Network Administrative Security Policy

Policy Title	**Network Administrative Security 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

TMA Systems must maintain secure networks to protect sensitive and valuable information both corporately, for their clients, and for their business associates. To achieve this, management must implement appropriate controls and protections on hardware, software, and resources; maintaining appropriate auditing and monitoring; and evaluating system threats and vulnerabilities on an ongoing basis. The goal of the Network Administrator is to protect the network from security breaches, whether accidental or malicious. This policy focuses on the Network Administrator providing a variety of defenses including: network users having proper privileges, proper access and keeping the network secure.

II. Policy

- **Communications and Operations Management**
- **Proper Privileges at TMA**
- **Identity and Access Management**
- **Patch Management - Prioritization and Scheduling**
- **Network Security**
- **Security Monitoring**
- **Segregation of Duties**

Communications and Operations Management

System communications protection refers to the key elements used to assure data and systems are available, and exhibit the confidentiality and integrity expected by owners and users to conduct their business. The appropriate level of security applied to the information and systems is based on the classification and criticality of the information and the business processes that use it. The System's integrity controls must protect data against improper alteration or destruction during storage, during processing, and during transmission over electronic communication networks.

The key elements of system and communications protection are backup protection, denial of service protection, boundary protection, use of validated cryptography (encryption), public access protection, and protection from malicious code.

Operations management refers to implementing appropriate controls and protections on hardware, software, and resources; maintaining appropriate auditing and monitoring; and evaluating system threats and vulnerabilities.

Proper operations management safeguards all of the Company's computing resources from loss or compromise, including main storage, storage media (e.g., tape, disk, and optical devices), communications software and hardware, processing equipment, standalone computers, and printers.

Proper Privileges at TMA

Proper privileges at TMA are based on the "principle of least privilege". The principle limits access for users to the minimal level that allows a user normal functioning. This principle of least privilege translates into giving people the lowest level of user rights that they can have and still do their job. This limits the potential damage from a security breach, whether accidental or malicious.

System administrators routinely require access to information resources to perform essential system administration functions critical to the continued operation of the Company. Such privileged access is termed "administrator" access. Privileged accounts enable vital system administration functions to be performed and are only to be used for authorized purposes.

The number of privileged accounts ("administrator") is to be kept to a minimum, and only provided to those personnel whose job duties require it. Administrators who require privileged accounts should also have non-privileged accounts to use when performing daily routine tasks and should not use their privileged accounts for non-authorized purposes. Activities performed using a privileged account is to be logged and the logs will be reviewed on a regular basis by an independent and knowledgeable person.

Personnel who manage, operate, and support Company information systems, including individuals who manage their own systems, are expected to use appropriate professional practices in providing for the security of the systems they manage. Responsibility for systems and application security must be assigned to an individual knowledgeable about the information technology used in the system and in providing security for such technology.

Basic information related to an Administrator who has a privileged Account:

- Privileged access is only granted to individuals authorized.
    - Users with privileged access will have two user IDs: one for normal day-to-day activities and one for performing administrator duties.
    - Administrators may only use their administrator account to perform administrator functions.
    - Administrators may not use their privileged access for unauthorized viewing, modification, copying, or destruction of system or user data.
    - Privileged accounts may only be used from the TMA LAN or via TMA's secure RDP gateway.

- Change of responsibilities or employment and related privileges
    - Privileged accounts must be reviewed. Access to corporate and client information, data and resources must be revoked or updated as appropriate for new positions and responsibilities.

- Temporary Accounts
    - Temporary accounts will be created when required to mitigate client-related issues or other corporate-based needs, as appropriate.
    - Temporary accounts must be requested and approved by the CIO. Request must include reason for need and duration.
    - When expired (duration has lapsed), temporary accounts must be disabled.
    - Temporary account requests must be maintained for a period of not less than 6 months.

- Mobile Devices and Laptops
    - Mobile devices and laptops used to access corporate resources, including e-mail, databases and other electronic media must be configured with a passcode of at least 8 digits, and must have an inactivity timeout of not less than 30 minute. (See Information Security Password Policy)
    - If a mobile device or laptop is lost or stolen, notification must be made within 1 business day to the CIO and Network Administrator.

Identity and Access Management

Identity and access management ensures accurate identification of authorized individuals and provides secure authenticated access to network-based services. Identity and access management are based on a set of principles and control objectives to:

- Ensure that there is unique identification of employees of the Company and they are assigned proper access privileges
- Allow access to information resources only by authorized individuals
- Ensure periodic review of associates and their authorized access rights
- Maintain effective access mechanisms through evolving technologies

Access Management refers to the process of controlling access to systems, networks, and information based on Company and security requirements. The objective is to prevent unauthorized disclosure of TMA's or client information assets. Company access control measures include secure and accountable means of identification, authentication, and authorization.

- Identification is the process of uniquely naming or assigning an identifier to every individual or system to enable decisions about the levels of access that should be given. The key feature of an identity process is that each user is uniquely identifiable from all other users.
- The authentication process determines whether someone or something is, in fact, who or what it is declared to be. Authentication validates the identity of the person. TMA Authentication utilizes passwords. For the purpose of access control, authentication verifies one's identity through IT. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. (See Information Security Password Policy.)
- Authorization is the process used to grant permissions to authenticated users. Authorization grants the user, through technology or process, the right to use the information assets and determines what type of access is allowed (read-only, create, delete, and/or modify).
- The access rights to the information must be entered into the security system via an access list, directory entry, or view tables, for example, so the authorization rules can be enforced. The level of control will depend on the classification of the data and the level of risk associated with loss or compromise of the information.
    - Criteria must be established by the Data Owner for account eligibility, creation, maintenance, and expiration.
    - Highly sensitive data must be individually authorized by the Data Owner and an annual confidentiality agreement must be acknowledged or signed by all authorized users.
    - Data Owners must periodically review user privileges and modify, remove, or inactivate accounts when access is no longer required.

    - Procedures must be documented for the timely revocation of access privileges and return of Company owned materials (e.g., keys) for terminated employees and contractors.
    - Inactivity time-outs must be implemented, where technically feasible, for terminals and workstations that access highly sensitive data. The period of inactivity shall be no longer than 10 minutes in publicly accessible areas. Audit trails exist for detective and reactive response to system penetration, infection of systems and data due to malicious code, catastrophic system loss or a compromise of data integrity.
- Remote access to information technology resources (switches, routers, computers, etc.) and to sensitive or confidential information (social security numbers, credit card numbers, bank account numbers, etc.) are only permitted through secure, authenticated and centrally-managed access methods. Systems that contain sensitive data will be available for off-site remote access through a centrally managed VPN that provides encryption and secure authentication.
- It should also be understood that when accessing sensitive data remotely, it is prohibited to store cardholder or other sensitive data onto local hard drives, floppy disks, or other external media (including laptops and Smartphones).
- External computers that are used to administer Company resources or access sensitive information must be secured. This includes patching (operating systems and applications), possessing updated anti-virus software, operating a firewall and being configured in accordance with all relevant Corporate policies and procedures.

Patch Management - Prioritization and Scheduling

TMA System’s Patch Management is to ensure that data is protected against malware threats, such as viruses, Trojans, and works which could adversely affect the security of the systems or data entrusted on TMA’s systems. Effective implementation of this policy will limit exposure and effect of common malware threats to the systems.

- The primary scheduling guidelines and plans exist as a comprehensive patch management program. First, a daily patch cycle exists that guides the normal application of patches and updates to systems. This cycle does not specifically target security or other critical updates. Instead, this patch cycle is meant to facilitate the application of standard patch releases and updates. This cycle is time based and when appropriate is event based; for example, the schedule can mandate that certain system updates occur quarterly, or a cycle may be driven by the release of service packs or maintenance releases. In either instance, modifications and customizations can and should be made based on availability requirements, system criticality, and available resources.

- The secondary scheduling plan deals more with critical security and functionality patches and updates. This plan helps the organization deal with the prioritization and scheduling of updates that, by their nature, must be deployed in a more immediate fashion. A number of factors are routinely considered when determining patch priority and scheduling urgency. Vendor-reported criticality (e.g. high, medium, low) is a key input for calculating a patch's significance and priority, as is the existence of a known exploit or other malicious code that uses the vulnerability being patched as an attack vector. Other factors that should be taken into account when scheduling and prioritizing patches are system criticality (e.g. the relative importance of the applications and data the system supports to the overall business) and system exposure (e.g. DMZ systems vs. internal file servers vs. client workstations).

Network Security

Network attacks launched from the Internet or other networks can cause significant damage and harm to information resources including the unauthorized disclosure of confidential information. In order to provide defensive measures against these attacks, firewall and network filtering technology must be used in a structured and consistent manner.

TMA must maintain appropriate configuration standards and network security controls to safeguard information resources from internal and external network mediated threats. Firewalls and Intrusion Detection Systems (IDS) are deployed and Intrusion Prevention Systems (IPS) are deployed on core services to augment normal system security measures to prevent denial of service attacks, malicious code, or other traffic that threatens systems within the network or that violates Company information security policies. Firewalls and or IDS/IPS are also deployed as appropriate to limit access to systems that host restricted or essential information.

Security Monitoring

Security Monitoring provides a means by which to confirm that information resource security controls are in place, are effective and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. Early detection and monitoring can prevent possible attacks or minimize their impact on computer systems.

Any equipment attached to the Company’s network is subject to security vulnerability scans. The goal of the scans is to reduce the vulnerability of Company computers and the network to hacking, denial of service, infection, and other security risks from both inside and outside the Company.

Segregation of Duties

Tasks involved in critical business processes must be performed by separate individuals. Responsibilities of programmers, system administrators and database administrators must not overlap, unless authorized by the Data Owner. Duties and responsibilities shall be assigned systematically to a number of individuals to ensure that effective checks and balances exist. Such controls keep a single individual from subverting a critical process. Key duties include authorizing, approving, and recording transactions; issuing and receiving assets; and reviewing or auditing transactions.

Segregation of duties should be maintained between the following functions:

- Data entry
- Computer operation
- Network management
- System administration
- Systems development and maintenance
- Change management
- Security administration
- Security audit

Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved. This standard requires supervisors to continuously review and approve the assigned work of their staff as well as provide the necessary guidance and training to ensure that errors, waste, and wrongful acts are minimized and that specific management directives are followed.

Communications and Operations Management

System communications protection refers to the key elements used to assure data and systems are available, and exhibit the confidentiality and integrity expected by owners and users to conduct their business. The appropriate level of security applied to the information and systems is based on the classification and criticality of the information and the business processes that use it. The System's integrity controls must protect data against improper alteration or destruction during storage, during processing, and during transmission over electronic communication networks.

The key elements of system and communications protection are backup protection, denial of service protection, boundary protection, use of validated cryptography (encryption), public access protection, and protection from malicious code.

Operations management refers to implementing appropriate controls and protections on hardware, software, and resources; maintaining appropriate auditing and monitoring; and evaluating system threats and vulnerabilities.

Proper operations management safeguards all of the Company's computing resources from loss or compromise, including main storage, storage media (e.g., tape, disk, and optical devices), communications software and hardware, processing equipment, standalone computers, and printers.

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**
- **Information Technology Policy**
- **Data Encryption Policy**
- **Monitoring and Logging Policy**
- **Business Continuity Policy**
- **Disaster Recovery Policy and Plan**

VII. Update Log

June 1, 2015: Policy issued.