RESOLUTION R-18-159

A RESOLUTION OF THE BOARD OF COUNTY COMMISSIONERS OF MANATEE COUNTY, FLORIDA, APPROVING AND ADOPTING AMENDMENTS TO THE INFORMATION TECHNOLOGY SERVICES POLICY; MAKING RELATED FINDINGS; RESCINDING RESOLUTION R-15-70; PROVIDNG FOR SEVERABILITY AND AN EFFECTIVE DATE.

WHEREAS, the advancement of technology, including computers, tablets, mobile devices, computer software and the internet have improved the productivity of the modern workplace; and

WHEREAS, Manatee County Government desires to make full use of these technologies to enhance the efficient and excellent services it provides to the citizens of Manatee County; and

WHEREAS, Florida law prohibits the use of government assets for personal, non-governmental use; and

WHEREAS, the Florida Public Records Act requires Manatee County to preserve for inspection its public records, including electronic records; and

WHEREAS, the Board of County Commissioners ("Board") adopted Resolution R-01-125, creating the County's first comprehensive Information Technology Services Policy ("IT Policy"); and

WHEREAS, in reaction to changes in technology and the law, the Board adopted Resolution R-07-183 and later Resolution R-15-70 to significantly revise and update its IT Policy; and

WHEREAS, the continued evolution and advancement of technology, and the laws addressing it, have resulted in the need to again revise the IT Policy; and

WHEREAS, the revisions to the IT Policy consist of minor grammatical and procedural changes, as well as updated language to comply with the Payment Card Industry Data Security Standard Compliance Project; and

WHEREAS, these revisions will better protect information given to the County by citizens, as well as clarify for agents and employees of Manatee County the permitted and prohibited uses of the County's technology resources.

NOW, THEREFORE, BE IT RESOLVED by the Board of County Commissioners of Manatee County, Florida, that:

1. The Board hereby approves and adopts the amended IT Policy, which is attached hereto and incorporated herein.

2. The County Administrator, or his or her designees, shall communicate the IT Policy to those agents, employees, contractors and other persons or entities to which the IT Policy may apply, shall post them so they may be electronically available, and shall make efforts to train and educate County agents, employees and contractors as to the responsibilities and duties which the IT Policy places upon them.

3. In each contract Manatee County enters into with outside contractors and vendors where access to, use of, or repair or modification of County computers or related hardware, software or internet-based systems is contemplated the contract should require the contractor to comply with the IT Policy.

4. The County Administrator, or his or her designees, shall have the authority to suspend or deviate from the IT Policy on a temporary or emergency basis as may be required to address changes in the law or exigent circumstances. However, if such revisions are recommended to become permanent changes to the IT Policy, the revisions shall be brought to the Board for adoption.

BE IT FURTHER RESOLVED that Resolution R-15-70 is hereby rescinded in its entirety and is replaced by this Resolution R-18-159.

BE IT FURTHER RESOLVED that the provisions of this Resolution are severable such that the invalidity of any one provision shall not operate to invalidate any other provision.

BE IT FURTHER RESOLVED that this Resolution shall take effect immediately upon its adoption.

DULY ADOPTED with a quorum present and voting this 27th day of November, 2018.

BOARD OF COUNTY COMMISSIONERS
OF MANATEE COUNTY, FLORIDA

By: Priscilla Trace
Chairperson

ATTEST: ANGELINA COLONNESO
CLERK OF THE CIRCUIT COURT AND COMPTROLLER

By: Robin Dittmore
Deputy Clerk

APPROVED AND ADOPTED BY RESOLUTION R-18-159

Manatee County
Information Technology Services

Business Value through Partnership…the Service Provider of Choice

Policy

Revised November 2018

Adopted by Resolution R-18-159

Introduction

This policy regulates the use of information technology resources of Manatee County. Due to the County's reliance on information technology in supporting its business, it is required that this policy be understood and closely followed by all persons who access, use, operate, maintain, or otherwise support these County resources.

Violation of the policy may lead to revocation of user privileges and disciplinary action up to and including termination of employment.

Many of the requirements established in this document require specific procedures to be followed. These procedures are defined in the Manatee County Procedures Manual and can be found on the County Intranet.

Use of County information technology resources constitutes a user's acknowledgement, understanding and acceptance of this policy and all County information technology procedures as well as applicable laws referenced therein.

Scope

This policy applies to all users, including Manatee County officers, administrators, employees, temporary personnel, contractors and their agents. It covers systems and information technology assets used in conducting County business, regardless of where the assets are used, or the work is conducted.

Notwithstanding the foregoing, the County may from time to time be required or elect to provide access to the County's information technology resources to users or other non-County agencies which require unique exceptions or adjustments to this policy, such as to accommodate rules concerning personal health information or attorney client communications. In such cases, Information Technology Services (ITS) will work with the requesting party to ensure the security and integrity of County assets is maintained.

Contact Information

Users having questions regarding this policy should direct them to their department director who will consult with ITS.

Generally Applicable Policies

License Agreements

Manatee County requires strict adherence to all vendor license agreements. Copying, using, distributing or altering software in a manner that is not consistent with the vendor's license is strictly forbidden.

Copyright

Use, reproduction, or distribution of copyrighted materials must only be done with the permission of the owner. Unless prior written permission from the copyright owner is obtained, making copies of material from Web sites, magazines, journals, newsletters, and other publications is prohibited. Questions regarding copyright should be directed to the County Attorney's Office.

Privacy

Users of County information technology should realize that their communications are not private and may constitute public records subject to inspection at any time under Florida law.

Unless otherwise prohibited by law, at any time and without prior notice, County management reserves the right to examine messages, files and directories, and other information stored on County devices or traversing County networks and systems. This examination assures compliance with internal policies and procedures and assists with overall management of County information technology systems.

Security Problems

ITS must be notified immediately when:

- Sensitive County information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties.
- County hardware, software, or data is lost or stolen, or is suspected of being lost or stolen.
- Unauthorized use of the County's information technology systems has taken place, or there is reason to suspect it has taken place.
- Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed.
- A computer or other device is known or suspected to be infected with malicious software such as a computer virus and could cause damage to systems or potential loss of data.

The specifics of security related problems should be treated with discretion, and should not be discussed widely, but shared only on a need-to-know basis.

For additional information on handling lost or stolen information, please reference the Security Incident Response Procedure within the ITS Procedures.

Acceptable Use

Accounts and Authentication

An important aspect of securing any information technology system is identifying users who are authorized to access and use that system. This process is known as authentication. The most common form of authentication is a combination of a username and a password. A username identifies a particular user and should be unique on any given system. A password is a secret that should only be known by the user associated with a particular username. For more sensitive or higher risk systems, stronger forms of authentication are available and may be appropriate depending upon unique circumstances. In all cases, users must comply with all username and password standards, which may include a minimum number of characters, complexity, change intervals, history, and other such parameters.

Those responsible for controlling access to information technology systems, and having specific privileges to grant such access must:

- Follow all policies, procedures and standards;
- Conduct all activity with their own user credentials;
- Not share their passwords or delegate their responsibilities;
- Not write down or otherwise store their passwords where they may be found by someone else;
- Immediately change their passwords when they suspect a security problem with an information technology system, device or account; and
- Use different passwords for personal versus County user accounts.

Office administrators, supervisors or managers shall not require users to disclose passwords, or to compile master lists of passwords. In the event that access is required, such as in an emergency situation, ITS can provide assistance upon request.

The user of a particular username and password combination is responsible for securing that information, and for the activities they perform on a system once authentication has been made.

ITS will work with Human Resources and system owners to enable or disable access for new users during the onboarding process, and to retire users during the off-boarding process.

Internet

Private County Internet services are provided for users and are to be employed for the conduct of County business. While an exemption may be made for limited personal use, the private network is generally not to be used for personal activities or business. Except for Internet content required in conducting sanctioned County business, accessing, storing, and distributing unauthorized or pirated software or content, account and password lists, credit card or other financial data, hacking tools and inappropriate or pornographic content is specifically prohibited.

Users from various County departments are assigned the specific role of maintaining the content of the County's Web sites, and only those users are authorized to post County information on either the County's Web sites or to other social media Web sites.

Users should be aware that standard Internet services, including email, provide no security protection against eavesdropping, forgery, or other risks. As such, sensitive information should not be sent without being protected by encryption, authentication, or other integrity checking mechanisms. County purchasing cards may be used online in accordance with Purchasing Department guidelines and procedures, however, users should not disclose personal information over the Internet such as credit card numbers, passwords, a home address or home phone number, while using a County device. Any user experiencing any type of harassment, threat or other inappropriate contact via the County Internet should immediately report it to the ITS Customer Service Center (CSC).

Public Representations

When engaged in Internet communications with the general public, only those users who are authorized by a County employee at the department director level or above to provide official support for County positions, products or services, may indicate their title or affiliation with the County. These may include a County administrator, information officer, or lobbyist representing an official County position. Whenever such users disclose an affiliation with Manatee County, they must clearly indicate that "the opinions expressed are my own and not necessarily those of Manatee County" unless the position is an official position of the County or they have received instructions to represent the County.

No department, division, user or other person shall create a Web site, page or other presence outside of the official County Web sites that purports or attempts to represent the County or uses any County symbol or logo. Official County Web pages will be based on content and standards established by ITS and approved by Administration or the Manatee County Board of County Commissioners.

Messaging (Email and Instant Messaging)

County messaging systems including email and Instant Messaging (IM) (for example, Jabber) are to be used only for official County business purposes. All messages sent or received by County messaging systems are County records and subject to possible public records disclosure. The County reserves the right to access and disclose all messages sent over its messaging systems for any purpose. Supervisors may review the communications of users they supervise to determine whether they have breached security, violated County policy, or taken other unauthorized actions. The County may also disclose messages to law enforcement officials or members of the public without prior notice to users who may have sent or received such messages.

Use of messaging must not involve non-County business, religious, charitable, political or financial solicitation, and must not contain material which may potentially embarrass the County. The Board of County Commissioners may, from time to time, make legislative findings by way of ordinance or resolution, that the County's partnership with a particular non-governmental entity serves a public purpose. Where the Commission makes such findings, and where the partnership calls for communication to users, the County Administrator may authorize use of the County's systems for that purpose. The text of the transmissions shall abide by the findings of the Commission and shall be free of any commentary or elaboration by users.

Messaging may be used for such things as setting office lunches, however, social discussions regarding such things as romance, religion, sports, investments, and charities, are strictly prohibited. If a user receives an unsolicited personal message from a known sender, the user should respond that the account is only for official business, and if appropriate, the sender should direct further correspondence to the user's personal home account.

In responding to messages, users should limit their response to only necessary users in an effort to mitigate lost productivity attributed to such things as "reply all". Group broadcast or mass mailing features in which everyone is included in the distribution should be kept to a minimum and may only be used with approval of a department director or above.

Users are prohibited from using County information technology resources to engage in free speech activities. Messages sent by authorized users to Internet discussion groups, electronic bulletin boards, or other public forums may be reviewed by County officials and removed if determined to be inconsistent with Manatee County policy. Messages in this category include political statements, religious statements, profanity or other foul language, and statements viewed as harassment based on race, creed, national origin, color, age, sex, military service or physical disability. When practical and feasible, users responsible for these messages will be given the opportunity to remove them.

Users must not use a messaging account assigned to another user to send or receive messages. If there is a need to read another user's messages, such as while they are on vacation, provisions can be made by the user to delegate temporary access to their account.

Signatures

The County email system may provide features that allow text and images to be appended to each message sent. Where applicable, users shall follow the County standards, and in all cases, such contact information should be in a professional format, color and font. Users are not permitted to append any other matter, including:

- inspirational, political, religious or humorous quotes

- images, pictures, graphics, photos, or non-County Web links
- legal disclaimers or confidentiality language unless approved by the County Attorney's Office

Text Messaging

Text messaging shall not be used for conducting County business unless expressly approved by a department director. The only exception to this is for transitory messages such as asking if someone is available to meet or where they are located.

Device Protection and Use

Usage

The use of both County and personal information technology assets for conducting County business must be approved by a department director or their designee. This includes but is not limited to desktop computers, virtual computers, laptops, tablets, smartphones, and other devices that require connection to the County network, systems, or services.

To maintain the proper operation and protection of the County's information technology resources, certain standards are necessary to ensure compatibility and interoperability of hardware devices and software. As such, ITS will establish and maintain a service catalog to select from, and users should consult this catalog or the CSC prior to purchasing a device or software. Users should not connect devices to the County network or make hardware or software modifications without coordinating with ITS first. This is particularly important in cases where personal devices have been approved to ensure that security requirements can be met.

All County-owned mobile devices, including tablets and smartphones, that require connection to the County network, systems, or services, must be enrolled in the Mobile Device Management (MDM) service. Personal devices, requiring access to Manatee County network resources, may also be enrolled.

To prevent unauthorized access, users should logout or lock their computer or other devices when they are away from their station or device.

The proliferation of mobile devices and remote access for County employees are enabling greater agility and flexibility for the mobile workforce. In many business areas, the need for remote access and mobile devices is both desired, and in some cases necessary, given that software application developers are designing extensively on Web-based and mobile platforms. This is creating challenges in managing a diverse workforce having access to County information and the ability to work from any location, at any time; and without regard for exempt or non-exempt status and the Fair Labor Standards Act (FLSA). As such, users who are non-exempt shall not use any mobile device or other computer hardware outside of their approved work schedule to conduct County business of any kind.

Upon retiring any device enrolled in the MDM program, all County information will be removed, and all reasonable efforts will be made to ensure that personal information, where applicable, remains unaffected.

Hardware

Devices should be protected against:

- electrical damage through the use of uninterruptible power supplies (UPS) or surge protectors
- environmental hazards including dust, fire, and water leaks
- theft, loss, destruction, unauthorized access, or misuse

ITS will work with customers to identify risks and appropriate steps to mitigate those risks.

ITS will maintain an inventory of information technology assets, and where applicable, will maintain a program to manage their lifecycle, providing for stability, performance, and overall cost effectiveness.

Upon separation from the County, all hardware and software in use by or assigned to a user must be returned to the appropriate Manatee County department, and access to the County network, systems, and services will be removed.

Software

Unless official information is received to the contrary, users should treat all software on County computers and mobile devices as though it is protected by copyright.

Commercial software purchased by the County is authorized for County use only. Any exception to this rule, such as when a County license includes a provision for home use, will be explicitly communicated to users. Making copies of software purchased by the County for personal use is illegal and prohibited.

Manatee County is not responsible for the legal defense and settlement of any claim where a user has been found guilty of copyright violation or the unauthorized duplication of software, manuals and other documentation.

Where required, ITS will review and authorize software for use on servers, personal computers, and other devices in accordance with its relative importance and sensitivity. In general, large enterprise systems of record and those that are used to acquire, process, and store regulated data will receive the most formal and detailed review. Use of any software found to conflict with, or otherwise negatively impact other software or systems may be restricted.

Music, videos, photographs, games or other software applications that do not directly relate to the performance of assigned duties shall not be resident on or used on County computers or laptops. Software applications used to conduct County business may be purchased and

installed on approved County and personal computers and mobile devices in accordance with the Purchasing Department's guidelines and procedures.

In no event shall audio or video be streamed using the County network on any device for non-business purposes.

ITS will establish and maintain appropriate procedures, standards and guidelines for secure configurations of information technology assets in order to mitigate or reduce risks such as data loss or corruption. This includes installation, configuration, and use of antivirus software on computers, mobile devices, servers, and other hardware. Users must comply with these procedures, standards, and guidelines and shall not circumvent these protections. Users should report to the CSC instances where antivirus or other security configurations are causing problems in performing County business functions.

ITS will develop an approach to update software in use on County networks, systems, and services. Timely software updates to all types of software applications are necessary to provide a stable information technology environment. Users must work with ITS and their vendors to perform updates to vendor applications, and other County software.

Data Protection and Use

Sensitive Information

Information technology is used throughout the County by all departments for a wide variety of functions. Some of this data is very sensitive in nature and requires special protection. Examples include:

- health information, for example, as defined by HIPAA (Health Insurance Portability and Accountability Act)
- law enforcement data, for example, as defined by CJIS (Criminal Justice Information Services)
- payment card information, for example, as defined by PCIDSS (Payment Card Industry Data Security Standard)
- financial records
- personally identifiable information (PII)

Users responsible for creating or maintaining sensitive data should contact the CSC to ensure that adequate protection is in place.

Data security safeguards will be put in place commensurate with the level of sensitivity of the data and will include access controls to ensure only authorized users may read, write, create, delete, or modify the sensitive data. These privileges must be defined in a manner consistent with job functionality.

Encryption may be employed as additional protection for data stored on hard drives, removable media, and backup tapes ("data at rest"), as well as data being transferred over a network ("data in motion"). ITS will establish and maintain encryption standards to ensure the encryption provides the proper protection.

In order to properly manage County information to meet public records obligations, ITS will established standards to mitigate situations where important data is encrypted with a key known to or accessible by only one person.

ITS will provide storage for data and files that is properly managed and backed up. Users must ensure they make use of these facilities in lieu of local storage on personal computers or other devices that are not protected by backups, redundancy, or other safeguards. Users should use local storage and desktop as a scratch pad only and save their data to a networked storage area. If not sure, users should call the CSC for assistance.

Some data may be stored on systems hosted by a third party. ITS will work with users to ensure such data is properly protected.

Users are not permitted to store County data on any computer or mobile device that has not been approved for use by the County.

Users of HIPAA-protected data must also ensure they are familiar with, and comply with, the County's HIPAA compliance rules (as published on the County's web site and the administrative procedures manual) when using, storing, transmitting or otherwise working with such data.

Manatee County has a fiduciary responsibility to taxpayers, customers and payment card processors to comply with Payment Card Industry Data Security Standards (PCI DSS) when handling payment card transactions. As such, Manatee County will maintain a Payment Card Industry Data Security Standard (PCI DSS) Security and Governance Procedure and required related procedures to comply with the PCI DSS Requirements.

Per the Payment Card Industry Data Security Standards, Manatee County employees:

- will not send or request Card Holder Data via e-mail, SMS, instant messaging or similar technologies
- will not take Card Holder Data over the County Phone System
- will perform quarterly credit card terminal inspections, as directed, if your area uses terminals to process credit cards.

Electronic Media Policy

County data shall be stored on County media including but not limited to hard drives, CDs, DVDs, and flash drives. Upon separation from the County, users must leave these assets with their supervisor. A user may not remove any data from the County upon separation unless prior written permission has been obtained from their supervisor.

When being removed from service, either temporarily such as when being sent for repair, or permanently such as when being retired at the end of its useful life; and once adequate measures have been taken to ensure all data is archived and will be accessible, all electronic media shall be securely erased or destroyed in order to ensure that sensitive data is not recovered by unauthorized parties. ITS will establish and maintain standard procedures for this secure data destruction. Many devices beyond personal computers, including copiers, printers, and scanners, may also store data, and users should contact the CSC when removing them from service so that they may be securely wiped as well.

Due to the risk of a portable device being lost or stolen, data shall be backed up prior to using such a device. In no case shall the only copy of sensitive data be stored on a portable device. Regarding data records protected by HIPAA, portable devices and laptops must never be used to transport data or be removed from County buildings absent prior approval to do so.

Public Records

All data captured, created or stored electronically by users under the Board of County Commissioners may be considered a public record under Florida law. Therefore, such data must be properly retained, backed-up and recoverable upon request. Data retention periods are dependent upon various State and Federal regulations, computer application requirements, customer requirements, and the type of information being stored. To facilitate Manatee County's compliance with applicable records laws, the following provisions are established:

- All retention periods for computer data shall be established by the County's Records Manager and shall be based upon the applicable statutes and regulations governing records retention. Retention periods may vary by application.

- Information technology has been implemented to archive all email sent and received by the County email system. In order to provide efficient storage and archives, email system users are encouraged to delete items in their email account if they have no long-term value. Users are discouraged from sending unnecessary copies of an email, and from attaching large data attachments when not necessary.

- Public records requests for computer records and email correspondence shall be directed to the County's Records Manager for appropriate response. Users are not permitted to grant access to records, or to refuse to provide records requested, or to assert any legal exemptions to disclosure, without prior approval of the Records Manager and, if required, guidance from the County Attorney's Office.

- Public records laws are not limited to data stored on County computers. Data transferred to a personal account or computer to allow a person to work away from the office may also be requested, even though the system and account are private. For this reason, users are not permitted to store any County information on personal computers or other personal devices.

Network Protection and Use

ITS will establish and maintain procedures, standards, and guidelines for the installation and operation of County networks and interconnection with other networks. These networks will provide sufficient reliability, performance, and security to meet the business needs of the County.

ITS will provide capabilities to access the County network, systems and services remotely, typically over the Internet. Due to the insecure nature of the Internet, these connections will have additional protection in the form of encryption and authentication provided by, among other things, a virtual private network (VPN) and dual factor authentication. Remotely-connected systems are an extension of the County network and therefore subject to the same rules and policies as though they were connected locally. ITS will establish and maintain procedures and standards for remotely accessing the County network, including from personal devices.

Wireless networking is provided in many County buildings. User devices accessing the wireless network must adhere to ITS standards in order to ensure proper operation, performance and protection. As a courtesy, the County may provide public access to the Internet via the wireless network. The public wireless network may only be used by users for personal business using personal equipment on personal time. All County business is to be conducted on the private wireless network.

Modems should not be used on County Property. Exceptions must be approved by ITS prior to installation or use.

Network infrastructure is routinely monitored and logged to ensure proper operation and security. County systems may also be actively scanned to identify risks and security vulnerabilities.

Manatee County Government Administrative Center
Commission Chambers, First Floor
9:00 a.m. - November 27, 2018

November 27, 2018 - Regular Meeting
Agenda Item #32

Approved in Open Session 11/27/18,
Manatee County
Board of County Commissioners

Subject
Updates to the Information Technology Services Policy

Briefings
None

Contact and/or Presenter Information
Paul Alexander, Director of Information Technology Services

Action Requested
Motion to adopt Resolution R-18-159 encompassing an update to the ITS Policy (November 2018).

Enabling/Regulating Authority
Resolution R-15-70, adopted by the Board on May 19, 2015.

Background Discussion

This Resolution (R-18-159) and ITS Policy will supersede Resolution R-15-70. The updates to the ITS Policy encompass minor changes to include individual awareness and responsibilities in protecting sensitive cardholder data in accordance with the Payment Card Industry Standards and security best practices.

Changes to the ITS Policy include:

1. Additions to the policy to address the requirements of PCI-DSS (Payment Card Industry, Data Security Standards);
2. Minor changes surrounding the use of mobile devices; and
3. Clarification of what constitutes sensitive information such as credit cardholder data.

County Attorney Review
Formal Written Review (Opinion memo must be attached)

Explanation of Other

Reviewing Attorney
Morris

Instructions to Board Records
Distributed to: D. Bassett, L. Stephens, P. Alexander 11/28/18, RT

Cost and Funds Source Account Number and Name
N/A

Amount and Frequency of Recurring Costs
N/A

Attachment: Attorney Response Memorandum.pdf
Attachment: Resolution R-18-159.pdf
Attachment: ITS Policy Revisions PCI 2018 - Final.pdf

OFFICE OF THE COUNTY ATTORNEY

MITCHELL O. PALMER, COUNTY ATTORNEY*
William E. Clague, Assistant County Attorney
Sarah A. Schenk, Assistant County Attorney**
Christopher M. De Carlo, Assistant County Attorney
Geoffrey K. Nichols, Assistant County Attorney
Pamela J. D'Agostino, Assistant County Attorney
Anne M. Morris, Assistant County Attorney
Katharine M. Zamboni, Assistant County Attorney
Alexandria C. Nicodemi, Assistant County Attorney

MEMORANDUM

Date: October 2, 2018

To: Paul Alexander, Director, Information Technology

Through: Mitchell O. Palmer, County Attorney MOP 10/2/18

From: Anne Morris, Assistant County Attorney AMM

RE: Manatee County's Information Technology Services Policy Revision; CAO Matter No. 2018-0467.

This memorandum is in response to the above referenced Request for Legal Services in which you asked this Office to review proposed revisions to Manatee County's Information Technology Services Policy ("IT Policy").

Attached to this memorandum is a redlined version of the revised IT Policy and Resolution 18-159 for adoption. Subject to the inclusion of certain information identified in the comments section of the redlined version, the IT Policy is in legally sufficient form for consideration by the Board of County Commissioners.

This completes my response to your Request for Legal Services. As always, should you have any related questions, please do not hesitate to contact me.

Enclosures
Copies to: Ed Hunzeker, County Administrator
Dan Schlandt, Deputy County Administrator
Cheri Coryea, Deputy County Administrator

* Board Certified in Construction Law

** Board Certified in City, County, & Local Government Law