cable and video home shopping services. (This requirement may differ for incumbent providers. See discussion of incumbent providers.) Revenues received from nonsubscriber services, such as advertising and home shopping commissions, are computed by multiplying the ratio of subscribers located within a municipality to the total number of the company's subscribers.

Franchise fees must be paid to the municipality within 45 days of the end of the quarter to which the payment applies. A city may audit the business records of the holder of the state certificate, but only for time periods within the previous three years. These audits may occur only once annually. All records reviewed by agents or employees of a municipality during the audit are confidential and not open to the public under the open records law. Each party must bear its own costs incurred in connection with these audits, although some relief is provided to local governments that must send agents or employees out of state to review records when the out-of-state audit results in a final determination that the holder underpaid the franchise fee by more than 10 percent. In these cases, the holder of the certificate must reimburse the city for travel costs incurred by the auditors or reviewers.

The law provides that complaints relating to the payment of franchise fees may be filed with the Tennessee Public Utility Commission by local governments or by certificate holders seeking refunds. The holder of a state-issued certificate may request a refund of fees paid to a city within five years of the end of the latest quarter. Either party may file an action in court to determine the correct amount of franchise fees due to a city within six months after a final determination by the Public Utility Commission or within one year after the complaint is filed with the Commission. A city may contract with the comptroller of the treasury or a third party to audit or review records. The law forbids compensating either the comptroller or third party on a contingency fee basis.

Incumbent or Current Franchise Holders

Companies currently providing cable or video services under a local franchise agreement that has expired may either negotiate a new franchise agreement with the city or apply for a state-issued certificate of franchise authority. By applying for a state-issued certificate, the provider receives interim authority to continue to provide services in the area.

An incumbent cable service provider operating under a franchise agreement on July 1, 2008, may terminate the local franchise agreement by filing an application for a state-issued certificate for that service area. The local agreement will be terminated on the date the certificate is issued to the applicant. Large companies operating under franchise agreements in numerous jurisdictions may operate under a state-issued certificate in some markets while continuing to operate under local franchise agreements in other areas. The law permits cable or video services providers to terminate specific franchise agreements without canceling all local agreements.

In an effort to “level the playing field,” the law provides that cable or video services providers seeking permission to provide services to an area in which an incumbent provider operates may simply adopt the terms of a negotiated franchise agreement between the incumbent and local government. The city is required to enter into agreements having the same terms and conditions with any service provider making such a request. These agreements entered into after July 1, 2008, remain effective through the expiration date without the option to terminate that the law provides to incumbent service providers.

Customer Service Complaints

Reference Number: MTAS-1399

Customer complaints against holders of state-issued certificates of franchise authority may be filed with the Tennessee Public Utility Commission. The law states that the customer should first follow the procedures in the service agreement before bringing a complaint to the state. The Public Utility Commission will apply the service agreement standards to determine if the provider has violated the agreement. There is no authority for the Commission to award judgments or levy penalties for violations of customer service agreements, but the Commission may order the provider to cure the violation or to provide a service credit for the time the customer’s service was affected. The maximum service credit that may be ordered is three months. The Tennessee Public Utility Commission may address only individual customer complaints and may not launch investigations into a provider’s service standards or regulate how the provider generally complies with customer service standards.

The statute contains anti-discrimination sections prohibiting the holders of state-issued certificates of franchise authority from discriminating against residential subscribers because of race, income, gender, or ethnicity. Twenty-five percent of households with access to services by a state franchise holder must be low income households within 42 months of the provider receiving the state franchise. Satisfying this requirement will provide the holder of a state-issued certificate with an affirmative defense against allegations of discrimination. The statute establishes a process for claims of discrimination against holders of state-issued certificates of franchise authority. Complaints may be received and investigated by the Tennessee Public Utility Commission. If a determination is made that the holder violated the anti-discrimination portion of the statute, the Commission has the power to levy fines against the state-issued certificate holder.

PEG Channels

Reference Number: MTAS-1400

When a cable service provider applies for a state-issued certificate to serve a city, the city must notify the state of the number of any public, educational, and government access channels (PEG channels) that are in use or have yet to be activated under any existing franchise agreement. In addition, the city’s notice must include the terms under which such PEG channels are provided under the existing agreement. This information is required to be filed with the Tennessee Public Utility Commission by the city, even if the application is not filed by the incumbent provider. Within 90 days of providing cable services, the holder of a state-issued certificate must provide the same number of PEG channels, under the same terms, as the number the city has activated with the incumbent provider.

The number of PEG channels a city is entitled to receive is the number provided under the existing franchise agreement on January 1, 2008, even if the agreement expires or is terminated for a state-issued certificate. Cities receiving no PEG channels under an existing franchise agreement may make a written request that PEG channel access be provided by the cable company serving the area, and the company must provide access based on population of the area served. Up to three PEG channels must be provided to a city with 50,000 or more households; up to two PEG channels for a city having fewer than 50,000 but more than 25,000 households; and, one PEG channel for a city with fewer than 25,000 households. The cities and counties served in the area shall determine how the PEG channels will be shared by the local governments.

The operation and content of programming for PEG channels is the responsibility of the local governments. Holders of state-issued certificates of franchise authority must transmit PEG channels by either interconnection or transmission of the signal from each PEG channel programmer's origination point. State-authorized PEG access support fees are available to cities in amounts not to exceed 1 percent of gross revenues. Incumbent agreements requiring PEG support fees will remain in effect. Local governments not receiving PEG access support fees under existing franchise agreements may adopt an ordinance or resolution requiring the holder of a state-issued certificate to make PEG support payments to the county or city. However, the PEG access support fees, combined with the franchise fees, may not exceed 5 percent of gross revenues.

Incumbent cable service providers that provide free cable service to schools or government offices in a city or county must continue to provide free service to those areas until the termination date of the existing agreement. The city or county must provide a listing to the cable company of locations at which free service is provided. Any other cable or video service provider or holder of a state-issued certificate that serves the same area must provide free service to the same locations.

Underground Utilities

Reference Number: MTAS-1509

In construction or redevelopment projects in which utility lines are to be placed underground, local governments must require developers or property owners, as a condition of receiving permits, to give at least 60 days notice to the cable or video services provider of dates on which the service providers may install their conduits or other equipment in the open trenches. Failure to serve this notice will result in the developer or property owner bearing the cost of new trenching for the installation of the cable or video services providers' equipment.

Developing an IT Disaster Recovery Plan

Reference Number: MTAS-2116

A disaster recovery plan (DRP) should be a collaborative process. At the minimum, you will need to have a knowledgeable representative from each department or area of the city that is touched by Information Technology. By involving as many of your users as possible, you will increase your ability to capture all the necessary information. Each representative will provide you with information about the types of services, software, and hardware that they would need in order to perform their respective jobs.

Step One

Your starting point for DRP should be a comprehensive inventory of hardware (servers, desktops, laptops, printers, wireless devices, routers, switches, etc.), software applications, and data. Your goal is to account for everything you would need to do business in the event of any or all types of disasters. Consider and document the different types of disasters that you are planning for and include disasters that your area or location might be more prone to for the specific location. For example, city hall is located in a flood zone. Include everything you would need to work at city hall or your disaster recovery site with redundancy, if physically and financially feasible (power, data connectivity, equipment, etc.).

Step Two

As part of the inventory, or once it is complete, take the time to classify or understand the impact level of your data and/or the security classification of the data. This information will be useful in the development of an IT Security Plan, a Business Continuity Plan, as well as with the DRP. Also make

note of where the data is located (server drive or local PC). The Federal Information Processing Standard 199 (FIPS 199), Standards for Security Categorization of Federal Information and Information Systems (2004) [13] defines three security objectives for information and information systems:

- Confidentiality – A loss of confidentiality is the unauthorized disclosure of information.
- Integrity – A loss of integrity is the unauthorized modification or destruction of information.
- Availability – A loss of availability is the disruption of access to or use of information or an information system.

Each of these is evaluated for the level of potential impact on the organization or individuals should there be a breach of security, loss of access, or in this case, a disaster of some sort.

- Low – The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
- Moderate - The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
- High - The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

While the availability is the most important security objective for developing your DRP, you need to keep all three objectives in mind during the planning process, as well as during a recovery process, to avoid breaching or compromising either of the other two during a recovery or disaster scenario.

Step Three

Once you have completed the inventory, including security classifications, you are ready to create the DRP. Begin developing the DRP based on the services you need to provide immediately following a disaster. Classify your hardware based on the same structure outlined above, as this will help you triage your equipment, in the event of a disaster. The DRP will help you reassign equipment from less critical services to more critical applications in order to get them up and running sooner, or until you are able to replace affected hardware. Classifying your hardware and equipment will be especially helpful if you plan to use existing low-use or low-priority equipment as your DRP replacements.

Step Four

Once you have a final DRP in place, you will want to test the DRP. Use the testing process to evaluate and further tune your DRP. You will want to update or evaluate the DRP annually to make sure that it stays current. Also, make sure to revisit the DRP as your environment changes.

Helpful Links

U [14]T Emergency Management Policy [15]

UT IT0128 - Contingency Planning [16]

Metro Government Nashville IT Contingency/Disaster Recovery Planning [17]

N [18]IST Computer Security Resource Center - Disaster Recovery Documents Search [19]

NIST CSRC SP 800-60 Vol. 1 Rev. 1 [20]

NIST CSRC SP 800-60 Vol. 2 Rev. 1 [21]

N [13]IST FIPS PUB 199 [22]

Disposing of a PC

Reference Number: MTAS-1391

Disposing of old computer hardware by auction or donation is a good way to get rid of older personal computers (PC) and provide them with a second life, which is also good for the environment. These are two noble ways to dispose of an old PC; however, something to keep in mind is that the hard drive on that PC could contain a treasure trove of information. A few examples of information that could reside on the hard drive are:

- Billing information;
- Credit/Debit Card Numbers;
- Driver License;
- Passwords; and
- Wireless Network Access Codes.

There are data thieves who purposefully mine places such as public auctions, flea markets and garage sales. These data thieves purchase old hard drives with the intent to find personal information to sell on the Internet. Not only do these thieves seek information on personally-owned equipment, they also look for public auctions of equipment such as PCs, printers, fax machines, copiers, etc. as all of this equipment contains hard drives and bits of electronic information that can be mined for profit.

According to the Tennessee disclosure statute (T.C.A. § 47-18-2107) releasing unencrypted personal information in this manner would most likely be considered a data breach. This, at the very least, would incur the notification section of the statute but could also go as far as a civil action against the information holder. In addition, the Fair and Accurate Credit Transactions Act (FACTA) contains a specific rule specifying the proper disposal of consumer information, which includes electronic records. FACTA also outlines penalties for “willful noncompliance” that also could include civil liability and punitive damages. Outside of what is required by law or statute it makes good cyber security sense to assure you do not have data left on an old PC.

For example, you have audited all your municipal PCs and know that you do not have any business processes that require you to gather and store consumer information, therefore not calling into effect either of the above instances. However, a PC might have an unencrypted file containing all of the user’s passwords, compromising that user or wireless network settings and puts the municipality’s wireless network security at risk, allowing someone access to municipal information technology (IT) resources.

A municipality should establish a written policy or procedure outlining the disposal process from start to finish, including methods of removing all data from existing PCs. The two options for removing the data from a hard disk are either a software tool to wipe (erase/overwrite) the data or physical destruction of the hard disk. Just deleting the files on the hard drive or reformatting and reloading the Operating System are not sufficient means to completely remove the data. If this has been your chosen method, the files can be recovered fairly easily.

A simple Internet search will help you find a number of good data recovery tools to retrieve files that have been deleted from the hard drive or other removable media. Some recovery tools will even work on drives that have been reformatted. I have used a few to recover photos and other files that have inadvertently been lost or deleted from PCs, memory cards, USB drives, etc. Most recovery tools have graphical user interfaces to make recovery as simple as possible. Most of the tools were not designed for nefarious reasons but could easily be used in such a manner. More sophisticated tools exist, but have a difficult time recovering data when using either of the data destruction methods discussed.

Written Destruction Procedures

Reference Number: MTAS-1392

Establishing a written procedure will help to assure everyone involved that the municipality has planned ahead and thought through the entire process of PC/data disposal. The plan should include the method of removing the data from all IT equipment so you can be assured that unencrypted data is not leaving your organization unintentionally. This policy should include a list of equipment that you know has or could potentially contain sensitive information. It could include copiers, fax machines, servers, laptops, smart phones, desktops or basically anything that contains a disk drive (memory) and stores information. You would also want to outline the basic process for each device. For example, you could use the same process for all of the hard disk-based equipment, but you might have to use a different process for a smart phone. Next, you would outline the process you will use to auction or donate the equipment. This could include your method of selecting the receiving entity.

PC Destruction

Reference Number: MTAS-1511

Software Destruction

A couple of software tools for software destruction include Blanco Drive Eraser [23] or KillDisk [24]. The Blanco Driver Eraser has a free single license trial. The cost for a license is around $19 per license and requires a license for each drive erased. KillDisk offers a number of paid versions ($55-$100) based on how many parallel erasures you would like to do at one time and other additional features with each version. Both vendors allow you to download the .iso file from their website. The .iso file is a CD or DVD image file that you will need to burn to the appropriate media. Windows versions Vista and later are able to do this natively, but Windows XP will need a third party utility such as Nero, Sonic or Ulead in order to burn the .iso file to CD/DVD. Once the .iso file has been burned to CD or DVD, you will then start from this CD/DVD on the PC containing the hard disk you would like to wipe. KillDisk also offers a "bootable USB/Floppy creator" that will allow you to create a bootable USB with the KillDisk DOS utility that will accomplish the same wiping task. This runs faster than booting from CD/DVD but essentially works the same. This will be a good option for PCs that do not have an optical device. NOTE: This procedure cannot be reversed. Once you have started wiping the disk, you will no longer be able to retrieve the data.

Both Vendors also offer a free version. However, both are only licensed for home/personal. The free versions are not designed to be used in a work environment and do not guarantee complete removal of all data. They also do not provide any verification of the data removal. The paid versions will remove all data (with different options for data removal) from an existing hard disk and render it very difficult, if not impossible, to recover. I would recommend either paid version for use in a municipal environment. Both products offer Third-Party certifications and approvals of compliance.

The biggest advantage of the software method is that it does not destroy the hard disk. This allows the hard disk to be reformatted and the OS reinstalled afterward, allowing the computer to be set up and once again become a functioning computer.

The biggest advantage of the software method is that it does not destroy the hard disk. This allows the hard disk to be reformatted and the OS reinstalled afterward, allowing the computer to be set up and once again become a functioning computer.

Physical Destruction

The second method of purging the data is physical destruction of the hard disk. This can occur in many ways, including a sledge hammer, industrial shredders, degaussed, etc. However, with this method, you are destroying the media so the PC would have to be sold/auctioned/donated without a hard disk. Depending on the information that was stored on the hard disk, this may actually be the preferred method. For example, if you have lots of confidential information (names, addresses, credit card numbers or Social Security numbers), you may want to choose physical destruction. Some advantages of this method include ease of use, time (typically much faster) and convenience. The software method of wiping data removes the data and then writes a series of 1s, 0s and random characters to the entire surface of the disk. KillDisk Professional defines the US DOD 5220.22-M standard as three complete writes of data across the disk. Both free versions of the software tools only make a single pass across the disk, effectively taking one-third the amount of time. Depending on the number of writes that you choose and the size of the disk, you could be looking at hours or days with some of the larger 1TB drives. However, with a sledge hammer and the proper safety equipment, destruction can be handled in a short amount of time. Just remember to make sure the platters are in multiple pieces when you are done.

PC Disposal Policy

Reference Number: MTAS-1767

MTAS recommends each city have a PC disposal policy.

Electronic Technology Act of 2009

Reference Number: MTAS-1401

Public Chapter No. 96, codified at T.C.A. § 4-30-101 *et seq.* enacted the Local Government Electronic Technology Act of 2009. This act requires local governments to file a plan with the office of the Comptroller of the Treasury before implementing any new electronic technology with a financial component. The stated intent is to encourage local governments to use their existing technological resources before purchasing new and likely costly systems. The burden of justifying new expenses to the comptroller presumably will discourage new purchases unless absolutely necessary.

Specifically, the bill requires a plan to be filed if the new technology is "associated with the disbursement of public funds; purchasing; or the sale of local government assets; or the collection of various taxes, fines, fees or payments." This rather broad definition covers a myriad of new technologies, including credit card processing systems, computerized billing systems, and accounting systems with check processing capability, and it likely encompasses all financial functions of a municipality.

Upon determining that the new technology meets the definition, the municipality must then file a plan with the comptroller at least 30 days prior to implementation. There is no requirement that the comptroller's office approve the plan. The plan must include the following information:

- A description of the business process and the technology to be used;
- A description of the policies and procedures related to implementing the technology;
- Documentation of internal controls; and
- An estimation of the implementation costs and a statement as to whether the plan can be implemented with existing resources of the office or if additional resources are needed and prior approval has been given by the local governing body.

These requirements should pose little difficulty as each should be given full consideration before implementing a new technology, regardless of this legislative directive.

Oddly, the public chapter does not explicitly add to or amend language in any particular section of the Tennessee Code Annotated. Hence, it is unsure where these new provisions will be codified.

Also, notable in the bill is the lack of an enforcement mechanism or penalty for failure to comply. Seemingly, as the program is administered through the comptroller's office, that office will take some measure to ensure compliance. Whether this is done through the audit or another avenue remains to be seen.

This new requirement went into effect immediately upon the governor's signature on April 27, 2009. Hence, any new technology covered by this bill that your city purchases from that date forward must be preceded by a plan filed with the comptroller.

Online Data Backup

Reference Number: MTAS-1775

As we have come to rely on electronic files being ever present on our computers, backing up these files is more important than ever. The target audience for this tip is cities that have a small number of computers, and do not use a central server system for file storage. For cities with a central file storage system, I would encourage you to discuss the current backup plan with your IT department or vendor. Everyone else should keep reading!

Having a backup plan in place is important because the majority of data is stored in a single location, which is generally on the hard drive of a single computer. Hard drive capacity and reliability have steadily increased over the years, but the hard drive is still the most likely piece of hardware in your computer to fail (one to four percent average failure, based on various sources). Other causes of lost data could include a PC being lost, stolen or compromised, software or file corruption, a Ransomware/ Encryption virus or natural disaster, etc. Any of these scenarios could cause you to lose access to your data. If you have data that you cannot replace, is critical to your operation, or would be very time intensive to rebuild, then keeping that data in one place could be catastrophic.

Think about the above data and or documents that you are responsible for and that are necessary for you to complete your job or tasks. This could be data related to a million dollar federal grant, and you must keep this data in order to report on how the grant money is being used or you risk losing the grant. It could be the minutes from a controversial city council meeting pertaining to purchasing contracts for a vendor that will most likely be challenged by the bidders that didn't win the bid. Whatever the data, it only resides on a single few bits within your hard drive.

Imagine the following scenario.

> You come in one day and you receive and email PDF invoice from someone you recognize. You open this email to learn that it is the invoice is for another company. You reply to the email to let them know they sent you someone else's invoice. You open a file before you leave for the day, but the file will not open. It is the end of the day and you decide to lock your computer and head home. The following day you come in, turn on your computer, realizing you are not able to open any of your electronic files. When you open a file it only shows you electronic gibberish. Next, you open your email to find an email from someone you do not recognize but the subject line says that it is important. As you read this email you realize the email is from a hacker. This hacker has encrypted all your electronic data and is holding the encryption keys and the data hostage for a ransom payment of $50,000.

You were the keeper of this data and the burden for its loss is on your shoulders. You have no possible way to recreate this data. Some of the data may exist in hard copy form, or it might be possible to hire a company that specializes in data repair or recovery, but this could be very expensive and or time intensive. The rasomware scenario the only way to retrieve the data is to get the encryption keys. Sometimes if the hacker is paid you will get the keys but sometimes you will not. The most practical way to protect your data is with a backup.

I recommend keeping your data in a minimum of two places, but in some cases using three might be desired.

- Local computer hard drive
- Local alternate media (external hard drive or USB flash memory) - optional
- Cloud storage or Cloud based backup solution

The first location is your hard drive, which is the most convenient and fastest place to access your data. Because the hard drive is usually the default storage location for the computer, it is the most popular. Continuing to use the hard drive as your primary data storage location is acceptable, but just be aware of the potential risk.

The second location can be a USB thumb drive or external hard drive. This location can be your quick go-to for recovery, as well as a portable option. This location is optional and does have some benefits over the third location such as portability, quick access, availability without Internet access, etc. However, if you also add the third location then keeping up with your files in all three locations could become cumbersome, and add unneeded or unjustified complexity to the process. If you have a slow or unreliable Internet connection, this optional location may be necessary. However, if you prefer to use only two locations, then eliminate this one and use option three as the secondary location.

The third location is a cloud-based backup or storage solution. Some cloud-based services could be your primary data storage location, depending on the speed and reliability of your Internet connection and the types of data you are storing. If you are storing Personally Identifiable Data for citizens or customers, you will need to be more cautious with the system that you choose (encryption, security, etc.). Your options for this service vary in features, design, ease of use, and cost. The selection and use of one of these services is outside the scope of this article, but I have included a brief overview and a list of some options. The two overall categories are: 1) backup systems whose primary design and purpose are for data backup; and 2) cloud document systems that were designed for cloud storage of your files (an online hard drive). Some of the cloud services overlap and share some of the same features.

The first category is an online/offsite backup service. If your primary goal is an automated system to back up your files from your hard drive to the cloud (set it and forget it solution) then you should consider the online backup category. Some backup services offer complete backup and restoration of the protected system. Some examples in this category include services such as Acronis [25], Carbonite [26], Crashplan for Small Business [27], Elephant Drive [28], IDrive [29], justcloud [30], myPCBackup [31], and SOS Online Backup [32]. Most of these products offer protection and automatic updating of local

files to the cloud storage. Features to consider are: the restore process, cost, security/privacy, encryption, and whether you can get physical media for the restore.

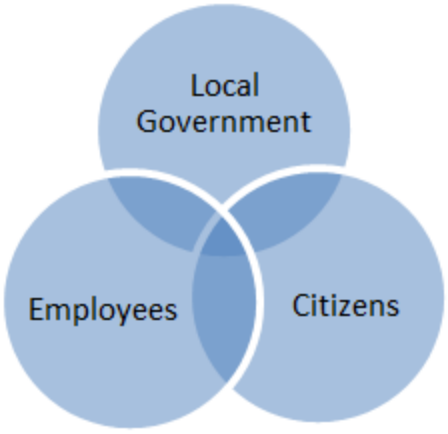
The second category is an online document system of services. These services are primarily designed as an online hard drive. Some of these options include G Suite by Google Cloud for government [33], personal Google Drive accounts, Microsoft Office 365 for governments [34], Microsoft OneDrive [35], Dropbox [36], SugarSync [37], CertainSafe Digital Safety Deposit Box [38] and box [39] that offer both personal and business versions. These services are primarily designed to store your working files, such as Word, Excel, and Powerpoint. Some services store limited file types, while others allow any type of file. A few offer encryption of your data both in transit and while at rest on the cloud storage. This is a very desirable characteristic if you plan to store all your files in the cloud. Some of these services offer a client that you install to make using the service and accessing the files quicker and easier. Various services keep a copy both locally, and in the cloud and keep those files synchronized in all the locations where you use the client. Other services offer a client for smartphones and tablets, as well, so you can access your files from many locations.

In closing, you need to choose a plan that works best for your city. Remember, if your data exists in only a single location and something happens to that data, or if you are not able to access that location, then your data is vulnerable to loss. Take time now to do something about it!

Social Media as a Tool for Government

Reference Number: MTAS-1601

This section will provide your city with information relative to the use of social media for purposes of communicating with employees, interacting with your community, and making hiring decisions. Before we move into “defining social media”, it is important to note that you should proceed carefully when considering your social media strategy and include your information technology department and legal department in any decisions made about the use of social media in order to ensure technical capability and policy compliance.



Social media is a way to use the internet and applications to communicate with people, groups, and other entities using an interactive process. These communication systems (typically accessed via the web with, computers, tablets and mobile devices) allow people to receive and share information quickly and efficiently for various purposes. Social media is a technology that supports a two-way exchange of communication.

Today, social media is a conglomeration of web based tools, forums, websites and other applications that encourages communication between the users of the social media platforms. Common social media programs are: Facebook, Twitter, Skype, LinkedIn, Tumblr, Instagram, Pinterest, Wikipedia, Yammer, YouTube, Snapchat, Xing, Mix, Xanga, Reddit, Yelp, Delicious, Classmates and Wordpress. The social media programs change and evolve with each year, but the concept of interactive web communication is here to stay.

Use of Social Media

Reference Number: MTAS-1602

Social media is a way for people to share information. An account can generally represent an individual, a company, municipality, or a group. While the three primary uses for social media are networking, socializing, and marketing, social media is also used to provide the public with information about city events, schools, traffic, new businesses, weather-related incidents, and new initiatives.

Social Media Statistics

Social media growth has appeared to level off somewhat since 2016 statistics were reviewed. Facebook is still the most popular site. In the United States, Facebook reaches 68 percent of the adult population with three-quarters of those users access Facebook on a daily basis.[1] The newest site to see a surge is YouTube which is not a traditional social site but does have many social element. YouTube is now used by 73 percent of U.S. adults and 94% of 18- to 24- year olds. The 18- to 24- year old segment stands out for using multiple Social Media platforms with 78 percent using Snapchat, 71 percent using Instagram and 45 percent using Twitter multiple times per day.[2] Other popular Social Media sites in the United States are Twitter, LinkedIn, Instagram and Pinterest each with a respective adult internet users proportion of 24 percent, 25 percent, 35 percent, and 29 percent.[3]

As of February 2018, 69 percent of the U.S. public uses some type of social media platform.[4] We are in an age where grandparents, while sitting in the comfort of their homes, are able to visit their grandchildren who live 500 miles away over FaceTime or Skype. Children today do not think twice about sending a video of themselves doing a hand stand to all their friends at school using SnapChat. Our workforce is adapting to the changes brought about by social media in their personal lives and we must help them adapt professionally in our workplaces and our communities.

---

[1] http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/ [40]

[2] Ibid.

[3] Ibid.

[4] http://www.pewinternet.org/fact-sheet/social-media/ [41]

Trends in Social Media

Reference Number: MTAS-1754

The trends in social media include a continued spread across demographics, some consolidation of services, as well as the number of users continuing to rise. Social media continues to add users with greater diversity, especially across age and income demographics. As the numbers have increased this has helped the user base grow more representative of the broader population. Young adults were the earliest adopters of social media but usage by older adults has increased in recent years.[5] Some consolidation has occurred among the different tools. Facebook acquired Instagram in the spring of 2012 for $1 billion dollars in cash and stock.[6] Facebook has continued to operate Instagram as a separate entity allowing the tools to integrate with one another. In the United States, Facebook is by far the most popular social media site. LinkedIn, Pinterest, Instagram, and Twitter are all very close in the rankings with one another. However, the most significant change for users has come in the form of mobile use. Over the last few years it has become clear that the future of social networking is via mobile devices. Smart phones, iPads, iPods, tablets and other mobile devices make connecting with one another much more accessible than being on a desktop computer tethered to a desk.

The number of registered users for each service has continued to climb. Facebook reports 2.2 billion, YouTube has 1.9 billion, Instagram has 1 billion, LinkedIn has 562 million, Twitter has 336 million, and Snapchat has 255 million active users.[7]

The following sections will explore a few popular social media tools but is not all inclusive, as new tools are emerging daily. Before deciding which social media tool will be of most use to your city, you will need to do some research about the demographics in your community. Since the city's goal is to reach as many citizens in the city as possible, it is important to know which social media platforms citizens are using. After your city implements the use of social media, you will want to stay involved in the evolution of social media and continuously look for new ways of doing business through social media, while at the same time remaining cognizant of and being vigilant about not falling into the many pitfalls that come along with the use of social media.

---

[5] http://www.pewinternet.org/fact-sheet/social-media/ [41]

[6] http://dealbook.nytimes.com/2012/04/09/facebook-buys-instagram-for-1-billion/?_r=0 [42]

[7] http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ [43] & https://www.linkedin.com/about-us [44]

Facebook

Reference Number: MTAS-2071

Facebook is a social media site that was started by Mark Zuckerberg in 2004.[8] It was launched at Harvard University. Facebook allowed students to create a profile containing personal information and then find other students in an online location. It started at a single university and then spread to other US colleges and universities. US high school students were the next target audience. Facebook then began spreading worldwide in the education market. In September 2006, the network extended beyond educational institutions to anyone with a registered email address.[9] The founder Mark Zuckerberg is the chairman and CEO for Facebook.[10] He has turned down very lucrative offers from companies wanting to purchase Facebook and continues to maintain a hands-on approach with the company.

Facebook describes itself as the place for people to share and discover.[11] If you want to share the message of your city with as many users as possible, then Facebook is a good place to start. It is a great marketing and communication tool. Facebook covers the widest number of users across all demographic areas, including age, ethnicity, income, education, etc.[12] Facebook also allows you to post most types of information, including text, pictures, short videos, and links to web sites. While Facebook allows you to post lengthy text, it is best to keep your message short and eye-catching. When using any of the social media tools, it is important to keep your post fresh and up-to-date in order to drive activity to your page.

To create a page for your organization, select the “create a page” option. Click the "Get Started" button under "Business or Brand" which will activate the "Name your Page" and "Add a category to describe your Page" fields. After naming the page, start typing "Government" in the category field. Next select "Government Organization" as your category unless one of the other government options is a better fit for the Facebook Page you are creating. This option will allow you to be under the “Amended Pages Terms [45]” for State and Local Governments.[13] The National Association of State Chief Information Officers (NASCIO) (http://www.nascio.org [46]) worked with Facebook in order to get terms that would work better for local and state governments. This option will also give you the benefit of using the publishing tools.

The most important thing to remember when creating the page is to have more than one administrator. In case something happens to one of the page administrators, the other can still perform as the admin for the page. Page roles will allow you to assign users as Admin, Editor, Moderator, Advertiser, or Analyst. The help file in Facebook [47] details what tasks each role is able to perform.

Each individual within your organization who has rights to make changes on the page must first have his/her own individual page and then must be given access to the organization’s page and assigned a role. The person who first creates the page will automatically be given the Admin role.

---

[8] https://www.facebook.com/facebook/info?tab=page_info [48]

[9] http://www.theguardian.com/technology/2007/jul/25/media.newmedia [49]

[10] https://investor.fb.com/corporate-governance/?section=board [50]

[11] https://www.facebook.com/facebook/info?tab=page_info [48]

[12] http://www.pewinternet.org/2015/01/09/demographics-of-key-social-networking-platforms-2/ [51]

[13] https://www.facebook.com/terms_pages_gov.php [45]

Twitter

Reference Number: MTAS-2072

Twitter is an online social networking service that allows users to send and read short 280-character messages called Tweets.[14] People who use Twitter want to consume information quickly and to stay informed. The information you see on your timeline page/feed comes from other accounts that you follow. Following someone on Twitter means you are subscribing to their tweets and when they tweet something you will see it on your home tab. Essentially, you search for and look for feeds that contain information you want. These other pages could be people, businesses, organizations, news outlets, or other accounts you find interesting. A tweet can contain text, links or a picture. Tweets typically contain small text bites with a link that sends you somewhere else to get additional information, much like an electronic billboard. A successful Twitter administrator is someone who is creative and passionate about getting the word out or circulating the message you want to distribute. Twitter accounts must be fresh and active to engage your audience and to attract new readers.

Twitter has different standards and rules and you should read through them prior to creating an account. Here is a link to Twitter policies and guidelines: https://support.twitter.com/categories/56#category_237 [52].

Twitter is always evolving. Twitter users have found creative ways to shorten tweets and to help people follow them or to easily locate a topic of interest. An example is placing the hashtag symbol (#) before a relevant phrase or keyword within your tweet. Twitter users were the first to use the hashtag, which has now been incorporated into Facebook and other social media tools. When the subject of a hashtag becomes really popular, those tweets are identified as "Trending Topics."

The hashtag of a Twitter post should identify the topic of your tweet to help others find your topic through a search. A city can search a hashtag to find out what topics people in the community are talking about or searching for information on. Keep in mind that you do not have exclusive rights to a hashtag, you should never use too many hashtags (best practice is no more than two), and whatever hashtag you are using should be relevant to your tweet.

In addition to tweets, Twitter allows subscribers to send direct messages. When you follow someone on Twitter, you will see their tweets on your home tab. That person is also able to send you a direct message. Your followers are the people who receive your tweets and they can send you direct messages.

Direct messages are similar to emails or group conversations that are only sent to and received by select individuals, whereas a tweet is information and can be seen by anyone worldwide in in a matter of seconds. Direct messages are, by default, only allowed to and from your followers. However, there is a setting you can turn on that allows anyone to direct message you.

---

[14] https://support.twitter.com/articles/215585 [53]

Instagram

Reference Number: MTAS-1756

Instagram is an online social media networking service that allows individuals a place to share pictures and short videos. You are able to tag other users, apply filters and hashtags. People who follow you are allowed to like the content and comment on it. Like Twitter, Instagram has a system of Followers and Following options. You can make your account public or private. If you make your account private, then only the people you allow to follow you will see your content. Lots of Twitter users also have Instagram accounts and use it as the photo/video repository for their Twitter accounts. This is partly because Twitter initially allowed only text in tweets. Since Twitter now allows photos, using an Instagram account as a Twitter repository is a matter of personal preference.

LinkedIn

Reference Number: MTAS-2073

LinkedIn is an online social media networking service designed to connect professionals. Some unique features of LinkedIn are that it can be used as a recruiting tool, a marketing tool, or a sales tool. Microsoft completed its acquisition of LinkedIn in December 2016.[15] When you create your presence on LinkedIn, you have two options: creating a Company page or a Group page. The person tasked with creating and managing either type page must create a personal LinkedIn user account and complete the profile for that user. The Company page has additional requirements that must be met before the page becomes active. The personal profile must be at least 7 days old and have a profile strength of intermediate or higher. The person in your municipality tasked with creating the Company page will need to make several connections to other users on his/her personal profile, must be a current company employee with his/her current position listed in the experience section, and the municipality's email address must be added to the page and then confirmed by LinkedIn. Finally the municipality's email domain must be unique to the municipality.[16] If you are not able to meet all of the criteria required to establish a Company page, you can create a Group page instead. With a Group page, you can choose to make it an open group or a members-only group. Whether you create a Company page or a Group page, set more than one person as the administrator in order to have a backup for administrative duties for the page.

---

[15] https://about.linkedin.com/ [54]
[16] https://help.linkedin.com/app/answers/detail/a_id/1594/related/1 [55]

Employers & Social Media Passwords

Reference Number: MTAS-1393

A number of national trends related to the use of social media and employment practices have surfaced in recent years. Most notably, employers across the country have asked applicants to provide their social networking account information and passwords on job applications. Several states have made this practice illegal through legislation.

Tennessee joined the fray in 2014, passing legislation dealing with this ongoing issue in the form of the ‘Employee Online Privacy Act of 2014 [56].’ Effective January 1, 2015, the act prohibits employers from asking employees for their user names and passwords to social media sites and personal email accounts, as well as prohibiting the employer from compelling the employee to add the employer to their personal contact lists, or accessing personal internet accounts in the employer’s presence.

Your city should be aware that improper use of social media information on applicants and employees may result in claims alleging discrimination, negligent hiring, violation of privacy, and open record conflicts.

In light of several federal laws including, but not limited to, GINA (Genetic Information Non-Discrimination Act) it is critical that employers not seek out information via social media that is not

applicable to the essential functions of the job. In some cases, an employer simply viewing protected information about an applicant can have illegal implications.

If an employer elects to use social media profiles as part of the background check it is recommended that the employer get signed consent from the applicant that outlines exactly what information the city is looking for, and how it will be used in the hiring/employment process. In addition, employers should have a designated trained professional (one who is not involved in making hiring decisions) review this information, and should only pass on information to the hiring authority if it is essential to the job (i.e., poor communication skills, conflict in resume, etc.).

All other non-job-related information that is ascertained should not be shared with hiring authorities and must be redacted. This will help to ensure that personnel decisions are not based upon non-work related or discriminatory information such as disability status, genetic history, ethnicity, age, etc.

Here are a few guidelines:

- Employers should never ask for an applicant/employee's social media user name or password.
- Employers should never ask that applicants/employees log into their accounts during the interview process.
- Employers should avoid asking the applicants/employees if they use certain social media sites, unless the question is job related.
- Employers and hiring authority should not "friend" an applicant or an employee unless the accounts are both job related (i.e., city business) and of a non-personal nature.
- Employers should not create social media accounts for the purpose of searching for information that is not intended to be public or that is a violation of the social media site's terms and conditions.
- Employers should never try to bypass or manipulate a user's privacy settings for the purpose of gaining information and access to an applicant/employee's information.
- Employers should not use technology or third-party applications to draw out information from applicants/employees profiles for purposes of gaining access to the individual's information.
- If an employer elects to use social media searches as part of the hiring/employment process a policy stating exactly what information will be searched for and eventually used must be in place.

What is Fair Game?

- Employers may have a policy that restricts access to social media sites while on the job.
- Employers may have a policy that allows them to use public social media profiles in their applicant screening.
- Employers may follow their own policies and make employment decisions based on job-related discoveries on public social media sites.
- Employers have the right to prohibit use of city logos, uniforms, photos, etc. from employees' personal social media sites.
- Employers have the right to investigate claims of harassment or misuse of city property via social media.
- Employers have the right to prohibit behavior that is harmful to the city or its employees, and may interfere with the city's operation, the employee's job, or department's function.

Other Concerns

Workplace harassment can take place on or off the clock, and happens frequently via social media avenues. Employees should be aware that potentially harassing activity (on or off the clock) may be subject to open records laws and court subpoenas.

First Amendment Rights

Employers may not infringe on employees' or applicants' First Amendment rights. Employees may have the right to express personal opinions on their personal social media pages when off the clock, even if the employer doesn't agree with them. It is important to note that not all personal views on social media are protected from impact on an employee/applicant's job status.

In summation, employer policies should not be overly broad in that they prohibit activity allowed by federal laws such as the discussion of working conditions, wages, and other concerted activity. While the laws are still being deliberated on in many jurisdictions, most legal and human resource professionals agree: spying on applicants and employees sends a poor message that violating applicants'/employees' privacy is an acceptable business practice.

Social Media: Legal Issues

Reference Number: MTAS-1609

Inaccuracies and Context

Employers should exercise caution when looking for information about a person online. Some of what is posted online is not controlled by the applicant or the employee. Additionally, there is always the possibility you are not looking at the correct person's profile or that someone is impersonating an individual. A joke or comment posted on someone's profile by a "friend" in bad taste may not accurately reflect the character of your candidate or employee. A remark taken out of context may appear much more severe than its intent. Most users protect themselves by setting their privacy settings so that their profile is not open to the public. While privacy settings are meant to protect a user's personal information, the settings do not protect applicants and employees against fraud, impersonation, harassment, photo tagging, and photo editing. Employers must develop social media hiring policies that outline exactly how social media will be used in the hiring process. This information should be provided to candidates upfront and before an application is submitted. *Again, employers should use a trained human resources professional to screen candidates based on social media policy. Only job related information should be forwarded to the hiring manager.*

The following topics in this section include more details regarding social media legal issues.

Social Media: Fair Credit Reporting Act

Reference Number: MTAS-1610

An applicant may claim to have legal causes of action if he or she has been turned down for a job as a result of online information. Pursuant to certain provisions of the Fair Credit Reporting Act (hereinafter "FCRA"), an invasion of privacy lawsuit could be established and some experts suggest social networking sites themselves may be vulnerable to lawsuits under the FCRA. Employers should provide a written notice that explains your city may obtain a consumer report for employment purposes. Employers are also required by the FCRA to obtain the applicant's signature before performing a background check and releasing the information This signature should be on a stand-alone FCRA notice and acknowledgement. A job application is not considered sufficient notice under the FCRA. If an adverse employment decision is made based on information discovered through a background check, the applicant should be notified as described in FCRA regulations.

Social Media: Discrimination

Reference Number: MTAS-1611

Discrimination Based on Protected Classes

Most social networking sites show an employer a person's gender or gender identity, race, age, sexual orientation, neighborhood, family members, religious views (or absence thereof), family status, pregnancy status, and political views. In some cases a person's profile may yield direct or indirect information about medical information, genetic issues, and health status. If potential employers have access to this information, how can they guarantee they will not use any of this information to make hiring or employment decisions? Once the information is viewed, there is no way to go back and undo what the employer has learned. This is perhaps, the largest employment risk associated with reviewing online profiles on candidates.

Potential liability arises when an employer uses the information found via social media to affect hiring and or employment decisions. For example, an employer is getting ready to make Sarah an offer, and suddenly finds Sarah's online profile and clearly sees she is pregnant. The employer may change the hiring decision based on the online information, which is illegal. In addition, the employer may have been able to determine Sarah's relative age, marital status, race and even religious and political affiliation. Employers making employment decisions based on information related to protected classes may be a violation of state, local, and federal laws.

Conversely, if the employer makes a poor hiring decision, the city could be accused of being negligent for failing to properly conduct background and pre-employment screening. With court dockets and other public information online, information on potential candidates is easier to obtain. For this reason, every city should have a policy on social networking and its use in the hiring process. Additionally, you should include in your policy if and when social media will be used in background checks and employee discipline and harassment investigations.

Discrimination laws prohibit employers from seeking out information that would disclose protected status information. If you will not ask a candidate if she/he has children in an interview, then it is not relevant to your online search either. Those with hiring or firing authority should be careful in accessing any profile that could reveal age, gender, relationship status, national origin, disability status, pregnancy status, health status etc. Employers should be following their social media policies and only consider legitimate job related information when hiring or making a decision that will impact someone's livelihood. Employers should always have a trained human resources professional administering social media background checks. Information not related to the job should not be forwarded to the hiring manager.

For human resource managers it is appealing to have a wealth of information on candidates. Viewing social media profiles can be a quick way to identify poor communication and grammar skills, offensive photos and remarks, and an exaggerated resume. However, a city must keep in mind that viewing an applicant's social media profiles may put them at risk for violating: GINA, Title VII of the Civil Rights Act, American's with Disabilities Act, the Pregnancy Discrimination Act, and the Age Discrimination in Employment Act. In addition, a city can open itself up to disparate impact and disparate treatment claims.

Social Media: Disparate Impact

Reference Number: MTAS-1613

General Employment Discrimination

In 1971 the Supreme Court formally recognized two primary types of employment discrimination, disparate treatment and disparate impact. Cities using information obtained on social media sites to make hiring decisions may be vulnerable to disparate impact and disparate treatment claims.

Disparate impact involves an employer with a practice that has an unintended, but unfair impact on a protected class. An example of disparate impact would be an employer who relies heavily or solely on social media for recruitment which will exclude certain segments of the applicant pool (i.e., older applicants) that may not use social media in the same manner as another group of applicants.

Employers who solely use social networking as a means to hire or recruit applicants may be vulnerable to a disparate impact claim. Disparate impact can occur when a city uses social media as a sole means to evaluate candidates or a when a city only considers applicants who use social media. It can also become an issue when a city shows preference for those applicants who have a more favorable online status as opposed to those who have a limited presence on social media. Perhaps the most concrete risk of disparate impact is that the population on social media networks is not representative of the real applicant pool that exists. This means this practice may be unintentionally excluding certain classes of applicants such as males, minorities, or older Americans. When using social media as a tool for recruiting and hiring, municipalities must be mindful of the fact that there is a marked difference in social media use in varied demographic groups, and even within those demographic groups there is a difference in the types of users that access different social media sites.

Social Media: Disparate Treatment

Reference Number: MTAS-1614

Disparate treatment involves intentionally different, and often adverse, treatment of individuals based upon their membership in a protected class. An example of disparate treatment may be the evaluation of applicants in a particular protected class through social media and others through another process. This may happen when a city lacks a recruitment plan and neglects other forms of job advertising. Employers should not use the information found on social media sites in an inconsistent way, or in a different way, for applicants applying for the same job. In other words, if you are going to use social media to make judgments about one candidate class, you should look at the same information for all applicants and document this process.

Social Media: Federal Employment Laws

Reference Number: MTAS-1615

As employers, applicants, and employees increasingly use social media for employment purposes it should be noted that cities must consider all applicable local, state, and federal laws in using these media forms. Remember, employment laws are currently the same for an employer who uses social media for any hiring procedure as an employer who does not use social media in the hiring process.

Here are applicable employment laws:

- USERRA / State Military Laws
- TITLE VII
- ADA
- ADEA
- PDA
- GINA

Federal Employment Laws

- ***Title VII of the Civil Rights Act*** prohibits discrimination based on race, color, sex, national origin, or religion. This federal law applies to local government with at least 15 employees. Additional protections have been extended to include pregnancy discrimination and sexual harassment.
- ***Americans with Disabilities Act of 1990 (ADA)*** prohibits employment discrimination based on disability. Also requires employers to make reasonable accommodations to persons with disabilities.
- ***Age Discrimination in Employment Act of 1967*** (ADEA) prohibits employment discrimination based on age forty and up. This applies to applicants as well as employees.
- ***Pregnancy Discrimination Act of 1978*** prohibits discrimination on the basis of pregnancy, childbirth, or related medical conditions.
- ***Genetic Information Nondiscrimination Act (GINA)*** This legislation prohibits employers from using individuals' genetic information when making hiring, firing, job placement, or promotion decisions. It also prohibits improper use of genetic information for purposes of health insurance and employment decisions. GINA broadly defined genetic information to include family members of employees which initially left employers concerned about the implications of using social media to interact with employees.

Social Media: Invasion of Privacy

Reference Number: MTAS-1617

You should be familiar with local, state, and federal rules concerning invasion of privacy. Under no circumstances should a city ask for log on identification or passwords, or use someone else's passwords to access employees' or applicants' social networking accounts. A popular restaurant chain found itself in court after asking employees for this information on a private "group" designed for the purpose of venting about work. The employees won the case because the employer gained unauthorized access to the social network by forcing employees to provide their user credentials.

In another situation, a city in Montana found itself on the front page after asking applicants to provide their user names and passwords as part of the hiring process and background check. The news of this went viral, and city officials promptly retracted their stance. Surprisingly, this was not an isolated incident that only occurred in this municipality.

The courts have stated that employers should not attempt to gain unauthorized access to private social networking profiles/groups for the purpose of spying on employees. Employers should be reminded that there is a risk in attempting to access employee/applicant content that is unauthorized or intended to be private.

Social Media: Off-Duty Behavior

Reference Number: MTAS-1618

A legal grey area exists when it comes to a public employer's ability to regulate an employee's use of social media when he/she is off-duty. In some instances, an employee's social media presence off-duty may be problematic and even dangerous for a municipality. An example of this is when police officers post inappropriate photos of themselves online while identifying themselves as public safety officers or undercover officers or post information that could comprise the integrity of a law enforcement investigation. These issues have prompted many police and fire departments to adopt a department-specific social networking policy.

A municipality may want to consider the following in creating their social media policy:

- Authorized use of uniforms, insignia, emblems, municipal logos and anything related to municipal business
- Anonymous "blogging" or information sharing regarding municipal business
- Discussing work issues or personal thoughts about municipal strategies online
- Protection of sensitive information
- Security of undercover public safety work (present and future) such as an employee's future capacity to move into an undercover position

A municipality should have clear policies in place to address certain off-duty online activity of employees. In public service, the off-duty behavior standard may be set high, particularly for public safety employees.

Because the test for determining whether an employee's off-duty use of social media can result in discipline, or is truly speech that is protected under the first amendment, is fact specific, it is important for you to consult legal counsel and your human resources professional before disciplining an employee for this type of conduct.

Social Media: Disciplining Employees for Online Activity

Reference Number: MTAS-1619

While each case is different and you should rely on the advice of your legal counsel, here are some questions that you should ask before disciplining or terminating an employee for their social media activity.

- Do we have a policy on social media?

- Did this employee's conduct relate to his/her job?
- Is the speech in question protected by law?
- What do we have that constitutes as "proof" of employee misconduct?
- Did the employee admit to the behavior?
- What valid policies, or local, state, or federal laws did the employee violate?
- How have we treated other employees in similar situations?
- Did you consider the issue of location-based services and time stamping (creation/modification time)?

MTAS has received a fair number of questions concerning Workers' Compensation claims and employees use of social media while on approved Workers' Compensation leave. A common issue that arises is the conflict between an employee's activities shown via social media and the employee being out on leave due to what has been reported as an illness or workplace injury. Before your municipality approaches an issue related to social media and workers' compensation consider the following.

Workers' Compensation

- Did the municipality obtain the information about the employee ethically and legally and within the social media site's term of use and within city policy?
- How will this action affect the current workers' compensation claim?
- If the employee is on workers' compensation, did the claims administrator deny claims based on this information?
- If the employee is on workers' compensation, is the employee being formally charged with fraud?
- Is the municipality using the time stamp or the date and time posted as their primary concern or is the content itself a violation of policy?

While some conduct may be viewed as frowned upon, there may be no legal basis for discipline. Before disciplining an employee for off-duty behavior on social media, or behavior observed on social media that conflicts with claims filed by or leave taken by the employee, review your personnel policies as well as your social media policy.

Location-Based Reporting and Time Stamps

The municipality should be mindful that the time stamp (creation/modification time) that appears on social media sites is not an accurate account of what the person was doing at that time. Most social media sites now let users control and often pre-set the time and date that a post is made and user settings can dictate incorrect times based on time zones. In addition, social media sites that use a GPS tracking or location based reporting are commonly incorrect.

Harassment

Social networking provides yet another vehicle for workplace harassment and bullying. Workplace harassment can take place via the internet just as it can in person or in writing. If a municipality is using social networking to promote its own interests, the social media venues should be closely monitored for harassment and potential acts of violence.

Upon discovering an employee is using social media to harass another employee, the municipal employer has a legal duty to address the situation within a reasonable period of time. Employers should treat these incidents just as seriously as an in person harassment situation.

Recordkeeping

If a municipality is accessing social media profiles as a means to make hiring decisions, the information retained is subject to the municipality's record-keeping policies and practices and may be subject to the Tennessee Public Records Act. If a municipality prints a profile, it is likely to contain information that should not be considered in the hiring process. The EEOC's current guidance is for employers to continue to structure non-discriminatory recruitment and selection processes and consistently focus on the job qualifications of all applicants, regardless of the information available to the employer about the applicant through social media. However, if you are using social media profiles as a means of screening applicants, that information should be maintained as a part of your record keeping until such time as it can be destroyed pursuant to the municipality's records retention schedule.

Politics and Social Media

Reference Number: MTAS-1763

Social media is being widely used in political campaigns at all governmental levels. Social media accounts provide news, information on candidates, discussion of the campaign issue, and voter outreach. It is important for your municipality to remain mindful of the fact that the municipality's social media site and all “political platform” sites are to be separate. Employees should be aware that any form of campaigning while on the job is in the majority of cases a violation of public policy.

---

http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/ [57]

Social Media: Frequently Asked Questions

Reference Number: MTAS-1623

Q: Shouldn’t candidates know that their online information could be viewed by a potential employer? Why should I have to provide a written release of this at time of application?

A: Not all social networking users prescribe to the same rules and precautions by making sure their information stays private. It is recommended that you provide a release along with the application that tells the applicant that you will be conducting a background check which may include social networking and online searches. This also provides the applicant with the requisite time to make changes to their privacy settings. In other words, let applicants know up front that a social media background check will be made and indicate how that information will be used.

Q: I had an employee call in sick, but was reported to be posting on her social media profile that she was at an amusement park for the day. Can I terminate the employee for this?

A: It is not recommended that you jump to any conclusions. Social media sites now have the option of backdating posts, as well as future scheduling the timing of posts, so there is no reliable way to know if someone was really at the park when they were supposed to sick. Additionally, social media sites such as Facebook are notorious for being inaccurate when reporting location or status update via GPS technology (see location-based reporting [58] and time stamps). However, if your municipality has conclusive evidence that an employee is abusing their sick leave, and that information is obtained legally and ethically, there would be no reason not to move forward with disciplining an employee for such behavior.

Q: I have an employee out of work on workers’ compensation. He posted pictures of himself doing physical activities that would conflict with his injury report. What should I do?

A: Such information, if obtained legally and ethically, should be forwarded to your municipality’s workers’ compensation provider (e.g., Tennessee Municipal League Risk Management Pool) or an attorney that specializes in workers’ compensation fraud.

Attorneys Gregory M. Duhl and Jaclyn S. Millner (William Mitchell College of Law) produced a detailed legal study on “Social Networking and Workers’ Compensation Law at the Crossroads” in September 2010. Their study can be downloaded from http://ssrn.com/abstract=1675026 [59].

Q: I have an employee that complained of being harassed by another employee online during and after working hours. What is my legal obligation to investigate? How do I handle the investigation if the profile/messages in question are private and not generally accessible?

A: Workplace harassment can occur at or outside of the workplace. If an employee is harassing a coworker online or elsewhere, the municipality has a duty to investigate upon becoming aware. The harassed employee has the duty to provide copies or transcripts of the alleged harassment if contained in private messages or profiles.

Q: Can we restrict all access to all social media sites during work hours?

A: A municipality, via an internet acceptable use policy/social media use policy, can prohibit or allow whatever internet access it deems in the best interest of the municipality. This includes banning employees from accessing the sites on their breaks and at lunch. Be aware, however, that most

employees can access the internet and their social media profiles through a handheld device or a cell phone.

Q: We have an employee making negative comments under our social media stories and announcements. This is reflecting negatively on us as an employer. Should we delete those comments? What about free speech?

A: The municipality's social media site should contain clear posting guidelines which include criteria for removing obscene or inappropriate posts. When an employee is posting in his or her official capacity, the content can be more heavily regulated. However, when the employee is not holding himself out to be an employee, he should receive the same free speech protections as any other citizen. It is also recommended that the municipality not allow free commenting and posting and that all correspondence, comments, and questions (including complaints) be directed to the municipality's email address, website, or office for appropriate handling. The municipality should focus on making its social media site more informational as opposed to interactive, unless there is a way to closely manage daily interactions or disruptive content.

Q: We have police officers who posted pictures of themselves in an official uniform drinking and partying. What can the municipality do about this? What if he/she was not wearing their uniform but their pictures are still accessible?

A: Such situations should be addressed by the department's policy on off-duty conduct unbecoming an officer. The municipality should also evaluate their social media policies to determine if this conduct is addressed appropriately. The department may want adopt a separate social media policy to address off-duty social media behavior. It is important to note, while the conduct may be viewed as unbecoming, there may be no legal basis for discipline.

Q: Can social networking be considered campaigning on the job, and therefore illegal?

A: Yes, if the activities engaged in on social media meet the legal definition of campaigning, then such activity could be illegal while on duty. However, true networking without political endorsement is not likely campaigning.

Q: What is MTAS' stance on using social media in the hiring process? Should we or shouldn't we?

A: MTAS' role as an advisory agency is to make you aware of the implications of such a practice. It will be up to your municipality to determine what role social media plays in your hiring process and background checks.

Q: We have a long-time employee that has cancer. She has authorized us to do a charity dinner on her behalf. Can we put this on our social profile?

A: It is not recommended that you discuss an employee's health condition except for what is included in the scope of business necessity (i.e., FMLA paperwork, ADA etc). An employee's health status and genetic information should be considered confidential and protected information. This health condition should not be advertised by the employer, even if the employer is attempting to do good will.

Q: We have an employee that talks on his personal blog about a serious health condition, but he has never come to us to request an accommodation under ADA. What should we do?

A: Nothing. Under ADA the employee would need to have direct dialogue with the employer (assuming the issue was not obvious). While the employee is not required to use the words "ADA or accommodation," they should be able to articulate a work issue or work barrier before the employer can evaluate the situation and determine if a reasonable accommodation can be made.

Your Website Domain

Reference Number: MTAS-1402

Select the Type of Developer

Selecting a website developer is a pivotal decision because it determines how involved in all of the steps you will need to be. The types of developers vary, but usually fall into one of the following categories: volunteer, in-house personnel, or a contracted individual or company. Each offers its own benefits other than costs, which are outside the scope of this section. In order to evaluate the developers, you will need to consider what you would like to accomplish with your website, as well as

the experience level each developer will offer you. Here is a quick overview of the categories of benefits you should consider when evaluating the developer to use.

BENEFIT	VOLUNTEER	IN-HOUSE	CONTRACTED
Experience level	Varies — requires evaluation	Varies — requires evaluation	Should be the highest
Cost	Free or very low cost	Minimal if personnel are already on staff	Higher than the other two
Development time	Generally slowest	Depends on other duties	Fastest
Quality of end product	Depends on experience	Depends on experience	Highest
Maintenance of website/design	Reliant on volunteer — could be slow	Depends on other duties	Depends on contract

Decide on a Domain Name

Reference Number: MTAS-1768

Deciding on a domain name is important as this will become your web address. The domain name could also become part of your city's identity on business cards, stationery, etc. A domain name consists of a top-level domain and a second-level domain. A top-level domain (TLD), or domain extension, is the part of the domain name located to the right of the dot, e.g., .com, .edu, .org, .gov, or .net. The part of the domain name to the left of the dot is called the second-level domain (SLD) name. This is the readable part of the domain name that refers to the entity or organization behind the Internet address.

The most common TLDs or generic TLDs (gTLDs) are .com, .net, and .org. These common extensions have certain guidelines, but are all options for a city to use. One additional option for a city to use is the *www*.ci.CITYNAME.tn.us form, which is part of the Country Code Top-Level Domains (ccTLDs). Some cities may register a name in all four TLD spaces. For example, if you are the city of MTAS you could register the names *www*.MTAS.com, *www*.MTAS.net, *www*.MTAS.org and *www*.ci.MTAS.tn.us. Shorter names are easier for people to remember, but if you want to include additional identifiers such as "town of" or "city of" that is acceptable as well. That might look like *www*.townofmtas.org or *www*.ci.townofmtas.tn.us.

Select a Registrar

Reference Number: MTAS-1769

This may not be necessary depending on the type of developer you choose. For example, if you are contracting with a professional website development firm, it could manage the entire process for you. It would be good to understand how to Register the Domain Name [60] in case you change companies at a later time. However, you may choose to register your own domain name so that the city maintains control rather than giving that control over to someone else.

The registrar is the retail company from whom you purchase the rights to your domain name. This company should be accredited by the Internet Corporation for Assigned Names and Numbers (ICANN) at http://www.icann.org [61] or by a national ccTLD authority to register Internet domain names. ICANN has authority over all the gTLDs, while the Internet Assigned Numbers Authority (IANA) at http://www.iana.org [62] has authority over ccTLDs.

The registrars for the gTLDs are numerous and the pricing is very competitive. Here is a link to the list of ICANN accredited registrars: http://www.icann.org/registrar-reports/accredited-list.html [63]. Some that you may recognize are GoDaddy [64] and NetworkSolutions [65].

For your ccTLD registration, there is only one registrar and that is Neustar at http://www.neustar.us/ [66]. In order to purchase a domain name such as www.ci.CITYNAME.tn.us [67] you will need to provide specific documentation to Neustar. If you have questions about this process you can email support.us@neustar.us [68] or call 844-677-2878 (Option 1, 2). The current steps are listed below. However, they do change so you should call or email first to confirm the following steps.

1. Print off and sign the .US Domain registration agreement: https://www.about.us/assets/pdf/us-locality-registration-agreement.pdf [69].
2. A city/organization letterhead cover letter
3. A completed delegated manager update template: https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/domain-names/delegated_manager_template.txt [70]

Once you have completed the above documents, send them to the following postal address.

.US Locality Registry

Neustar Customer Service

1650 Lyndon Farm ct.

Suite 300

Louisville, KY 40223

Register the Domain Name

Reference Number: MTAS-1770

The process of registering the domain name may differ slightly depending on the registrar you choose, but will be similar in several ways. First, you will need to provide contact information for your domain name. Four types of contacts exist for all domain name registrations: registrant, administrator, technical contact, and billing contact. Depending on the registrant, additional information may be required. The listed registrant is considered the domain owner. The registrant should be the city and the city's contact information. The administrator is the contact who can interact with the registry or registrar for the domain owner. The technical contact is the person who manages the domain. The billing contact receives invoices for domain registration fees. Each of these contacts can be different entities or the same.

If you are outsourcing your web presence, all of these may have the company or person with whom you are contracting as the contact person. However, you should request in the contract that the city be listed as the registrant.

Most registrars give access to their registration database by letting you create a user name and password when you register your domain name. Therefore, if you allow an outside vendor or person to register your name, and do not have in the contract that the city will retain ownership of the domain name after the contract expires, the company could actually keep the domain name, sell it to someone else, or just let it expire. Getting the rights back to the name could be difficult, expensive and time consuming. If you do maintain your own domain name, make sure that your contact information is accurate because most registrars will automatically list an expired domain name for auction on The Domain Name Aftermarket (TDNAM). Some registrars will give you a grace period to claim the name, but if they are unable to contact you and someone else bids on and purchases the name, you lose the rights to it. You will then be put in the position of trying to purchase your name from the person or company that on the auction.

Point Your Domain Name to your Website

Reference Number: MTAS-1771

This will vary based on the registrar and where your website is hosted. If the registrar is hosting your website, or if you have contracted this out to a vendor, then this should be handled by that party. If you maintain your website in house or with a vendor other than your registrar, you will have to make DNS changes to your domain name. These settings can be obtained from your host company, and the steps to make the changes can be found on your registrar's website. Once your domain name is registered and your website is live, let us know so we can update our records to reflect your new web address.

Written Email Policy Required

Reference Number: MTAS-1069

Tennessee governments — including cities — that operate or maintain an electronic-mail (e-mail) system must adopt a written policy about monitoring e-mail communications.

The written policy must include:

- the circumstances that warrant e-mail monitoring; and
- a statement that the employee's e-mail correspondence may be a public record under Tennessee's Public Records Law and may be inspected by the public. T.C.A. § 10-7-512.

The statute, adopted in 1999, does not require a city to monitor e-mail; that is each municipality's decision. If a city chooses to monitor e-mail, its policy must meet both conditions stated above. In a municipality that does not monitor e-mail, however, the policy must at least satisfy the public record statement requirement.

Should the city monitor its e-mail?

City officials and employees who must answer that question should review the reasons whether or not to monitor e-mail. Some of the reasons not to monitor include:

- the practice may be seen as intrusive and obnoxious;
- distrust between management personnel and employees, and even between employees can be generated;
- monitoring may be expensive, particularly the cost of retrieving deleted e-mail ; and
- monitoring involves some serious legal privacy issues that apply generally to all government employees.

Some of the reasons **for** monitoring include:

- improper misuses could have serious legal and financial repercussions for the city, such as the disclosure of medical or other confidential files or information;
- remarks or jokes disseminated and forwarded by e-mail that may have been intended to be harmless but may be grounds for a suit against the city for creation of a hostile work environment, for racial, religious, or sexual discrimination, or for even libel or defamation;
- software owned by the city may be used to conduct non-city business;
- software may be duplicated illegally for home or other use, which might constitute software piracy copyright infringement; and
- e-mail is subject to the discovery rules in litigation.

What are the major problems involved in monitoring e-mail?

The General Assembly pointed to those problems in monitoring e-mail. In adopting T.C.A. § 10-7-512, it directed that an e-mail study be conducted, *"to balance the privacy interests and practical limitations of public officials and employees with the public policy interests in access to government information."* [Author's emphasis.] The General Assembly said that the use of e-mail by governments creates the following "unique circumstances": generally, telephonic communications are not stored in any form and are regarded as private, but e-mail creates an electronic record that may be used or retrieved in paper format; and e-mail is becoming more common and important, but public officials are not equipped to act

as official custodians of such communications and to determine whether or not the communications might be public records. Certain federal and state statutes and case law also protect the privacy of workplace e-mail communications.

How does the city handle the privacy problem?

Generally, the statutes and the cases that protect the privacy of e-mail in the government workplace permit monitoring of such e-mail where the government employees have been given notice that their e-mail communications are subject to being monitored. The most successful notice is written notice. For that reason, the city can ensure that the e-mail policy it adopts in accordance with T.C.A. § 10-7-512 includes provisions notifying employees that the city intends to monitor e-mail. Employees should be required to read the policy and to acknowledge with their signature that they understand it.

How does the city handle the open records problem?

T.C.A. § 10-7-512 does not require city's to monitor its e-mail. However, if the city decides not to monitor, its e-mail policy must include the statement that employee's e-mail correspondence may be a public record under Tennessee's Public Records Law (T.C.A. § 10-7-503), and subject to inspection under "this part." The "this part" phrase suggests that a person claiming access to a city's e-mail might base his or her claim under both Tennessee's Public Records Law and T.C.A. § 10-7-512.

Most municipal records are open under T.C.A. § 10-7-503, but that law contains several exceptions, including some found expressly in the law, and some found in other state and federal laws. Generally, a city can answer the question of whether a particular e-mail message or document is open or closed by determining whether the "hard copy" of the same e-mail message or document would be open or closed under the law. The answer to some of these questions will be obvious while others will require thought and even legal consultation.

Reminder : Even if the city decides not to monitor its e-mail, it must adopt a policy that contains at least a provision stating that its employee's e-mail may be a public record and subject to inspection under Tennessee's Public Records Law and "this part." T.C.A. § 10-7-512.

Sample Acknowledgement Email Policy

Reference Number: MTAS-1070

ACKNOWLEDGMENT OF RECEIVING AND READING THE POLICY FOR USE AND MONITORING OF EMAIL

I hereby acknowledge that I have received and read a copy of the city of _____'s Policy for the Use and Monitoring of E-mail. I understand that all e-mail communications systems are the property of the city, as is the information received from, transmitted by, or stored in these systems. I understand that, except with respect to certain content deemed confidential by state and federal law, I have no expectation of privacy in connection with any e-mail messages, the use of city equipment, or the transmission, receipt, or storage of information in this equipment.

I acknowledge and consent to the city's monitoring my use of both Intranet and Internet e-mail at any time the city deems it necessary in accordance with its policy. Monitoring may include reading and printing out all electronic mail entering, stored in, or disseminated by the city of _____'s system and equipment. I agree not to use a code, access a file, or retrieve any stored information unless authorized to do so. I understand that this consent is a condition of my employment and/or continued association with the city. I understand all the provisions specified in this policy. Further, I recognize that a violation of this policy may result in disciplinary action, including possible termination.

_____

Employee

_____

Supervisor/Employer

_____

Date

Links:
[1] http://www.mtas.tennessee.edu/reference/records-management-municipal-governments
[2] http://www.mtas.tennessee.edu/reference/retention-schedules
[3] https://gsuite.google.com/products/vault/
[4] https://products.office.com/en-us/government/compare-office-365-government-plans
[5] http://www.symantec.com/enterprise-vault
[6] http://www.emc.com/campaign/ediscovery/index.htm
[7] http://www.zlti.com/data-sources/email/
[8] http://wireless2.fcc.gov/UlsApp/AsrSearch/towairSearch.jsp;JSESSIONID_ASRSEARCH=VdNnNnpdcg1J4y8k33dsfmCPLBGlXfy683wJxTC6nK2HFCPjGKdF!
[9] https://wia.org/wp-content/uploads/Advocacy_Docs/PCIA_Model_Zoning_Ordinance_June_2012.pdf
[10] http://wireless.fcc.gov/siting/
[11] http://www.fcc.gov/Forms/Form854/854.pdf
[12] http://www.comptroller.tn.gov/OSAP/sapform.asp
[13] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
[14] https://universitytennessee.policytech.com/dotNet/documents/download.aspx?docid=158&DocRevisionNum=1&SaveToMyComputer=true&rnd=1513035234851&a
[15] https://universitytennessee.policytech.com/docview/?docid=178&public=true
[16] https://universitytennessee.policytech.com/docview/?docid=167&public=true
[17] https://www.nashville.gov/Portals/0/SiteContent/ITS/docs/Information%20Security/14_ITContingencyDisasterRecoveryPolicy.pdf
[18] http://csrc.nist.gov/publications/PubsSPs.html
[19] https://csrc.nist.gov/publications/search?keywords-lg=disaster+recovery&sortBy-lg=Number+DESC&viewMode-lg=brief&ipp-lg=ALL&a
[20] https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final
[21] https://csrc.nist.gov/publications/detail/sp/800-60/vol-2-rev-1/final
[22] https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf
[23] http://www.dban.org/
[24] http://www.KillDisk.com/
[25] https://www.acronis.com/en-us/business/backup/
[26] http://www.carbonite.com/
[27] https://www.crashplan.com/en-us/business/resources/
[28] http://home.elephantdrive.com/
[29] https://www.idrive.com/small-business
[30] http://www.justcloud.com/
[31] http://www.mypcbackup.com/
[32] https://www.sosonlinebackup.com/
[33] https://www.google.com/enterprise/apps/government/
[34] https://enterprise.microsoft.com/en-us/industries/government/state-and-local/
[35] https://onedrive.live.com/about/en-us/
[36] https://www.dropbox.com/
[37] https://www.sugarsync.com/
[38] https://certainsafe.com/digital-safety-deposit-box/
[39] https://www.box.com/
[40] http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/
[41] http://www.pewinternet.org/fact-sheet/social-media/
[42] http://dealbook.nytimes.com/2012/04/09/facebook-buys-instagram-for-1-billion/?_r=0
[43] http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[44] https://www.linkedin.com/about-us
[45] https://www.facebook.com/terms_pages_gov.php
[46] http://www.nascio.org
[47] http://www.facebook.com/help/289207354498410
[48] https://www.facebook.com/facebook/info?tab=page_info
[49] http://www.theguardian.com/technology/2007/jul/25/media.newmedia
[50] https://investor.fb.com/corporate-governance/?section=board
[51] http://www.pewinternet.org/2015/01/09/
demographics-of-key-social-networking-platforms-2/
[52] https://support.twitter.com/categories/56#category_237
[53] https://support.twitter.com/articles/215585
[54] https://about.linkedin.com/
[55] https://help.linkedin.com/app/answers/detail/a_id/1594/related/1
[56] http://www.capitol.tn.gov/Bills/108/Bill/SB1808.pdf
[57] http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/
[58] http://www.mtas.tennessee.edu/reference/
social-media-disciplining-employee-online-activity
[59] http://ssrn.com/abstract=1675026
[60] http://www.mtas.tennessee.edu/reference/register-domain-name
[61] http://www.icann.org
[62] http://www.iana.org
[63] http://www.icann.org/registrar-reports/accredited-list.html
[64] http://www.godaddy.com/
[65] http://www.networksolutions.com/
[66] http://www.neustar.us/
[67] http://www.ci.CITYNAME.tn.us
[68] mailto:support.us@neustar.us
[69] https://www.about.us/assets/pdf/us-locality-registration-agreement.pdf
[70] https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/domain-names/
delegated_manager_template.txt