Information Technology Policy (IT Policy)

Policy Title	**Information Technology Policy (IT Policy)** **Part of Information Security Policy Framework**
Responsible Party	Chief Security Officer ("CSO")
Endorsed by	Information Security Policy Committee
Contact	Chief Security Officer, Stuart Zimmerman; (918) 858-6684
Effective Date	June 1, 2015
Last Update	July 1, 2021

I. Policy Statement

This policy deals with acceptable use of TMA Systems IT and digital resources. It defines acceptable uses for provisioning information technology resources at TMA Systems and the associated responsibility of authorized users when accessing these information technology resources. These resources include, but are not limited to, TMA Systems' network, computer systems and software, access to the Internet, electronic mail, telephony and related services.

As stated in the TMA Systems, LLC Employee Handbook ("Employee Handbook") employees and consultants ("employees") of the Company are expected to be familiar with and adhere to these policies.

The policy is based on the following principles, which must be adhered to by all those responsible for the implementation of this policy and to whom this policy applies:

- The information technology resources of TMA Systems are provided to support the Company's business;
- Authorized users are granted access to valuable Company resources, sensitive data and to external networks on the basis that their use of IT resources shall be responsible, ethical and lawful at all times;
- Authorized users are required to observe Company policy, and State, Federal, or local laws which may apply;
- Data and information relating to persons and other confidential matters acquired for business purposes shall be protected;
- Company Business information shall be protected from unauthorized and/or accidental disclosure; and
- Company IT resources must not under any circumstances be used to humiliate, intimidate, offend or vilify others on the basis of their race, gender, or any other attribute prescribed under anti-discrimination legislation.

II. Policy

- **Acceptable Use of TMA Systems IT and Digital Resources**
- **Who Must Comply? What Penalties Pertain?**
- **Appropriate use of TMA Systems IT and Digital Resources**
- **Company Access; Your Right to Privacy**
- **Managing Electronic Information (including e-mail)**
- **Protecting the Company's Good Name**
- **Use of Technology for Commerce or Solicitation**
- **Use of Technology for Political Activity**
- **Your Responsibility for Network and Information Security**
- **Your Responsibility Regarding Shared IT Resources**
- **Ensuring Network Performance**
- **Honesty, Integrity, and the Law**
- **Copyright and Intellectual Property**
- **Violations and Penalties**
- **Protection for You**

Acceptable Use of TMA Systems IT and Digital Resources

The Acceptable Use of TMA Systems IT and Digital Resources govern all use of TMA Systems information technology, digital resources, and Internet access. Departments, programs and offices of the Company that create specialized computing or network policies for their constituencies must work with the Company's CSO before doing so in order to ensure that such specialized policies are consistent with, and not in conflict with, this Policy Statement. Once approved, such specialized policies will be cross-referenced in future editions of this Policy Statement.

In addition, the Company's information technology resources and the access provided by the Company to global networks and networked and digital resources are governed by the general policies and rules set forth the Employee Handbook. For example, policies and rules set forth in the Employee Handbook related to other subjects also apply to those areas when they involve computers or mobile devices; when they entail use of, or publication via the World Wide Web, including, but not limited to, websites, message boards, wikis, chat rooms, social networks, media-sharing sites, and other similar electronic venues; when they involve participation in virtual reality or gaming environments, or whether the technology involved is something like multi-user gaming, Company-provided voice technology such as telephony Unified Messaging, locally-produced and broadcast video, or YouTube or other public arena videos or images involving Company activities or operations. Individuals also are expected to be familiar with and comply with the requirements of the Company's Information Security Policy.

Reasons for this Policy

Some rules for appropriate use of the Company's information technology resources derive from legal considerations. The Company must also address actions that may violate its agreements with outside vendors or clients. Additionally, these rules are intended to ensure that Company resources are used for proper and acceptable business purposes.

The Company is a “producer”, "publisher", and “carrier” of information via electronic channels hence, except with regard to official Company publications, not expected to be aware of, or responsible for, materials or communications that individuals may post, send, or publish via the World Wide Web, Internet discussion groups, Facebook, YouTube, or any social networks; make available via any file-sharing method; or send via e-mail, tweeting, instant messaging or video; or any actions taken by individuals’ avatars within on-line virtual reality or gaming environments. However, under certain circumstances, the Company may be required to respond to complaints regarding the nature or substance of such materials or communications.

Examples

The examples presented in this Policy focus on matters related to information technology, but derive their broader meaning and significance from the basic rights, rules and responsibilities that apply to all aspects of the Company. The examples are illustrative, not exhaustive. If something is not specified in the Policy as inappropriate, it still may violate the principles set forth in the Employee Handbook and be subject to Company sanction. It is important to use common sense and critical thinking in evaluating new situations.

Because technology changes so rapidly, and the human imagination is boundless in exploring what technology can do, this Policy must and will continue to evolve. In addition, the Company's is charged with the task of revising the Employee Handbook and any changes made to the Employee Handbook that could affect the language of this Policy.

Who Must Comply? What Penalties Pertain?

Compliance

This Policy applies to Company-owned devices and systems and to Company-contracted systems and services, as well as privately-owned or publicly-provided devices using the Company’s networks and resources. This Policy applies to technology administered within the Company’s Internet domain and network by individual departments, the employees or contractors of the Company, or to personally-owned devices connected by wire or wireless service to the Company networks. This Policy applies also to actions of visitors to the Company who avail themselves of the Company’s temporary visitor wireless network access service.

Privately-owned computer systems or mobile devices owned by individuals or organizations, other than the Company, when attached to, or connected via, the Company data network and/or other Company-contracted services, are subject to the same responsibilities and regulations as they pertain to Company-owned devices and systems. Company Employees who use computers or mobile devices belonging to others to connect to the Company network either directly or via secure remote access software must ensure that the devices are in compliance with Company regulations before making such connections.

In general, as stated in the Employee Handbook, the Company normally does not impose penalties for misconduct off-premises beyond the local vicinity. However, electronic misconduct directed by a member of the Company against others may be actionable regardless of the location from which the misconduct originated or the network or devices used. Consistent with the Employee Handbook, judgments about such incidents will depend on the facts and circumstances of an individual case.

Penalties

All employee and contractor computer users, and authorized visitors, and others who may be granted use of the Company's systems and network services or Company-contracted services, must comply with the Company's policies. When a member of the Company is found to be in violation of this Policy, any disciplinary action is handled by the normal Company authority and via the normal disciplinary process that would apply for other types of infractions. When an authorized visitor is in violation of policy, the Company sponsor or host may be held accountable. If the matter involves illegal action, law enforcement agencies may become involved, as they would for any other actions that do not involve the information technologies or Internet.

Appropriate use of TMA Systems IT and Digital Resources

Business Use

As an employee of the Company, you are provided with the use of work-related tools, including (but not confined to) access to computer systems, servers, software, printers, services, databases and other electronic devices; to the Company telephone and to the Internet As a general matter, your use of all such information technology should be for purposes that are consistent with the business and mission of the Company.

Computing and network equipment and mobile devices purchased by the Company remain the property of the Company even if they are dedicated for your use. Equipment purchased for other purposes is vested with the Company though it is to be used for the purposes of a specific project. When Company-owned equipment no longer is needed, its disposition must be in compliance with Company policy and may not be determined independently by the user of the equipment.

Tampering with Company-owned IT equipment, including cell or smart phones, is defined as making unauthorized changes to the hardware or system-level software that may be in conflict with license or may void applicable warranties. Company employees must not perform or condone such actions. Exceptions sometimes may be made for other authorized purposes.

Personal Use

Personal use of the Company's IT and digital resources should be incidental and kept to a minimum. For example, use of such resources by an employee for other than work-related matters should be reasonable and limited so that it does not prevent the employee from attending to and completing work effectively and efficiently, does not incur additional cost to the Company, and does not preclude others with work-related needs from using the resources, including the shared Company network and Internet bandwidth. The Company or departments may place additional restrictions on personal use of the resources by employees.

Company Access; Your Right to Privacy

The Company's Right to Access Files

All contents in storage on Company and Company-contracted data and voice systems are subject to the rules of TMA Systems, including the Company's ability under certain circumstances to access, restrict, monitor and regulate the systems that support and contain them. In general, and subject to applicable law, the Company reserves the right to access and copy files and documents (including e-mail and voice mail) residing on Company-owned equipment and in storage contracted by the Company from outside enterprises. This includes access without notice, where warranted. Non-intrusive monitoring of Company network traffic occurs routinely, to assure acceptable performance and to identify and resolve problems. If problem traffic patterns suggest that system or network security, integrity, or performance has been compromised, network systems staff will investigate and protective restrictions may be applied until the condition has been rectified.

Some departments that maintain servers or internal networks may collect usage data and may monitor such servers or networks to ensure adequate technical performance. Departments that collect such data are expected to protect the privacy of those using the resources. It is also important to note that the Company may be required to produce such data in compliance with a valid subpoena or court order.

The Company also provides some access to files and documents residing on Company-owned equipment (and/or transmitted via the Company's network services) to outside vendors who have been contracted with to provide technology services. The Company contracts with such vendors contain firm provisions for security of information and for the privacy of members of the Company who may use those services.

Degrees of Privacy

Company employees, who are provided with the use of Company resources for work-related purposes, are afforded a lesser degree of privacy. For example, employees may be directed to share certain work files and information with others or to make a computer account accessible to a supervisor to assure effective backup or execution of the work when no other practical means exist for sharing the needed information readily and securely. In the event that business-related files (including e-mail and digitized voice messages) stored on an employee's account or workstation must be accessed, whether because of unexpected absence, death, or termination of employment, or other necessity, such files may be accessed by the Company after consultation with Senior Management based on business need. On employee termination, supervisors are expected to assure that passwords to computers, other networked devices, and accounts are obtained and changed if the work of the unit requires access to data or resources previously managed by the employee, and that copies of critical work product remain available following the employee's separation from the Company.

Others' Files

If you are a supervisor who has access to an employee's files or e-mail, or have been designated by a supervisor to access another employee's files or e-mail, you should be careful to avoid reading personal items that may be stored in the same area. For example, upon learning that an e-mail or voice mail message is personal, and not business-related, the supervisor or designee should immediately exit the file or message. The supervisor or designee should be careful to avoid examining any personal information the Company may provide to the employee via password access, such as benefits or payroll data. Departing employees are not entitled to remove any documents created by them or others, unless otherwise permitted by the Company. The Company's record retention policy also must be observed. Where the General Counsel has issued a "Legal Hold Notice," individuals may be required to suspend regular retention practices and to retain information until further notice from the General Counsel, including after an employee's departure from the Company.

Disclosure

In addition to information you may store on devices owned by the Company, the Company and its contractors maintain certain system backups and logs of e-mail and network transactions. If the Company is presented with a valid subpoena or court order requiring that such information be produced (or preserved), or directing that the Company assure that its employees produce (or preserve) such information, the Company may be bound by law to comply. Similarly, the Company also may be obligated to disclose the identity of an account-holder or identity of the person who owns a computer or other registered network device, is responsible for a Company- owned computer or networked device, or holds a Company-assigned account used in some electronic transaction.

Supervisors are encouraged to communicate the Company's expectations regarding privacy of employee files and e-mail, and to remind employees of these expectations periodically. Supervisors also are expected to take prompt action to retrieve or preserve employee files needed to continue the work of the Company when an employee is about to separate from their employment with the Company.

Managing Electronic Information (including e-mail)

Retention and Disposal

Employees, including those who are designated as regular, term, visiting, and temporary, are responsible for retaining information that is of value to the Company, whether that is for business processes, for legal purposes, or historical value. The Company's Record Retention Policy offers recommended retention periods for common Company records whether on paper or electronic.

Employees of the Company, should understand that electronic information is governed by the same laws and regulations as paper documents historically have been, including statutes protecting the privacy of employee records, medical information, and other kinds of personal information. Employees are expected to apply to electronic information the same security and record retention practices applied to paper documents.

There are three ways of preserving e-mail: on the e-mail system, within an office's paper files, or in some form of electronic record-keeping system, for example, the Set Regarding feature in MSCRM. As a general rule, the longer the message must be maintained or the more it needs to be shared, the greater the need to remove it from the e-mail system and store it in the MSCRM system or in the electronic storage system (SharePoint). Attachments must also be identified and linked to the original message so that they may be easily located. In all cases, the authenticity and integrity of the entire e-mail message should be preserved.

E-mail retained in electronic format must be migrated to new software and storage media as upgrades occur.

Like all records, many e-mail messages eventually will cease to be useful to or needed by the Company, and at that point should be deleted by the account-holder. Then the account-holder is responsible for assuring that the "Trash" or "Deleted Items" folder is emptied (either manually or on an automated schedule) to properly dispose of the e-mail records.

When an employee's computer or other network device is replaced, it is required that the employee or the employee's computing support specialist use appropriate, effective software to remove any and all data from the hard drive, or if warranted, destroy the hard drive by means approved by the Company. As with the disposition of any other Company records, e-mail disposal should be done on a standardized and regular basis. With respect to back-up media, it is recommended that these storage devices be physically destroyed through approved Company channels when no longer needed. However, it is imperative that copies of critical work and work product be maintained until no longer needed.

Outside E-mail

Employees who have personal e-mail accounts with services outside the Company should use only their Company-provided e-mail accounts for communications regarding Company matters. Using Company e-mail protects the privacy and security of Company data; allows for verification of sending and receipt of critical correspondence regarding Company matters; and facilitates responses to subpoenas and other situations that may require the retrieval, inspection, or production of documents including e-mail.

TMA Systems account-holders should not copy or forward email to an outside account. These practices can interfere with the business of the Company as well as impede communication for other employees of the Company. In addition, this activity may be in violation of contractual obligations with clients or other entities.

Protecting Data

If you are responsible for data that is important to the Company or clients and that is created or stored on portable devices, you also are responsible for ensuring that the information is backed up regularly in a form that permits ready retrieval.

If you are an employee and have custody of data important for completion of your company project(s), you are responsible for assuring that adequate and appropriate back-up of the information is maintained.

Some kinds of information are considered restricted and/or confidential. Some information is defined confidential by law, for example by HIPPA. Some contractual agreements require protection of related information. In general, information should be protected as consistent with the Company's Information Security Policy.

As an employee, whether you have authorized or inadvertent access to what the Company defines as restricted or confidential data, you must comply with the Company's Information Security Policy.

You also must confine your access to or viewing of such data to situations in which only your Company responsibilities require such access or viewing.

Any handling of confidential data, whether in hard-copy form, on Company-owned equipment, or via personally-owned home devices, should be done in the most secure, confidential manner, consistent with the Information Security Policy.

In the event of unauthorized access to Company data, whether through theft or loss of portable devices such as USB drives, laptops, smart phones or other devices, or any other kind of breach of security, the individual who possessed the device or learns of the breach is responsible for notifying the appropriate Company officials of a potential data breach, and assisting with the Company's data breach response.

If the individual suspects the breach involves illegal action by a member of the Company, the employee should contact management and the Company General Counsel.

Restricted or confidential data ordinarily should not be stored on portable devices that are easy to carry away. If it is absolutely necessary to do so, the information must be encrypted to protect it from view should the device fall into unauthorized hands. The portable device and, ideally the files as well, must be password protected. It also is essential to provide adequate physical security for any device, including a desktop machine that contains confidential data.

The Company-endorsed encryption product or protocol should be used whenever possible. If the Company has not yet endorsed a particular product or protocol for the platform you use, you should be prepared to use one when it is announced as endorsed.

Those who travel abroad on Company business should know that some encryption software may not be taken out of the United States. For that reason, and to avoid transporting restricted or confidential data unnecessarily, it may be prudent to travel with a computer or mobile device specially configured for travel rather than with the laptop or mobile device used locally.

The advent of storage services in "the cloud" provides a useful alternative for those who use portable network devices or have computers stationary in several locations. The Company has arrangements with certain providers for some secure cloud-based services. Those services should be used by employees. However, if the Company has authorized an employees to use another cloud services it still must adhere to the standards set forth in this document. Until the Company can endorse you doing so, storing confidential or private Company information in other "cloud" service poses serious risks, and should be avoided.

Peer-to-peer file-sharing software may not be installed or used on Company's computers or other devices attached to the Company network because such applications could expose information that is private, confidential, or Company-related.

Protecting the Company's Good Name

Good Judgment

You are responsible for knowing the regulations and policies of the Company that apply to your use of Company technologies and resources. You are responsible for exercising good judgment in use of the Company's technological, digital and information resources.

As a representative of TMA Systems, you are expected to respect the Company's good name in your electronic dealings with those both within and outside the Company.

Use of the Company's Name

No employee of the Company may use the name TMA Systems for any non-business use. Deliberate misuse of the name of the Company or other trademarks by any employee of the Company will be regarded as a serious offense. Any employee of the Company who misuses the data in such a way may be subject to disciplinary action.

Directory Use

Information in the Company's employee directory is provided solely for use by employees who wish to reach specific individual or resource at the Company. Use of the information for solicitation by mail, e-mail, telephone, or other means, or for creation of a database for such use or for other purposes, is prohibited.

Enabling Others

The privilege of using Company equipment, wiring, wireless access, computer and network systems and servers is provided to employees of the Company and may not be transferred or extended by employees of the Company to people or groups outside the Company without authorization.

Use of Technology for Commerce or Solicitation

Commerce

Employees are prohibited from using Company information technology and digital resources for commercial purposes.

Solicitation

Electronic mail or World Wide Web, message board, social media, or Twitter solicitation using the Company's resources is prohibited.

Use of Technology for Political Activity

Employees may not use Company resources with respect to political activities. Any employee of the Company who engages in these activities utilizing company resources may be subject to disciplinary action.

Your Responsibility for Network and Information Security

Protecting Accounts

As an employee, the Company has provided you with accounts that provide you access to the Company's systems, networks, voice mail services or other technological facilities. You are accountable to the Company for all actions that are performed by anyone who uses these accounts. Therefore, you are expected to take reasonable measures to prevent your accounts from being used by others. Since passwords are a primary method of protecting Company systems against unauthorized use, you, as a Company-provided account holder, are expected to change any pre-assigned default password at the first possible opportunity, to select strong passwords that are difficult to guess, and to safeguard them from casual observation or capture. Thereafter, the Company requires that passwords for Company- provided accounts be changed at least once a year and for greater security recommends they be changed even more often. (See Information Security Password Policy for further details.)

Intentional sharing of such passwords with associates, friends, or family is prohibited, unless required by the terms of your Company employment or the nature of the group to which the account has been assigned. If there are alternate and practical ways to share work-related information readily and securely, these should be used rather than one Company employee's being given the password of another.

A password used for access to a Company account or resource should not be the same as those used to access non-Company-affiliated resources. For example, account-holders should not use any of their Company passwords as the password for a social media site, or a personal banking site, or other outside resources.

There are Internet services designed to allow you to store personal information such as passwords, PIN numbers, credit card numbers and other data for ready retrieval by smart phone or other mobile device. If you elect to store your Company password(s) through such a service, you risk exposure and subsequent misuse of your Company account access and files.

Your Responsibility Regarding Shared IT Resources

Appropriate use of Shared Resources

The technological resources centrally administered by the Company are intended to be used for business purposes and to carry out the legitimate business of the Company. Such resources include Company computer clusters, the Company's World Wide Web server, local-area networks, the Company wireless network, Intranet access, the Company telephone and voice mail systems, general Company multi-user computer systems and servers, SharePoint, and access to the Company's e-mail service, and other shared Company facilities and services.

Appropriate uses are defined as Company business. Company business relies on reasonable performance from the component units and the connections that allow interchange among them, and on the security and integrity of the resources. For these reasons, and because there often are times when some resources are in shorter supply than can easily meet the demand, certain performance-related or sharing guidelines pertain.

Employees are expected to sustain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for the others who rely on such services.

Temporary Visitor Access to IT Resources

The Company provides temporary visitor wireless network access service primarily for use by Company visitors with computers or other devices equipped for wireless access. The temporary visitor wireless network access is not intended to provide service to devices used regularly within the facilities. Such devices presently must be registered properly for network connectivity.

Employees may use the temporary visitor network access with other wireless-enabled devices, provided such use is infrequent and the devices are not disruptive to network availability and performance. Temporary visitors and employees of the Company who use the visitor wireless service must comply with the TMA Employee Handbook regarding network and Internet use. Abusive behaviors that disrupt Company services can result in a device being blocked indefinitely from further use of any Company network services.

Mass Mailings

At TMA Systems, mass electronic mailings are permitted only as authorized by appropriate employees. The same authority would govern e-mail to those constituencies, even if the sender does not use the official list, but creates multiple smaller groups to accomplish the same end. In general, the same authority approves the use of large e-mail lists as approves large paper mailings to the same audiences. You may not send large mass e-mailings or voice mailings without the appropriate Company authorization.

Appropriate authorization also must be obtained to conduct Web-based or e-mail surveys, whether among employees of the Company or of people outside the Company. Surveys must obtain approval from the Company's Senior Management Team.

Use of Limited Resources

You must refrain from unwarranted or excessive amounts of storage on central computing systems and servers, and from running grossly inefficient programs when efficient ones are available unless you have been directed or given approval.

Unless given specific authorization, you must not run servers or daemons within the Company network or utilizing Company resources.

Where the Company has obtained very limited licenses for software, you must use only one share, not several concurrently.

Company shared computing resources may not be used for game playing or other trivial applications.

Paper and Printing Resources

Unnecessary printing is wasteful in dollar cost and is in conflict with the Company's sustainability goals. Employees of the Company should practice thrifty and judicious printing. When a work is in progress, editing should take place on-line whenever possible rather than on a printed draft. Information that can be shared effectively electronically should not be printed at all. When it is necessary to print notes or reference material, consideration should be given to placing multiple pages on each sheet of paper and using two-sided (duplex) printing whenever possible.

Ensuring Network Performance

You must not attempt to intercept, capture, alter, or interfere in any way with information on local network pathways. This also means you may not run "sniffers" (programs used illegitimately to capture information being transmitted) on the Company network or any network resources. You may not operate Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BootP) servers on the Company networks without authorization.

You must not attempt to obtain system privileges to which you are not entitled, whether on Company resources or on systems outside the Company. Attempts to do so will be considered serious transgressions. Any employee of the Company who engages in these activities utilizing company resources may be subject to disciplinary action.

Computer procedures, programs, websites and scripts that permit unauthenticated or unauthorized senders to send e-mail to arbitrary recipients from unrestricted sources are prohibited.

You must refrain from any action that interferes with the supervisory or accounting functions of the systems or that is likely to have such effects. You must refrain from creating and/or implementing code intended, even periodically, to interrupt or interfere with networked systems or services. You must refrain from knowingly propagating computer viruses or presumed computer viruses. You must not conduct unauthorized port scans. You must not initiate nuisance or denial-of-service attacks, nor respond to these in kind.

Wireless access points may not be installed by individuals within the Company without authorization from the Chief Information Officer. If authorization is provided, the individual must comply with any rules regarding the wireless access point established by the Chief Information Officer.

Wireless access service is provided by the Company. Some commonly used appliances could interfere with wireless network service. If a device interferes significantly with the Company's wireless network service, the individual may be required to relinquish use of the device. Malicious use of any such device to disrupt network service will be considered a serious violation of Company regulations and subject to disciplinary action.

Computers, smart phones, and other network devices connected to the Company's network must be approved for network use. Each will be assigned an Internet Protocol (IP) address or, if mobile, "leased" an address by the Company's network management servers. Using other than the assigned IP address can disrupt normal network operation for others, so users and owners of such devices are expected to refrain from supplying other IP address for use in any network transaction.

Honesty, Integrity, and the Law

The Law

The Company, through its employees, must comply with local, state and federal law, including copyright laws.

Employees of the Company may not knowingly assist others with use of the Company's information technology resources or Internet access for purposes of violating the law, including copyright laws. Employees who are asked for such assistance must refuse.

Employees of the Company should report suspicion of crime involving, or revealed by, Company technology resources (such as computers, mobile devices, network or Internet access, e-mail) to Senior Management or the Company's General Counsel. For suspected crimes in progress or where there is an imminent or serious threat to individual safety, appropriate law enforcement agencies should be contacted immediately. In all cases, employees must treat information regarding potentially unlawful activity with discretion and sensitivity to the privacy rights of others.

Dishonest Actions

There are actions which may not be specifically prohibited by law, but which are nonetheless dishonest. Employees of the Company are expected to be honest and straightforward in their official dealings with Company processes, activities, personnel, and clients. This obligation includes honoring contracts and agreements and providing accurate information on official forms and documents as well as official Company communications. Deliberate violations of this provision will be considered a serious offense; subsequent violations, or systematic violations will be considered extremely serious. Such actions also are unacceptable when conducted by means of the Company information technology resources and Internet access.

You must not create, alter, or delete any electronic information contained in, or posted to, any Company computer or network for fraudulent or deceptive purposes that may be harmful to others. Moreover, signing an electronic document (including e-mail), or posting to a Website, message board, or social network, with someone else's name will be a violation of Company rules. It also will be considered a violation of Company rules if you use the Company's electronic resources or Internet access to create, alter, or delete electronic information contained in or posted to any computer system on or outside the Company for which you are not authorized to do so.

Unauthorized attempts to browse, access, solicit, copy, use, modify, or delete electronic documents, files, passwords, images, films, music, sounds, games or programs belonging to other people, whether at the Company or elsewhere, will be considered serious violations.

You must not use another's account-affiliated resource or personal computer or networked device without authorization. If you encounter an open session that exposes another's account-affiliated resource, lock the session and try to notify the individual. It is considered a serious transgression to exploit the accidental exposure of another's account or to borrow or steal another's identity. Without authorization, you must not attempt to enter and listen to another person's voice message, or enter and read another person's e-mail, or other electronic messages or files, even when these are accidentally exposed to your access. It is considered a very serious transgression to gain unauthorized access to another's account-affiliated resources or another's personal device or workstation, e-mail, or files, through deliberate action.

You must not attempt to fool others into revealing their log-in credentials or passwords, whether by use of social engineering, by tricking others into entering their credentials where key-loggers can capture the information, or by any other means. Login credentials (e.g., network IDs, user names and passwords) are highly confidential. To obtain another's login credentials without that person's knowledge and consent is unacceptable. Any attempt to capture another person's login credentials is a serious offense and may be subject to disciplinary sanctions.

You must not create and send, or forward, electronic chain letters. To do so may also violate federal law, even if the chain letter assures the reader that it is not illegal and cites statutes as "proof." The redistribution of chain letters is a violation of Company policy even when there is no mention of money in the letter. Some chain letters which appear to relate to genuine causes often are "urban legend" by the time they reach you; if you research the issue you may discover the cause existed long ago and the letter no longer is meaningful.

You must not post "pyramid scheme" messages. A pyramid scheme calls for escalating numbers to send money, usually small amounts, to others, with the expectation that a large amount of money will come to them. Any posting or message that suggests such a scheme is a violation of Company policy and may violate federal and other laws.
You may not "borrow" an Internet Protocol address assigned to another person or entity, create fraudulent IP addresses for a device you own or are using, or attempt to use with one device the IP address assigned to another device you own or use. You may not operate a server that assigns, or attempts to control IP addresses on the Company network.

You may not falsify a hardware address for a device connecting to the Company network or a wireless interface used to connect a device to a Company network.

You should be aware that there are federal, state and sometimes local laws that govern certain aspects of computer, broadcast video, and telecommunications use. With considerable focus on

U. S. Homeland Security and the national infrastructure, and with escalating pursuit of copyright infringers continuing to generate concern, additional legislation is evolving. Members of the Company are expected to respect the federal, state and local laws in use of the Company's technologies and Company-provided network access, as well as to observe and respect Company-specific rules and regulations.

Gambling

Gambling is prohibited for employees in the workplace. This prohibition includes Internet gambling.

Copyright and Intellectual Property

Copyright

The Company protects intellectual property. The Company and its employees are both holders and users of protected intellectual property. The Company seeks to facilitate the responsible exchange of intellectual property and, to that end, works to raise awareness about issues of copyright, educating employees about principles of fair use.

It is important to understand the legal context for copyrights. They are created by law and violations of the owner's rights can be enforced through lawsuits. Even when the owner claims a violation has occurred, there are defenses and justifications for use of some copyrighted material, but it is crucial to start by considering whether the materials are protected by copyright – or not.

Understanding Copyright

"Copyright" is one name for a bundle of rights, including the right to make copies, distribute copies, making derivative works, and the public performance and/or public display of works. Copyright protects written works, paintings, sculptures, photographs, videos, recorded music, sheet music, computer programs, video games, architectural design, choreography, etc.

Copyright does not protect every idea or scrap of paper. It does not protect ideas, concepts facts, data, titles, names, phrases, procedures or methods of operation. It also does not protect unoriginal works or works that are not fixed in a tangible medium (such as paper or digital code).

Works created by employees in the context of their employment by TMA Systems are owned by the Company. The Company can choose to allow certain uses by the public, and may even donate the work to the public domain. This however, can only be granted by the Company.

Protection for You

Phishing

The growth of the Internet has brought with it increased opportunities for exploitation. Each day, billions of e-mail messages "phishing" for personal and financial information traverse Cyberspace. Despite all the warnings published by financial institutions and e-commerce enterprises and news coverage of such schemes, some people are fooled. For example, people at the Company have seen e-mail messages very cleverly designed to look as if they came from a banking institution. Please use caution when receiving these emails. When you are not sure whether such a message is genuine, it is appropriate and in fact preferable to check with the Chief Information Officer or other person in authority before responding or releasing information. It also may be appropriate to ask that the request for information be made in writing by mail or facsimile.

Social Engineering

The term "social engineering" refers to more than technology. A scammer with a convincing story might telephone an office worker and claim to work for the Company or at some financial institution, and ask the person for his or her account and password for some plausible-sounding security purpose. It is important to use critical thinking skills even for telephone or live approaches from people you do not know.

Self-exposure

Another type of danger is self-exposure. The rise of Facebook, MySpace, and other "social networks" encourages people to let their metaphoric hair down and to express themselves in ways that, in retrospect, might be a little too open for comfort. While communications or postings in online formats, such as Facebook are fun, they can possibly expose you and the Company to serious unintended consequences.

Also, when creating public postings, tweets, or blogs of any kind, keep in mind the power of the World Wide Web to broadcast and preserve your statements. Any ill-considered postings may survive your commitment to them, and, because of the distributed nature of Web indexing, may be very difficult to expunge in the future.

Where to Turn

The Company is committed to protecting employees from abusive actions by others both within and outside the organization. If you experience abusive incidents related to the technologies, or if you are a supervisor who believes that an employee is abusing access to the information technology resources or Internet access, you should report the matter to the most appropriate contact. You also can report abusive actions involving Company technology, whether the perpetrator is an employee of the Company or not.

III. Procedure

There is no content for this section.

IV. Who is affected by this Policy

All Company employees and consultants are affected by this policy.

V. Definitions

There is no content for this section.

VI. Related Policies

- **Information Security Policy Framework**
- **Information Security Policy**
- **Information Security Plan**
- **Information Security Password Policy**
- **Information Security Incident Management**
- **Network Administrative Security Policy**
- **Data Encryption Policy**
- **Monitoring and Logging Policy**
- **Business Continuity Policy**
- **Disaster Recovery Policy and Plan**

VII. Update Log

June 1, 2015: Policy issued.