Information Security Policy
For
Macon County

The enclosed IT security policies have been developed to protect Macon County critical operations, partners, assets, staff and customers. Compliance to these policies is mandatory. If you have any questions regarding any of the policies or your responsibilities in implementing them, please contact your supervisor.

Version 1.0

Approval Date:September 8, 2015

Primary Contact:Information Technology Director

TABLE OF CONTENTS

1. Introduction

The data that resides at Macon County is of great value to Macon County. Due to the increasing value of the data we collect, store, process, and share with our partners, it is a high priority for Macon County to protect such data.

The management of Macon County is committed to developing, adopting, and maintaining appropriate information security policies, standards and procedures to ensure integration of information security with Macon County's mission, business strategy, risk posture and in accordance with applicable regulatory guidelines.

This will be accomplished by active Macon County owner and management oversight, effective management and monitoring of information security risks, delineation of clear accountability for information security and establishing appropriate organizational processes to ensure that information security risks are appropriately and regularly identified, monitored and controlled.

This policy applies to all Macon County employees, contractors, service providers and vendors. Additionally, this policy is supported by daily operational security procedures that have been developed in conjunction with this policy.

This policy is necessary in order to maintain Macon County compliance with applicable laws and standards, protect the Macon County from liability and protect the confidentiality, integrity and availability of Macon County information systems, data and network resources.

Macon County's information security policy represents the combined efforts of Macon County's Information Services Department (IS), Human Resources Department (HR), Finance and user communities.

Macon County may at any time, make changes to this policy.

Reference: PCI DSS v3.0 requirements 12.2, 12.4

Document Approval

Date of Last Review	Name and Title of Approver
September 8, 2015 (adopted)	Board of Commissioners

Definitions

Availability	Ensuring that information systems, data and network resources are available and ready for use when they are needed.
Confidentiality	The protection of data from unauthorized disclosure.
Contractor	Use standard Macon County definition
DMZ	Demilitarized zone. Network added between a private and a public network to provide an additional layer of security.
Employee	Use standard Macon County definition
Emergency Change	A change which, due to urgency or criticality, needs to occur outside of the Macon County's formal change management process.
Encryption	Process of converting data into an unintelligible form except to holders of a specific cryptographic key.
Information System	Information systems include, but are not limited to, laptop computers, workstations, servers, mainframe computers, routers, switches, cell phones, telephones, fax machines and personal digital assistants (PDAs).
Integrity	The accuracy, completeness and validity of information.
Logical Controls	Controls that limit logical access to information systems and/or electronic data. For example, passwords, user accounts, firewall rules
Malicious software	Software designed to damage or disrupt information systems, data or network resources.
Network Resource	Communication links and network bandwidth.
Physical Controls	Controls that are physically implemented. For example, surveillance cameras, motion alarms, door locks, security guards.
Risk	The likelihood of a given threat exercising a particular potential vulnerability, and the resulting impact of that adverse event on an organization.
Security Incident	The attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or services used or provided by the Macon County.
Sensitive Data	Sensitive data includes but is not limited to, passwords, Social Security numbers, credit card information, protected health information (PHI), personally identifiable information (PII), bank account numbers and tax ID numbers that are stored, processed or transmitted on or by Macon County information systems or network resources.

Strong Cryptography	A cryptographic algorithm or protocol that makes it very difficult for an unauthorized person to gain access to encrypted data.
Threat	Condition that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the Macon County.
Two Factor Authentication	The use of two independent mechanisms for authentication. For example, a security token and a password.
User	Anyone who accesses Macon County information systems, data or network resources.
Visitor	A vendor, guest of an employee, service personnel, or anyone who needs to enter a Macon County facility containing information systems, data or network resources for a short duration, usually not more than one day.

2. Roles and Responsibilities

While responsibility for information security on a day-to-day basis is every Macon County employee's duty, specific guidance, direction, and authority for information security is the responsibility of Macon County's Security Committee. The Security Committee is comprised of the Finance Director & IT Director and has assigned the day-to-day responsibilities for information security to Macon County's Information Services (IS) Department. Accordingly, this Department will:

- Establish, document and distribute information security policies, standards and procedures.
- Monitor and analyze security alerts & information and distribute to appropriate Macon County employees.
- Establish, document, and distribute security incident response and escalation procedures
- Administer user accounts, including additions, deletions, and modifications
- Monitor and control all access to *sensitive data*

Reference: PCI DSS v3.0 requirement 12.5 (12.5.1 – 12.5.5)

3. Risk Assessment

Macon County IT Director must regularly identify, define, and prioritize risks to the confidentiality, integrity, and availability of its information systems, network resources and data. Macon County Information Technology Department must conduct an annual formal, documented risk assessment of its information systems, data and network resources. The assessment must identify and prioritize the threats and vulnerabilities to Macon County's information systems, data and network resources and define the likelihood and impact of risks.

The risk assessment must be used in conjunction with Macon County's risk management process to identify, select, and implement appropriate and reasonable controls to protect the confidentiality, integrity, and availability of Macon County's information systems, network resources, and data.

Macon County must conduct risk management on a regular basis and select & implement reasonable, appropriate, and cost-effective controls to manage, mitigate, or accept identified risks. All such controls must be commensurate with identified risks.

Annually, Macon County's IT Director of Information Services must submit an information security risk management report to appropriate Macon County management. The report must identify the significant risks to Macon County information systems, data and network resources that have been identified during the past year, the risks that have been accepted and which risks have been mitigated.

Reference: PCI DSS v3.0 requirement 12.1.2

4. Logical Access Control

Macon County employees, contractors, commisioners, service providers and vendors must not attempt to gain logical access to Macon County information systems, data or network resources for which they have not been given proper authorization.

Logical access to Macon County information systems and media containing sensitive data must be denied until specifically authorized by appropriate Macon County personnel.

Appropriate Macon County information system owners and/or data custodians or their designated delegates must define and approve logical access to Macon County information systems and media containing sensitive data.

Logical access to Macon County information systems and media must be provided only to those having a need for specific access in order to accomplish a legitimate task and must be based on the principles of need to know and least possible privilege.

Macon County must have a formal, documented user management process which enables the controlled addition, change, and termination of logical access rights on Macon County information systems, data and network resources. The process must be capable of granting different levels of access to Macon County information systems, data and network resources.

A unique user name must be used by all persons accessing Macon County information systems and media containing sensitive data. Along with the unique user name, one of the following authentication methods must be used:

- Password
- Token devices
- Biometrics

Two factor authentication must be used by employees, contractors, service providers and vendors for remote access to Macon County information systems and media containing sensitive data. Macon County employees who telecommute must take all precautions necessary to secure any and all sensitive Macon County data in their homes and prevent unauthorized access to any Macon County information system or data.

Vendor maintenance ports on Macon County information systems that contain sensitive data must be disabled until the specific time they are needed by the vendor. After appropriate use by the vendor, they must again be disabled.

Group, shared or generic accounts or passwords must not be used on Macon County information systems that store, process or transmit sensitive data. The following requirements must be met for passwords on such systems:

- User passwords must be changed at least every 90 days.
- Passwords must be at least 7 characters long and include both numeric and alphabetic characters.
- First time passwords must be unique for each user and must be changed upon first use.
- Password reuse must be restricted to no more than once every 4 uses.

- Via the use of strong cryptography, all passwords must be unreadable during transmission and storage on all information systems that store, process or transmit sensitive data.
- User accounts must be locked after six failed login attempts. The lockout must be for at least 30 minutes or until authorized Macon County personnel unlock the account.
- Macon County employees must not use passwords that are also used for non-Macon County accounts.

Activation of information system locking software or log off must occur when a user session on a Macon County information system is inactive for more than 15 minutes.

User identity must be appropriately verified before any password, which enables access to a Macon County information system or network resource, is reset.

User accounts that are inactive for more than 90 days on Macon County information systems that store, process or transmit sensitive data must be disabled or removed.

At least every 6 months, appropriate Macon County information system owners and/or data custodians or their designated delegates must review and verify logical access rights to Macon County information systems and media containing sensitive data. Such rights must be revised as necessary. Inactive accounts over 90 days old must be either removed or disabled.

Macon County employees and contractors experiencing a change in status (e.g. termination, position change) must have their logical access rights promptly reviewed, and if necessary, modified or revoked.

Reference: PCI DSS v3.0 requirements 7.1 (7.1.1 – 7.1.4), 7.2 (7.2.1 – 7.2.3), 8.1, 8.2, 8.3, 8.5 (8.5.1 - .16)

5. Physical Access Control

At least annually, Macon County IT Department must identify all of its physical areas that must be protected from unauthorized physical access. The assessment must take into consideration areas where sensitive data is stored, processed, or transmitted as well as the location of any supporting assets or critical infrastructure.

Macon County information systems and electronic & non-electronic media containing sensitive data must be located in physically secure areas ("limited access area"). Typically, such areas have a defined security perimeter such as a card controlled entry door or a staffed reception desk. Macon County information systems located in unrestricted, public access areas must be physically secured to prevent theft.

Access to limited access areas must be denied until specifically authorized by appropriate Macon County personnel. Such access must be provided only to those having a need for specific access in order to accomplish a legitimate task and must be based on the principles of need to know and least possible privilege. Access privileges to limited access areas must be reviewed at least annually.

Cameras or other access control mechanisms must monitor the entry and exit points of Macon County physical areas containing information systems that store, process or transmit sensitive data or electronic & non-electronic media containing sensitive

data. Camera data must be stored for at least three (3) months unless otherwise restricted by law.

Macon County IT Department must control and restrict physical access to publicly accessible network jacks; it must also restrict physical access to wireless access points (WAPs), gateways and handheld devices located at Macon County facilities.

Backup media, both paper and electronic, that contains sensitive Macon County data must be stored in a secure location. The location's security must be reviewed at least annually. An inventory of all such media must be conducted at least annually.

Macon County electronic and non-electronic media containing sensitive data must be classified so that it can identified as "confidential." Distribution of such media outside the Macon County must be tracked and logged. Such media must only be distributed outside Macon County via a delivery method that can be tracked.

Appropriate Macon County management must approve the movement of any Macon County media containing sensitive data from a limited access area.

Macon County must have a formal, documented process in place that clearly identifies and distinguishes between employees, contractors, and visitors.

Visitors to limited access areas must be formally authorized by an appropriate Macon County employee to access such areas. Visitors to limited access areas must be given a physical token (i.e., a badge) that has an expiration date and that identifies a visitor as a non-employee. Visitors must return their physical token upon leaving a limited access area or at the expiration date.

Visitors must sign a visitor's log prior to being granted physical access to limited access areas. The log must document the visitor's name, the company represented, the authorizing Macon County employee, and the date & time of entrance and departure. Unless otherwise restricted by law, visitor logs must be retained for at least three (3) months.

Reference: PCI DSS v3.0 requirements 9.1 (9.1.1 – 9.1.2), 9.2, 9.3 (9.3.a – 9.3.c), 9.4, 9.5, 9.6, 9.7, 9.8 (9.8.1 – 9.8.2), and 9.9

6. Security Training and Awareness

Macon County IT Department must ensure that employees and contractors are provided with sufficient training and supporting reference materials to enable them to appropriately protect Macon County information systems, network resources, and data. Macon County IT Department must provide information security awareness to its employees and contractors upon hire and then at least annually.

Macon County must provide regular security information and awareness to its employees and contractors via methods such as log-in banners, posters, memos and periodic meetings. Such information and awareness must include, but is not limited to:

- Any significant revisions to Macon County information security policies
- Significant new Macon County information security controls or processes
- Significant changes to Macon County information security controls or processes

- Significant new security threats to Macon County information systems, network resources, or data
- Information security best practices

Employees must acknowledge, at least annually, that they have read and understood Macon County's information security policy.

Reference: PCI DSS v3.0 requirements 12.6 (12.6.1 – 12.6.2), 12.7

7. Employee Technologies

Employee technologies (i.e., remote-access technologies, wireless technologies, removable electronic media, laptops, PDAs) that access sensitive Macon County data must only be used by employees and contractors if the following controls are in place:

- Appropriate Macon County management approval for the use of the technologies
- Appropriate authentication with ID and password is used
- A regularly updated inventory of devices, approved network locations for their use, and list of the persons authorized to access the devices
- Devices are labeled with owner name, contact information, and a description of the device's purpose
- Devices are appropriately used and placed in appropriate network locations
- Macon County maintains a regularly updated list of approved devices

When payment card data on Macon County information systems is remotely accessed, the data must not be copied, moved, or stored onto local hard drives or removable electronic media.

Remote access sessions to Macon County information systems containing sensitive data must be disconnected after twenty (20) minutes of inactivity. Remote access technologies used by vendors to access Macon County information systems containing sensitive data must be turned off when not in use by the vendors.

Reference: PCI DSS v3.0 requirements 12.3 (12.3.1 – 12.3.4, 12.3.6 – 12.3.10)

8. Data Retention and Disposal

Macon County IT department must keep the storage of sensitive data to the minimum necessary required for business, legal and/or regulatory purposes. When no longer required for such purposes, sensitive data on Macon County information systems or on Macon County electronic and non-electronic media must be appropriately disposed of. The following disposal methods must be used:

- Non-electronic media must be cross-cut shredded, incinerated or pulped.
- Electronic media must be purged, degaussed, shredded or otherwise destroyed so that sensitive data cannot be reconstructed.

Sensitive data on Macon County electronic media and information systems must be securely and thoroughly erased before such items can be re-used

Macon County information systems and electronic & non-electronic media that contain sensitive data must be inventoried and audited on a quarterly basis to ensure that the stored data does not exceed Macon County's data retention requirements.

After a payment card transaction is authorized, the following types of data must never be stored in electronic or non-electronic form at a Macon County facility:

- Magnetic stripe data
- CVC2/CVV2/CID/CAV2
- PIN/PIN Block

Unless otherwise authorized, credit card primary account numbers (PANs) on Macon County information systems must be masked; the first six (6) and the last four (4) digits of the PAN are the maximum that can be displayed.

PANs stored electronically on Macon County information systems or portable storage devices must be made unreadable. One of the following methods must be used:

- Strong one-way hash functions
- Truncation
- Index tokens and pads
- Strong cryptography

Cryptographic keys must be securely stored and comply with the following key management procedures:

- Generation of strong keys
- Maintenance of an inventory of encryption keys
- Secure key distribution
- Periodic key changes
- Destruction of old keys
- Split knowledge and dual control of keys
- Prevention of unauthorized substitution of keys
- Replacement of known or suspected compromised keys
- Revocation of old or invalid keys

Key custodians must sign a form specifying that they understand and accept their key-custodian responsibilities.

Reference: PCI DSS v3.0 requirements 3.1, 3.2 (3.2.1 – 3.2.3), 3.3, 3.4, 3.5, 3.6, 9.10

9. Transmission of Data

If sensitive data must be sent over an open, public network (i.e., the Internet), strong cryptography such as SSL, TLS, or IPSEC must be used to encrypt the data.

If a Macon County wireless network is used to transmit sensitive data, strong encryption (i.e. WPA2, IPSEC or SSL) must be used.

Strong cryptography must be used whenever sensitive data is sent via end-user messaging technologies (e.g., email, instant messaging, chat).

Reference: PCI DSS v3.0 requirements 4.1, 4.2

10. Malicious Software Protection

Macon County IT Department must deploy anti-virus software on its information systems commonly affected by malicious software. Such software must be capable of detecting, removing and protecting against malicious software including spyware and adware.

Anti-virus software must be kept actively running and capable of generating audit logs. Anti-virus software must be enabled for automatic updates and conduct periodic scans.

Reference: PCI DSS v3.0 requirements 5.1, 5.2, 5.3.

11. Patch Management

Macon County IT Department must have a formal, documented process for regularly identifying and prioritizing relevant and necessary security and functional patches for its information systems and applications that process, transmit or store sensitive data. Macon County IT Department may use a risk based approach for prioritizing security patch installations. All critical new security patches must be applied within one (1) month of release.

*Reference: PCI DSS v3.0 requirements 6.1, 6.2***.**

12. Change Control

Macon County IT Department must develop and implement a formal, documented change control process for information system and software configuration changes. The process must include:

- Identification and documentation of significant changes
- Assessment of the potential impact, including security implications, of significant changes
- Appropriate management approval of all changes
- Ability to terminate and recover from unsuccessful changes
- Testing procedures to ensure the change is functioning as intended
- Communication of completed change details to appropriate persons
- The updating of appropriate information system or software documentation upon the completion of a significant change

Only properly authorized persons may make an emergency change to Macon County information systems, data or network resources. Such emergency changes must be appropriately documented and promptly submitted, after the change, to Macon County's normal change management process.

Reference: PCI DSS v3.0 requirements 6.4 (6.4.1 – 6.4.4)

13. Network Security

Macon County IT Department must develop and implement formal, documented standards for its firewalls and routers. Such standards must include:

- A formal process for approving and testing all network connections and changes to Macon County firewall and router configurations.
- Current diagram(s) of Macon County's computer network . The diagram must show all connections to Macon County information systems that process, transmit or store sensitive data. Changes to the diagram(s) must be appropriately documented.
- Requirements for a firewall at each logical point where Macon County's network connects to the Internet and between any demilitarized zone (DMZ) and Macon County's internal network(s).
- A description of groups, roles, and responsibilities for logical management of Macon County firewalls and routers.
- Documentation and business justification of all services, protocols, and ports allowed by Macon County firewalls and routers, including documentation of security features implemented for insecure protocols (e.g. Telnet, FTP).
- A requirement to review Macon County firewall and router rule sets at least every six (6) months.

Macon County's firewalls must perform stateful inspection and must restrict connections between untrusted networks (i.e. the Internet) and Macon County information systems that process, transmit or store sensitive data. The firewalls must prohibit direct access from the Internet to such information systems, must restrict inbound and outbound traffic to that which is documented as necessary for organizational purposes and explicitly deny all other traffic.

Configuration files on Macon County routers must be secured and regularly synchronized.

A firewall(s) must be installed between any wireless networks and Macon County information systems that process, transmit or store sensitive data. Such firewalls must deny or control traffic from any wireless networks to these information systems.

Outbound traffic from Macon County payment card applications must be sent to IP addresses within a Macon County DMZ; such traffic must not be sent directly to the Internet. Inbound Internet traffic to Macon County payment card applications must be limited to IP addresses within a Macon County DMZ.

All Macon County databases that store sensitive data must be placed in the Macon County's internal network(s) and be segregated from any Macon County DMZ.

Personal firewall software must be installed and active on any mobile and/or Macon County employee-owned computers with direct connectivity to the Internet that are used to access the Macon County's internal network. The personal firewall software must be configured to specific standards and prevent unauthorized users from altering or disabling it.

IP masquerading (e.g., port address translation [PAT] or network address translation [NAT]) must be used for information systems on Macon County's internal network(s).

Reference: PCI DSS v3.0 requirements 1.1 (1.1.1 – 1.1.7), 1.2 (1.2.1 – 1.2.3), 1.3 (1.3.1 – 1.3.8), 1.4.

14. Security Incident Response

Macon County must have a formal, documented security incident response plan. The plan must include:

- Roles, responsibilities, and communication strategies in the event of a security incident including notification of appropriate parties
- Specific incident response procedures
- Business recovery and continuity procedures
- Data back-up processes
- Legal requirements for reporting security incidents
- Coverage and responses for all critical Macon County information systems
- Reference or inclusion of payment card brand incident response procedures
- Procedures for responding to alerts from intrusion detection (IDS), intrusion prevention (IPS) and/or file integrity monitoring systems

The security incident response plan must be tested annually and must designate specific personnel to be available on a 24/7/365 basis in order to respond promptly to information security alerts. The plan must be reviewed regularly and modified as necessary.

Macon County employees who are responsible for responding to security incidents must receive regular and appropriate training in security incident response processes.

Reference: PCI DSS v3.0 requirements 12.10 (12.10.1 – 12.10.6)

15. Logging and Auditing

Appropriate logging and monitoring controls must be implemented on Macon County information systems, data and network resources.

Macon County IT Department must implement automated audit trails on its information systems that store, process or transmit sensitive data. The audit trails must be able to reconstruct the following events:

- Individual accesses to sensitive data
- Actions taken by any individual with root or administrative privileges
- Access to audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of audit logs
- Creation and deletion of system-level objects
- For each of the above events, the following must be recorded:
- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

Logs and audit trails on Macon County information systems that store, process or transmit sensitive data must be reviewed daily. Such logs and audit trails must be monitored by file integrity or change detection software. Log reviews must include intrusion detection and authentication, authorization and accounting (AAA) servers.

Information generated by logging and monitoring controls implemented on Macon County information systems, data and network resources must be protected from unauthorized access. Access to such information must be limited to only those individuals with a need-to-know. Such information must be promptly backed up to a centralized log server and/or media that is difficult to alter. Logs for Macon County external-facing technologies (i.e., firewalls, DNS, email) must be copied onto a log server on the Macon County's internal network. Unless otherwise restricted by law, audit and log file information must be retained for at least one year.

Macon County information systems must have their system clocks and times synchronized with a master time source (e.g. network time protocol [NTP]). Internal Macon County time servers must not all receive time signals from external sources. Specific Internet time servers must be designated from which time updates will be accepted.

Reference: PCI DSS v3.0 requirements 10.1, 10.2 (10.2.1 – 10.2.7), 10.3 (10.3.1 – 10.3.6), 10.4, 10.5 (10.5.1 – 10.5.5), 10.6, 10.7.

16. Information System Configuration

Macon County IT Department must develop and implement formal, documented configuration standards for its information systems. Such standards must be consistent with system hardening best practices as defined by organizations such as SANS, NIST and CIS. At a minimum, the standards must require the following:

- One primary function for servers that process, transmit or store sensitive data
- Disabling of unnecessary and/or insecure services and protocols
- Appropriate configuration of system security settings
- Removal of unnecessary functionality (e.g., scripts, Web servers, subsystems)
- Changing or removing vendor-supplied defaults (i.e., passwords, accounts, SNMP community strings)
- All remote logins that enable administrator access to Macon County information systems storing, transmitting or processing sensitive data must be encrypted.

Macon County IT Department must have a formal, documented process to identify newly discovered security vulnerabilities and update Macon County configuration standards to address new vulnerabilities.
Reference: PCI DSS v3.0 requirements 2.1, 2.2 (2.2.1 – 2.2.4), 2.3, 2.4, 6.2

17. Personnel Vetting

As determined necessary by Macon County's risk assessment, new Macon County employees must be adequately vetted before being hired. Such vetting can include, but is not limited to, background checks, credit checks and/or personal references. Such vetting is especially important for positions that involve access to sensitive data.

New employees who will access sensitive data must sign a confidentiality (non-disclosure) agreement. This agreement must be regularly renewed.

Reference: PCI DSS v3.0 requirements 12.7

18. Information Security Testing

Macon County IT Department must annually, or after any significant changes to its information technology environment, perform internal and external penetration tests of its information systems that process, transmit or store sensitive data. The penetration tests must include both network and application layer tests.

At least quarterly, a wireless analyzer must be used at Macon County facilities to identify all wireless devices in use or a wireless IDS/IPS must be deployed which is capable of identifying all wireless devices in use at Macon County facilities.

Macon County IT Department must conduct appropriate quarterly external vulnerability scans against all of its information systems that are Internet reachable. Macon County must also run quarterly internal vulnerability scans against all of its information systems that process, transmit or store sensitive data.

Per its risk assessment, Macon County must implement and maintain network IDS, host based IDS and/or IPSs to monitor all traffic to Macon County information systems that process, transmit or store sensitive data.

Macon County IT Department must deploy file integrity monitoring software on its information systems that process, transmit or store sensitive data. The software must perform critical file comparisons at least weekly.

Reference: PCI DSS v3.0 requirements 11.1, 11.2, 11.3 (11.3.1 – 11.3.2), 11.4, 11.5.

19. Service Provider Management

If Macon County shares sensitive data with service providers, then Macon County must develop and maintain a service provider management program that meets, at minimum, the following requirements:

- Maintenance of a list of service providers.
- Written acknowledgement from each service provider that they are responsible for the security of the sensitive data the service provider possesses or has access to.
- An established process for engaging service providers that includes proper due diligence prior to engagement.
- Development and maintenance of a program to monitor service providers' PCI DSS compliance.

Reference: PCI DSS v3.0 requirement 12.8 (12.8.1 – 12.8.5)

20. Policy Distribution and Review

This policy must be published and distributed to all appropriate Macon County employees, contractors, vendors, service providers and business partners.

This policy must be reviewed at least annually and revised as necessary.

Reference: PCI DSS v3.0 requirements 12.1, 12.1.1

21. Compliance

Macon County employees and contractors must comply with all applicable parts of this security policy. Compliance is necessary to ensure the confidentiality, integrity and availability of Macon County information systems, data and network resources.

Macon County employees and contractors who do not comply with all applicable Macon County security policies may be subject to disciplinary actions, up to and including termination of employment.

Third party persons (i.e. vendors, service providers) who do not comply with this policy may be subject to appropriate actions as defined in contractual agreements.

Policy Acknowledgment

I have received a copy of Macon County's Information Security Policy and I have read and understand the policy. I agree to observe the terms and conditions of this policy.

Signed Name: _____

Printed Name: _____

Date: _____