Liberty County
Georgia

Information Security and Usage Policy

Effective Date: July 1, 2017

Last Reviewed and Modified: July 1, 2017

Table of Contents

1.0 Introduction

Liberty County information systems collect, manage, and store sensitive information on a regular basis to support County business operations. Liberty County is committed to preserving the confidentiality, integrity, and availability of its information resources while also preserving the open information-sharing requirements of a county government. Liberty County must protect its information assets, provide for the integrity of county processes and records, and comply with all applicable laws and regulations.

2.0 Purpose

The purpose of this policy is to define how to conduct County business in a manner that provides information security to protect the confidentiality, integrity, and availability of information, physical assets and County, employee/ citizen information being stored, viewed, and transmitted on the Liberty County network, Liberty County Radio Network, and over the internet.

3.0 Scope

This policy applies all Liberty County employees, elected officials, consultants, contractors, vendors, temporary employees, non-employees, and volunteers who are employed, contracted, or volunteering with Liberty County and who receive, create, store, handle, or transmit Liberty County sensitive information or personally identifiable information in hard copy or electronic format.

4.0 Policy Review and Governance

It will be the responsibility of the Liberty County Information Technology to review this policy on an annual basis. Governance of this policy shall be achieved at the Departmental level following review by the Liberty County Information Technology.

5.0 Information Security

The purpose of this section is to define how business is conducted in a manner that provides security to protect the confidentiality, integrity, and availability of information assets, physical assets, Liberty County information, and citizen/ customer information. Information Security is established and maintained by the Information Technology department, and includes the following elements:

- Roles and responsibilities for the Information Security;
- Information security policies and procedures to provide for the confidentiality, integrity, and availability of information regardless of the form of the information asset;

- Computer access controls, including the identification, credentialing and authentication of employees, administrative consultants, contractors, non-employees, and clients;
- An incident response plan ("IRP") to cover physical assets;
- Laptop/mobile computing and radio device controls for remote access/transmission of data and information;
- Annual risk assessment to identify reasonably foreseeable risks based on present threats and vulnerabilities to the security and confidentiality of the Liberty County network;
- Investigation of improper behavior or potential criminal acts generated or transmitted electronically utilizing qualified personnel with investigative training, experience, and knowledge in pertinent laws and toolkits for doing forensics;
- Security Awareness Training and Education ("SATE") which emphasizes the importance to the county of protecting County Sensitive Information and personally identifiable information ("PII") during different states, as well as, how and when to report a potential security breach or incident to Information Technology;
- Monitor and audit all aspects of Information Technology use and implementation for compliance with our Information Security goals;
- Monitor for intrusions and other unauthorized use;
- Annually revisit Information Security policies and procedures for changes in laws, as well as, technology and standards changes; and
- Support the Human Resources Department with ensuring continuity between the ISP (Information Security Policy) and its operating procedures, such as background investigations, terminations, computer breeches, fraud, embezzlement, unlawful acts, or other forms of dishonesty and violations of County policies.

5.1 Information Security Program

1. The Director of Information Technology shall be designated to perform oversight, conduct constant review and monitoring, complete maintenance and updates, and coordinate changes and deployments to stay in compliance with legal regulations, technical advancements, and industry best practices.
2. The County Attorney and County Administrator will assist the Director of Information Technology in matters regarding the safeguarding of Liberty County Sensitive Information and PII and compliance issues to uphold our ISP and keep it current.
3. The Information Technology Department plays a key role in the deployment of technology and implementation of appropriate access controls to maintain the confidentiality, integrity, and availability of Liberty County data.

4. The Director of Information Technology and the Information Technology department will work closely to coordinate security measures to negate the possibility of data security breaches early during the software development and/or deployment lifecycle.
5. The Director of Information Technology is responsible for ensuring that all Information Security policies, standards, and practices are implemented in the deployment and use of the Liberty County network, as well as, followed by all employees and other users provided electronic access to Liberty County Sensitive Information, PII or other Liberty County data.
6. Users, whether employees, administrative consultants, contractors, vendors, or third parties, elected officials, volunteers are responsible for following Information Security Policies, standards, and practices.
7. It is the responsibility of each department to notify the Information Technology Department of any suspected data breach or computer incident/anomaly.

5.2 Information Security Policy ("ISP")

1. All Information Security Policies are created to define our expectations for security practices in the Liberty County computing environment. These policies assist in meeting regulatory and legal requirements mandated by the Federal Government, State of Georgia, or Liberty County Board of Commissioners by defining how data is to be handled and safeguarded while developed, stored or transmitted.
2. Policies, standards, and practices are established to provide definition and the means for guidance on implementation and maintenance of our information security posture.
3. Policies should be written in a manner which requires little change as technology advances. In most cases, users are discouraged from identifying specific technology or products unless it relates to a mandated requirement or law.
4. Policies, standards, and practices should be reviewed annually to ensure they provide best practices for the handling and safeguarding of Liberty County Sensitive Information and PII based on recent legislation.
5. Approved policies will be made available on the County Internet and Intranet.
6. All users will be required to sign an acknowledgement of the highlights of this policy, that requires each user to become fully familiar with the entire policy, before the user is granted access to the Liberty County Network or any Liberty County information system, mobile device, smart phone or radio. ***(see appendix C)***

6.0 Physical Security

6.1 Purpose

The purpose of physical security is to provide a safe and secure working environment and promote the protection of our assets. The security of our confidential information (such as Liberty County Sensitive Information and personally identifiable information ("PII"), as well as, the information shared with us by our citizens must be maintained. Customer-friendly procedures shall be engaged to ensure only authorized employees, administrative consultants, contractors, vendors, and visitors have access to our facilities.

6.2 Scope

This section applies to the physical areas where information assets are kept. These areas include server rooms, telecom closets, radio rooms, radio tower sites, and certain offices areas that may contain Liberty County Sensitive Information or PII. These areas must be physically secured to prevent theft, tampering, tapping, recording, or damage.

6.3 Physical Security Policy

6.3.1 Facility Access Control

It is every employee's responsibility to work toward, and maintain and preserve a secure physical work environment.

- Department heads, elected officials and supervisors are responsible for ensuring that proper building security practices are maintained and that their employees follow access control policies and procedures.
- The Human Resources Department ("Human Resources") and/or the Liberty County Sheriff's Office will authorize the issuance of badges (Liberty County Photo ID badge) to new employees granting them appropriate facility access beginning on the date of hire. Employees shall wear their issued badges always while on Liberty County premises.
- The Human Resources Department, Information Technology Department and Sheriff's Office are responsible for activating all badges and providing them to employees of long-term contractors. Security Officers and deputies are responsible for providing visitor badges if required by other policies.
- All employees are to enter the building at the facility's designated employee entrance.
- At termination, all employees must return their badges to their supervisor, department head, elected official or Human Resources.
- At termination, it is the department head, elected official or Human Resources responsibility to retrieve the badge from the terminated employee and return it to the activating entity for deactivation and shredding.

- Human Resources develops and maintains procedures to follow when employees forget or lose their badges.
- No individual will be permitted to access secure areas of our facilities beyond the main reception area without an appropriate badge worn visibly unless escorted by an employee.
- County Administration is responsible for developing policies and procedures to control the use and dissemination of physical building keys. Lost or stolen keys must be reported to County Administration or Building Maintenance immediately.

6.3.2 Effective Building Security

Effective building security is possible through the cooperative efforts of County Administration, Building Maintenance, Information Technology, and the Sheriff's Office. The following rules apply:

- Keys and badges are not to be left unattended in plain view or carried in a way that makes them easy to be lost or stolen.
- When employees enter, or leave a building after hours, the exterior doors must be locked to prevent unauthorized access.
- If a door does not close or lock properly, Building Maintenance should be notified immediately.
- County Administration must be notified whenever a potential or actual security problem exists, including unauthorized entry, theft of property, or loss of keys or badges.

6.3.3 Protection of Sensitive and Critical Information

The physical areas where information assets are kept must be protected from unauthorized access. The following rules apply to physical access:

- No laptop or portable computer that potentially contains sensitive personal information, that has an unencrypted hard drive(s) and/or does not meet the security requirements specified within this policy shall be allowed to leave County facilities (local County network) until such changes are implemented on the device. Employees will not be issued a laptop or portable computer as their primary workstation unless approved by Information Technology.
- Employees, contractors, and vendors must secure their work areas to protect Liberty County Sensitive Information and PII.
- Workstations, laptops, tablets, and smartphones shall be placed in locations that protect the confidentiality of data. All confidential documents and media must be securely stored.
- Workstations, laptops, tablets, and smartphones must be secured in accordance with the password policy.

- All documents and media containing PII must be discarded carefully. Documents, DVDs, and CDs containing PII must be shredded. Electronic media containing PII must be destroyed by Information Technology.
- Information Technology will provide high-level physical and environmental protection of the technical infrastructure to minimize the risk of unauthorized access and environmental hazards.
- Information Technology will protect telecommunications lines and equipment by locking and controlling access points in all buildings and structures to ensure both availability and confidentiality.

Any movement of information, software media, hardware or other IT physical assets will be strictly controlled. Only authorized personnel are permitted to take Liberty County property off-premises. Computing equipment taken off-premises is subject to the Laptop/Mobile Computing and radio Security Policy.

6.3.4 Physical Security Audits

It is the responsibility of the Liberty County Sheriff's Office and or Building Maintenance to conduct periodic physical security audits to ensure compliance with this policy.

- The Sheriff's Office will conduct an audit of the physical security on the perimeter of the building to ensure door alarms and access control devices are working properly.
- IT will conduct an audit of the physical security of interior doors leading to server rooms, telecom closets and other secure areas of the Liberty County Network to ensure door alarms, access control devices, physical locks and environmental control systems are working properly and have been properly maintained and serviced.

7.0 Internet Usage Policy

Liberty County, Georgia is dedicated to using the Internet as technology enabling efficient delivery and exchange of information within the county, with other governmental agencies, and for the public. However, due to the derisive nature of the Internet, it is necessary to define and bar inappropriate usage.

7.1 GEORGIA COMPUTER SYSTEMS PROTECTION ACT

Liberty County is under the jurisdiction of the Georgia Computer Systems Protection Act, enacted by the 1991 Georgia General Assembly and signed into law by the governor effective July 1, 1991, which establishes certain acts involving computer fraud or abuse or crimes punishable by defined fines, imprisonment or both.

O.C.G.A § 16-9-93 states:

(a) Computer Theft. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;

(2) Obtaining property by any deceitful means or artful practice; or

(3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property shall be guilty of the crime of computer theft.

(b) Computer Trespass. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;

(2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or

(3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass.

(c) Computer Invasion of Privacy. Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.

(d) Computer Forgery. Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter, shall be guilty of the crime of computer forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to the crime of computer forgery if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument.

(e) Computer Password Disclosure. Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure.

(f) Article not Exclusive. The provisions of this article shall not be construed to preclude the applicability of any other law which presently applies or may in the future apply to any transaction or course of conduct which violates this article.

(g) Civil Relief; Damages.

(1) Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits and victim expenditure.

(2) At the request of any party to an action brought pursuant to this Code section, the court shall by reasonable means conduct all legal proceedings in such a way as to protect the secrecy and security of any computer, computer network, data, or computer program involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party.

(3) The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

(4) A civil action under this Code section must be brought within four years after the violation is discovered or by exercise of reasonable diligence should have been discovered. For purposes of this article, a continuing violation of any one subsection of this Code section by any person constitutes a single violation by such person.

(h) Criminal Penalties.

(1) Any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than $50,000.00 or imprisoned not more than 15 years, or both.

(2) Any person convicted of computer password disclosure shall be fined not more than $5,000.00 or incarcerated for a period not to exceed one year, or both.

O.C.G.A § 16-9-93.1 provides:

(a) It shall be unlawful for any person, any organization, or any representative of any organization knowingly to transmit any data through a computer network or over the transmission facilities or through the network facilities of a local telephone network for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information if such data uses any individual name, trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely identify the person, organization, or representative transmitting such data or which would falsely state or imply that such person, organization, or representative has permission or is legally authorized to use such trade name, registered trademark, logo, legal or official seal, or copyrighted symbol for such purpose when such permission or authorization has not been obtained; provided, however, that no telecommunications company or Internet access provider shall violate this Code section solely as a result of carrying or transmitting such data for its customers.

(b) Any person violating subsection (a) of this Code section shall be guilty of a misdemeanor.

(c) Nothing in this Code section shall be construed to limit an aggrieved party's right to pursue a civil action for equitable or monetary relief, or both, for actions which violate this Code section.

7.2 Definitions and Terms

Definitions and common terms used in discussing the Internet are:

- Client: One end of a network protocol that provides a user interface to the server end.
- Computer Ethics: Accepted manners to be observed while using the Internet.
- Electronic Mail (E-mail): A means of sending messages between computers using a computer network or over a modem connected to a telephone line.
- Internet: A medium through which information or electronic mail may travel. Computer users can currently use the Internet like a telephone or fax to exchange information quickly and efficiently.

- Server: Computer(s) that provide information to client programs via the Internet through programs that send information to Web browsers such as Netscape Navigator and Microsoft Internet Explorer.
- Web Page: A single page displayed by a Web browser.
- World Wide Web (WWW or the Web): That part of the Internet that provides a way for organizations or individuals to publish information that is then available to a worldwide audience.

7.3 Minimum Internet Usage Policy Requirements

7.3.1 Information Content and Use of the System

Liberty County reserves the right to monitor and/or log all network activity, with or without notice, including e-mail and all web site communications. Users should have no reasonable expectation of privacy in the use of these resources.

Uses that are acceptable:

- Communications and information exchanges directly relating to the mission, charter, tasks and work of Liberty County;
- Announcements of state laws, procedures, hearings, policies, services, or activities; and
- Use for advisory, standards, research, analysis, and professional society or development activities related to the user's governmental duties.
- Occasional use for personal reasons (i.e., email from/to friends or relatives)

Uses that are unacceptable:

It is unacceptable for a user to use, submit, publish, display, or transmit on the network or on any computer system any information that:

- Violates or infringes on the rights of any other person, including the right to privacy;
- Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;
- Violates agency or departmental regulations prohibiting sexual harassment;
- Restricts or inhibits other users from using the system or the efficiency of the computer systems;
- Encourages the use of controlled substances or uses the system for criminal intent; or

- Uses the system for any other illegal purpose.

It is also unacceptable for a user to use the facilities and capabilities of the system to:

- Conduct any non-approved business;
- Solicit the performance of any activity that is prohibited by law;
- Transmit material, information, or software in violation of any local, state or federal law;
- Conduct any political activity;
- Conduct any non-governmental-related fund raising or public relations activities;
- Engage in any activity for personal gain or personal business transactions; or
- Make any unauthorized purchases.
- Regularly transmit data associated with non-work related material.

7.4 Copyrighted Material

Users may download copyrighted material, but its use must be strictly within the agreement as posted by the author or current copyright law. The federal Copyright Act at 17 U.S.C. 101 et. seq. (1988), protects and prohibits misuse of all original works of authorship in any tangible medium of expression. This includes a prohibition on plagiarism (using someone else's ideas or writing and passing it on as one's own).

7.5 Public Domain Material

Any user may download public domain programs for his/her own business-related use, or may redistribute a public domain program non-commercially but does so with the knowledge that by doing so, he/she also assumes all the risks regarding the determination of whether a program is in the public domain.

7.6 Electronic Mail [E-Mail]

E-mail is considered network activity; thus, it is subject to all policies regarding acceptable/unacceptable uses of the Internet and the user should not consider e-mail to be either private or secure.

7.7 Regulation and Enforcement

The Liberty County Information Technology Department, Liberty County Administration and the Liberty County Sheriff's Office are responsible for compliance with provisions of this policy and for investigating suspected non-compliance. These duties include, but are not limited to:

- Investigation of alleged or suspected non-compliance with the provisions of the policy; and
- Suspensions of service to users or of user access with or without notice when deemed necessary for the operation and/or integrity of the state communications infrastructure or connected networks.
- When an instance of non-compliance is suspected, or discovered in a computing system or network connected to the state network, the agency shall proceed in accordance with Liberty County rules. Internal discipline, up to and including discharge, may be appropriate in some cases of non-compliance with this policy. Criminal or civil action may be initiated in appropriate instances.

7.8 Liability

Liberty County makes no warranties of any kind, whether expressed or implied for the service that is the subject of this policy. In addition, Liberty County will not be responsible for any damages whatsoever which employees may suffer arising from or related to their use of any Liberty County electronic information resources, whether such damages be incidental, consequential, or otherwise, or whether such damages include loss of data resulting from delays, non-deliveries, mistaken deliveries, or service interruptions whether caused by either a Liberty County negligence, errors, or omissions. Users must recognize that the use of Liberty County electronic information resources is a privilege and that the policies implementing usage are requirements that mandate adherence.

8.0 Mobile Computing, Smartphone and Radio Security and Issuance Policy

8.1 Purpose

The purpose of this policy is to define guidelines for the safety and security of laptops, tablets, smartphones, radios and other mobile computing devices.

8.2 Applicability

This policy applies to all employees, elected officials, administrative contractors, temporary personnel, volunteers and the like who have been permitted access to Liberty County Sensitive Information or Personally Identifiable Information ("PII") on the Liberty County network via a laptop computer or other pervasive/mobile computing devices such as tablets, iPad, iTouch, iPhone, Palm, Blackberry, Android, WebOS, netbook, web-enabled cellphone, public safety portable and mobile radios and like devices ("laptop/mobile device").

8.3 Scope

Protection of laptop/mobile devices, especially when used off-site, is necessary in order to reduce the risk of both unauthorized access to the data contained on the device, as well as the data that the device has access to on the Liberty County network. Protection is also necessary to safeguard against loss or damage of the device itself. Generally, a laptop or other mobile computing device should be given the same level of protection as Liberty County Sensitive Information or PII in hard copy, on the Liberty County network, or in other Liberty County controlled environments.

8.4 Policy

1. Shipments of new, unassigned or returned laptops/mobile devices (to include all tablets, smartphones, radios etc.) are to be stored by Information Technology in a locked and secured closet or other secure area to ensure the devices are unaltered or tampered with before issuance to employees.
2. Laptops/mobile and radio devices will be configured and issued only by Information Technology following IT Department issuance procedures outside of the scope of this policy.
3. Security instructions to users will be included with any laptop/mobile and radio devices issued by the Information Technology department.
4. A locking cable to secure the laptop/mobile device to a large stationary object, such as a desk or table, will be issued upon request or as needed with each laptop/mobile device, except smartphones.
5. In 'open' access areas, a laptop restraint/lockdown device will be used when the computer is left unattended if deemed necessary to protect it.
6. Tamper-proof identification labels printed with "Property of Liberty County Georgia" and an inventory identification number and barcode shall be visibly placed on all laptops/mobile devices and radios, except smartphones, to assist in identification if

stolen or misplaced and inventory accountability. (Where a safety issue is involved, the local security environment may necessitate masking the label.).

7. The laptop/mobile and radio device make, model, serial number, configuration, and media access control address ("MAC address") as well as any other identifiable information about the device, is to be recorded and stored in a safe location, or in a secure program or database, in order to give precise information to authorities in the case of theft or loss. This information is to be collected and maintained by the Information Technology department.
8. The Information Technology Department ("IT") is responsible for assuring that all laptop/mobile and radio devices owned by or used by Liberty County have the most recent software, hardware or firmware configuration and available upgrades installed.
9. Only the Information Technology department is authorized to reprogram, alter, or change any Mobile Device, smartphone or radio.
10. IT is responsible for assuring that all laptop/mobile devices and smartphones are joined to the Liberty County domain and are given the least required security access to the Liberty County network and that all devices are joined to or installed in any Mobile Device Management ("MDM") system Liberty County is using or has employed prior to the issuance to any employee, elected official or another non-employee user.
11. Unattended storage standards for laptop/mobile devices and radios should be the same as those for the storage of similar hard copy information.
12. NO laptop/mobile devices or radios will be issued until a signed hand receipt showing in detailed what was issued, any identifiable information (IE: Serial numbers, inventory number, make, model and cost), date of issuance, employee or non-employee or volunteer that the device was issued and purpose of the issuance has been obtained by the Information Technology department. ***See Appendix B for an example hand receipt to be used if no electronic version is available.***
13. The user being issued the laptop/mobile device or radio has overall responsibility of the confidentiality, integrity, availability and accessibility, condition, and loss of his/her assigned Liberty County laptop/mobile device, smartphone or radio and the data or information on or accessible through such device(s).
14. Encryption to maintain confidentiality and protect against the bypass of the software controls (IE. Booting for a system disk or USB, file encryption) must be utilized. Encryption will be used with sending and receiving Liberty County Sensitive Information or PII whenever possible.
15. Anti-virus/anti-malware software will be installed on the laptop/mobile devices and all incoming disks/magnetic/digital media/jump drives etc. should be virus checked before being used in accordance with the Anti-Virus and Malware policy.
16. Users must take steps to prevent casual overview, listening or attempted use by unauthorized personnel. The use of privacy screens or screen savers is encouraged.
17. Radios should be at the lowest volume possible when in public or unsecured areas.
18. Mobile Devices should have any available firewalls enabled always if such an option is available depending on the Mobile Devices operating system or firmware.

19. Virtual Private Networking "VPN" should be employed and used by all Mobile Devices whenever possible and practical to communicate with Liberty County when away from the Liberty County Network and for all internet communications.
20. User ID and authentication is required before access is given to data and applications residing on any laptop/mobile device. Some smartphones that allow for pattern or PIN authentication without a User ID, is acceptable for accessing the device itself.
21. A screensaver and password or "clear and lock" feature will be used on all laptop/mobile devices to protect the devices if the user must leave the activated device: a user password must be entered for further access.
22. Password and PINs must meet the standards set forth in the Liberty County Active Directory Account, Password, and PIN Policy.
23. To help prevent damage and theft, a laptop should not be placed in or as checked baggage. If a laptop/mobile device, smartphone, or radio must be left in or installed in an automobile, it must be locked and secured in the truck or otherwise out of plain view whenever possible.
24. Losses of any laptop/mobile device, smartphone or radio will be immediately reported to the Information Technology Department and the user's supervisor or department head. Any such loss of a device shall be treated as a Security Incident and handled as per the Liberty County Incident Response Plan ("IRP").

8.5 Personal Mobile Device Use

Liberty County provides its employees with Laptops/mobile devices, smartphones, and radios to use in their assigned jobs and roles while employed with Liberty County. The use of personal laptops/mobile devices, smartphones, and radios is prohibited. Employees are also prohibited from using their personal devices to store, transmit, view or email any Liberty County Sensitive Information or PII without permission of the Director of Information Technology.

9.0 Sensitive Information Handling Policy

9.1 Purpose

The purpose of this policy is to define the types of sensitive information stored by us or available to Liberty County users, and to set forth guidelines for handling Liberty County Sensitive Information and Personally Identifiable Information ("PII") while in transmission, storage (at rest), or in use/creation.

9.2 Scope and Applicability

This policy applies to all employees, elected officials, administrative consultants, contractors, vendors, temporary personnel, non-employees, volunteers, and the like who receive, create, store, handle and transmit Liberty County Sensitive Information or PII in hard copy and electronic format.

9.3 Policy

This policy establishes the guidelines for safeguarding PII or Liberty County Sensitive Information during transmission or while in storage (at rest), or when being initially received, developed, or processed. This policy also covers the hard copy of this information from initial collection or printout.

9.3.1 Labeling and Identification

- All data that is transmitted electronically that contains sensitive personal information such as but not limited to date of birth or social security number will be encrypted.
- Public information does not require any special labeling.
- Liberty County Sensitive Information may or may not require labeling. The author, project manager, department head or elected official should provide specific guidance on appropriate labeling. If in doubt, label the information as "Confidential" until instructed otherwise.
- PII should not be labeled as to not bring attention to it. A cover sheet can be placed on it and marked as "Confidential".
- Labels should be used both on printer/hard copies and electronic formats.

9.3.2 Safeguarding During Transmission

- All transmittal of Liberty County Sensitive Information and PII on public networks or wireless systems will be done using encryption technology. For instance, email encryption, PGP, VPN, secure file transfer, WPA2 and SSL can be used.
- When faxing Liberty County Sensitive Information or PII, the sender should ensure that the recipient is available to receive the fax and validate the number of pages received or that the receiving fax requires a PIN or other form of identification (IE. RFID card) to receive the information.

- If transmittal is via mail, some form of certified mail or a service which provides a chain of custody (IE. UPS or FedEx, or certified mail with delivery confirmation) should be used.

9.3.3 Safeguarding During Storage (At Rest)

- When Liberty County Sensitive Information and PII is stored on Liberty County information computing assets, it should be protected appropriately using available user authentication and file privileges, such as encryption when required.
- Encryption meeting IT standards will be used when storing Liberty County Sensitive Information or PII on laptops, PC's, smartphones, or any other devices.
- Storage of personal information should be avoided on unencrypted USBs, jump drives, CDs, or DVDs.

9.3.4 Safeguarding During Creation/Development/Processing

- When initially receiving Liberty County Sensitive Information and PII, the information may be handwritten, perhaps on a form. If this is the case, the same care must be taken to protect this initial piece of paper as you would the formal hardcopy or printout of this information. At a minimum, this information should be secured in a locked office, filing cabinet or desk.
- Liberty County Sensitive Information or PII placed in a document or spreadsheet should be labeled as confidential prior to saving.
- A file or folder containing Liberty County Sensitive Information or PII should not be shared with anyone who is not authorized to access such information.

9.3.5 Disposal of Liberty County Sensitive Information and PII

- Written notes or hardcopy/printout and faxes when no longer needed or required to be retained must be disposed of in an appropriate shred/burn bin or shredded using a cross cut shredder. (Current shredders can be used until replaced with cross cut shredder)
- Whenever possible, ensure that your screen is not visible to others.
- Discarded computer equipment (including copiers, printers, and fax machines, hard drives, ribbons, memory modules) must be decommissioned and the hard drive destroyed by the Information Technology department using a program or method that permanently eliminates any Liberty County Sensitive Information or PII.
- Any computer equipment being sold or transferred to other organizations must be properly sanitized (securely cleared of all information) by the Information Technology Department.

9.3.6 Access and Sharing of Sensitive Information

- The security and safeguarding of information and employee information should be taken seriously. Failure of an individual to successfully complete the background check, including drug testing, may result in non-use of information computing

resources. Employee access to information computing resources will not be provided until a background check is completed by Human Resources and all checks above have been completed and reviewed.

- Prior to being provided access to Liberty County Sensitive Information or PII, users must acknowledge the safeguarding requirements outlined in the Information Security Policy.
- The release of Liberty County Sensitive Information or PII, whether written, oral, or electronic, to persons outside of Liberty County is prohibited unless authorized by applicable law, elected official, Information Technology, County Attorney, or County Administration.
    - In such cases, a signed nondisclosure agreement should be entered between the recipient of Liberty County Sensitive Information or PII and the person, persons or company receiving the information.
    - Information may be disclosed if it is required by legal process, court order or Georgia Open Records Acts or as may be determined by the County Attorney or County Administration.

9.3.7 Termination

- Individuals having access to Liberty County Sensitive Information or PII who are terminating their employment/relationship with Liberty County will have their user ID disabled, access control ID card revoked and will be advised as to the responsibilities with respect to Liberty County Sensitive Information and PII.
- All user accounts will be disabled and retained for a period of at least (6) six months following termination of employment.
- The terminating employee will be alerted to the legal consequences of using, retaining or disclosing Liberty County Sensitive Information or PII for any purpose not expressly authorized by us in writing.

10.0 Active Directory Account, Password, and PIN Policy

10.1 Purpose

The purpose of this policy is to define and establish access controls and minimum security requirements to all Users that access the Liberty County network.

10.2 Policy

10.2.1 Account creation and deletion

1. Information Technology will maintain the Liberty County Active Directory which is a central repository of all users, groups, and email accounts on the Liberty County network.
2. Information Technology will create user and group accounts for all users on the Liberty County network granting them only the least amount of permissions required to perform their jobs.
3. Information Technology will review all user and group accounts contained in the Active Directory on a semi-annual basis disabling and/or removing any accounts that are no longer needed or accounts of employees that are no longer employed by Liberty County.
4. Information Technology will ensure that all computers connected to the Liberty County network are configured to provide automatic screen locking on any computer that is unused for a period of (30) minutes and that the computer requires a user to provide login information or password to regain access to the computer or Liberty County network.
5. Human Resources, department heads, supervisors and elected officials will notify Information Technology anytime an employee leaves the employment of Liberty County within (24) twenty-four hours of termination or separation from Liberty County.
6. These accounts, along with their e-mail mailboxes, will be retained for a minimum period of (6) six months or according to records retention law from separation or longer as instructed by the County Administrator, department head or elected official.

10.2.2 Securing workstations when not in use

- Liberty County employees will ensure that their workstations, laptops and other mobile devices are secured and locked
    - anytime the user is away from their computer for an extended period of time
    - or any time the computer is out of the employee's direct sight
    - or anytime a citizen or other unauthorized person or person(s) are in or near the employee's computer.
    - If the employee is leaving their computer for an extended period and plans to return, the employee will lock the computer by doing the following:
      Pressing CTRL + ALT + DELETE
      Selecting "LOCK" from the menu presented.

Not be transmitted in the clear, written down, or given to any other user of the Liberty County If the employee is leaving for the day, or at the end of the scheduled work day, the employee will log off of their computer and remain at their station to verify that the computer has successfully logged off or completely shut down before leaving work.

10.2.3 Passwords

Liberty County employees will follow the following minimum password requirements for their user account on the Liberty County network. Employees that do not follow the minimum password requirements will be suspended from accessing the Liberty County network, their workstation, and any information until the password is brought in to compliance with this policy. Passwords shall:

1. Be a minimum of (8) characters in length;
2. Be a complex password consisting of both capital and lowercase letters, numbers and at least one special character (IE. $,#,%);
3. Not be a dictionary word or proper name;
4. Not be the same as the user's active directory user name or contain the user's first or last name;
5. Be required to be changed every (90) ninety calendar days;
6. Not be the last (10) ten previously used passwords;
7. Not be transmitted in the clear, written down, or given to any other user of the Liberty County network, the Information Technology department, the user's department head or elected official.
8. Not be displayed when typed in by the user on any Liberty County computer.
9. User accounts shall be locked out for a period of no less than (30) thirty minutes following (5) five failed login attempts. Accounts shall remain locked until the thirty minutes has passed or Information Technology unlocks the users account.

Information Technology will not ask for any user's password for any reason. If Information Technology requires a user password, the user will either be asked to input the password where required or Information Technology will temporarily reset the password to accomplish a required task and will then require the user to create a new password after the task if finished.

10.2.4 Personal Identification Number (PIN CODES)

Smartphone screen locks and some computer systems may require a PIN code as a replacement for a screen lock password. PIN Codes shall:

1. Be a minimum of (6) six digits (wherever possible depending on the operating system);
2. Have no repeating digits (IE. 112233);
3. Have no sequential patterns (IE. 123456);
4. Not be the same as the user name or password;

5. Expire within 180 calendar days;
6. Not be identical to the previous (3) three PIN codes used;
7. Not be displayed when typed in by the user on any Liberty County computer (IE. It will be masked with ***** when typed).

10.2.5 Screen Savers and Screen Locks

For computers, laptops, and servers:

1. Information Technology will configure the computer, laptop, or servers operating system to automatically lock after (30) thirty minutes of inactivity and may display a screen saver once the system locks itself.
2. Users will be required to provide their password before regaining access to the computer, laptop, or server.
3. Users shall not alter or disable the screen saver or automatic screen lock in any way that prevents the system from locking itself after (30) minutes of inactivity.
4. Users may change the picture or image displayed as the screen saver provided that their doing so does not prevent the system from locking itself after (30) minutes of inactivity.

For smartphones and tablets:

1. The smartphone or tablet will be configured with a passcode set by the user before the smartphone or tablet is given to the user in the presence of Information Technology.
2. The passcode must adhere to the PIN code section of this policy (10.2.4)
3. Fingerprint and biometric authentication is required on devices that support using the user's fingerprint(s) or facial features to gain access to the device.
4. The smartphone or tablet will be set to automatically lock itself after a maximum (10) ten minutes of inactivity.
5. Users shall not make any changes to the smartphone or tablet or install any software or apps that prevent the device from locking itself after the period of inactivity set by Information Technology

10.2.6 Changing Passwords

1. Liberty County users can change their passwords any time they wish from their computer by pressing CTRL+ALT+DELETE and selecting change password from the menu presented. Passwords changed in the fashion must follow all sections of this policy.
2. Users that have been locked out of their computers because their password has expired or has been reset for any reason can call Information Technology to receive a temporary password to use to access their computer and change their password.

10.2.7 Unauthorized Use of a User's password or Active Directory Account

1. Any user that suspects, thinks, or has evidence that their password has been used by others or that their password is in some way compromised should contact the Information Technology department immediately to have their password reset.
2. Any user that suspects, thinks, or has evidence that someone has used their user account other than the user or believes their account has been compromised in any way should contact Information Technology immediately.
3. Information Technology will disable the users account and may initiate the Incident Response Plan if they find evidence that the users account has been hacked or used in a way not approved by the owner of the account.

10.2.8 System Use Notification Banner

All computers, where practical, shall display a login notification banner that reads:

"NOTICE: Access to this computer system and the Liberty County network is restricted to employees of Liberty County only. System usage while using this computer system is subject to monitoring, recording and auditing. The Georgia Computer Systems Protection Act and Federal Law prohibit unauthorized use of this system, and may be subject to criminal and/or civil penalties. Use of this computer system indicates consent to monitoring and recording of all activities."

11.0 Antivirus and Malware Prevention Policy

11.1 Purpose

The purpose of this section is to set the minimum guidelines necessary to make sure that the confidentiality, integrity, and availability of data on the Liberty County network are protected from hostile code such as malware, viruses, and worms. To do this, deployment of antivirus and malware prevention software on all systems of the Liberty County network as a mandatory standard.

11.2 Applicability

This section applies to all computing environments, networks, and computer systems owned, contracted, leased or operated by Liberty County, Liberty County appointed board or committees, and elected officials that have computer systems attached to the Liberty County network or use computers not connected to the Liberty County network to conduct Liberty County business. It may also apply to personally-owned or third party computers transmitting Liberty County sensitive data electronically or connecting directly to the Liberty County network, including any websites operated by any entity mentioned above.

This policy also applies to all users, including administrative consultants, employees, contractors, vendors, non-employees, volunteers, administrators and third parties.

11.2.1 Policy

1. The willful introduction of a computer virus, malware, and disruptive/destructive code to the Liberty County network is prohibited by this policy and applicable Georgia and Federal Laws.
2. Information Technology is responsible for deploying and maintaining approved antivirus/malware prevention software to all systems it supports, maintains and administers and providing timely updates for all components of the software on:
    a. Any externally facing servers, firewalls and gateways
    b. Proxy servers
    c. Application servers such as mail servers and/or mail gateways, FTP servers, web servers, audio/video server
    d. Data management servers such as back-up servers and database servers
    e. Liberty County deployed desktops, laptops, tablets.
    f. Cell phones, smart phones and PDA’s (when technically feasible).
    g. Non-Liberty County deployed laptops or mobile devices, to ensure that both up-to-date antivirus/malware prevention software and a personal firewall are deployed on the connection device prior to granting permission to connect to the Liberty County network.
3. Users are not to make any changes to their system that will disable or remove our approved antivirus and malware prevention software or otherwise prevent the software from performing its intended purpose.

4. Users are not to open any files, macros, or web links attached to an email from an unknown, suspicious, or untrustworthy source. All unexpected content received from a trusted source should be verified with that source prior to opening.
5. Computer systems that are unable to run antivirus and malware prevention software must be restricted to an isolated network with sufficient network-level protections deployed to prevent viruses/malware from spreading into any other areas of our network (IE running antivirus technology at its "gateway" to the Liberty County network).
6. Antivirus/malware prevention updates will be installed and scheduled to run at regular intervals or upon electronic notification of a new security update, patch, vulnerability, or threat. Wherever possible, computing resources should be set to auto-apply/update security patches on a regular basis.
7. Antivirus and malware prevention scanning should be programmed to run/initiate upon startup and/or reboot of PCs, servers and other computing devices.
8. For Pcs, servers and other computing devices that are not normally rebooted, antivirus and malware scanning should be "always on" when technically feasible. If not possible, the Information Technology department will ensure that antivirus and malware remediation is accomplished for the protection of electronic assets.
9. Information Technology is responsible for reviewing and acting upon alerts (via automated alert, email, text, news, etc.) promptly to ensure minimal exposure and security risk to the confidentiality, integrity, and availability of our electronic assets.
10. Critical security patches should be deployed by Information Technology a maximum of 48 hours after release by the operating system software or application vendor, unless there is a reason to believe the patch might negatively impact a business-related activity or application.
11. After appropriate testing, updates without issue will be made available to all PCs, servers, and computing devices, as well as, remote employees.
12. Information Technology will run malware prevention software scans routinely.
13. Information Technology will run antivirus and malware prevention software immediately after the installation of any new software, not normally supported by Information Technology (IE. Required software purchased and downloaded from the internet that is not normally used on county computers).
14. Suspicious content (files or macros attached to email) should be quarantined for review or permanently deleted immediately.
    a. Suspicious content attached to emails should not be forwarded to the Information Technology department under any circumstances.
15. All downloads should be scanned with an updated Liberty County standard antivirus/malware prevention scanner immediately (automatically, if possible).
16. Computing systems will be rebooted as required to ensure virus definitions (as well as operating system updates) are updated and that the antivirus software can run to check for viruses.
17. Information Technology default settings will be set up so that antivirus software runs upon startup or reboot.
18. Users shall not alter, remove or change settings on antivirus software to stop or prevent it from running at startup or reboot or make any change that prevents the

software from checking for updates or preforming scheduled scans of the user's computer in any way.

19. Information Technology is responsible for maintaining all firewalls and gateways on the Liberty County network, and ensuring that each device is updated with the latest software and that the devices scan all traffic in to and out of the Liberty County network for viruses and malware.
20. Users who suspect that they have received an infected file or email should immediately contact Information Technology for mitigation of the issue before continuing to work on their computer or mobile device.

12.0 Content on Liberty County Websites and Social Media Accounts Policy

12.1 Purpose

The purpose of this policy is to clearly establish guidelines for the posting and removal of user-provided information ("Content") on Liberty County internet resources ("Liberty County Sites"), which include but are not limited to message boards, blogs, social networking site, Twitter feeds, Instagram, Snapchat and websites.

12.2 Applicability

This policy applies to all users of Liberty County Sites, including administrative consultants, employees, contractors, vendors, non-employees, volunteers, interns and third parties ("Users"). It is Liberty County's expectation that the policy requirements included in this policy be implemented on both internally and externally facing Liberty County Sites to ensure appropriate use of such Sites. With respect to internally facing Sites used by Liberty County employees only, other policies may augment or supplant this policy, as applicable.

12.3 Policy

12.3.1 Creation of a Website or Social Media Account.

- Any Department, agency, board, or employee under the direct employment of the Liberty County Board of Commissioners shall get approval from the Liberty County Administrator and the Director of Information Technology before creating any website, social media account or page, Twitter account, etc.
- Departments, agencies, boards, and employees receiving permission to create a Site listed above will ensure that Information Technology receives an account that allows the department Full Administrative Access to the Site created and the Information Technology has full permissions to add, remove and edit users and content of the Site.

12.3.2 Unacceptable and prohibited Content.

- **Defamatory Content**. A defamatory statement is a false statement concerning a third party that is communicated or published to a third party and harms the party about which the statement was made. Defamatory Content is prohibited on Liberty County sites.

- **Intellectual Property Infringement**. Intellectual property is material owned by a third party that is subject to trademark, copyright or is a protected trade secret.
    - **Trademark**. Trademarks indicate a source of goods or services, and can be protected by U.S. federal or state law. Trademark use in any Content posting is prohibited without the explicit permission of the trademark owner. Additionally, trademarks shall not be used in user account names or other user identifiers. Liberty County reserves the right to delete any such accounts and require new account names without a trademark.

- **Copyright.** U.S. copyright protects original works of authorship including literary, dramatic, musical, technical (software) and other works. Content containing material subject to copyright, whether federally registered or not, shall only be used by the copyright owner. Any other use of copyrighted material in Content is prohibited.
- **Trade Secrets.** Information kept secret by an individual or organization to create a competitive advantage or maintain the value represented by such information may comprise trade secrets and can be protected by state and federal law. Content containing trade secret information is prohibited from posting by any user not authorized by the trade secret holder.

- **Privacy and Right of Publication.** Users shall not post personally identifiable information or information that would violate another's right to privacy or right of publicity.

- **Inaccurate, False, or Otherwise Unacceptable Content.** In addition to defamatory content or content that may infringe intellectual property rights, Liberty County shall remove content found to be inaccurate, false or otherwise unacceptable for posting on Liberty County sites.

12.3.3 Removal of Unacceptable Content

Liberty County shall internally and externally provide contact information on a contact page where available and how any individual, whether a User or not, may report Unacceptable Content to Liberty County. Upon becoming aware of any Unacceptable Content, Liberty County shall take steps to review and, if appropriate, remove such Content from Liberty County Sites in the timeliest manner possible. The only option available to Liberty County in dealing with Unacceptable Content is to remove such Content in its entirety. Under no circumstances shall Liberty County revise or otherwise edit Content. Where possible, Liberty County shall provide the User responsible for such posting notice of the removal and the reason for such removal. This accomplished by emailing webmaster@libertycountyga.com.

13.0 Security Awareness Training and Education Policy

13.1 Purpose

The purpose of this section is to define the security awareness training and education (SATE) program for Liberty County and to establish the minimum requirements for the program.

13.2 Applicability

This section applies to all employees, elected officials, administrative consultants, contractors, vendors, temporary personnel, non-employees, interns, volunteers and third parties, and the like. Information Technology is responsible for coordination of this training.

13.3 Scope

It is understood that, to have a successful Information Security Policy, it is necessary to train the individuals using information resources and handling sensitive information on how to protect this information and what is expected of them.

13.4 Policy

13.4.1 Types of SATE

1. General security training will be provided by Information Technology . An acknowledgement of this is signed at the end of the training. For non-employees, such as contractors, and third parties, security policies may be set by contract.
2. Application-specific security training may be given on a specific software or web-based application. It emphasizes the types of sensitive information that are accessed and processed on the specific application, as well as, important access control features to protect and handle Liberty County Sensitive Information and PII contained by the application.
3. Job-specific security training may be provided to employees who have access to Company Sensitive Information and PII.
4. Information response security training for Information Technology professionals shall provide Information Technology personnel the appropriate education to know how to react to a possible incident or prevent a threat from becoming an incident. This training helps reduce risk through appropriate training as first responders.
5. Web-based security training (e.g., security videos and security briefings/presentations on the web) shall be utilized to provide security awareness on handling, transmitting and storing sensitive information.
6. Security reminders, such as emails, newsletters, articles, postings will be provided on a regular basis.

7. Security awareness briefings will be done at least annually by the Information Technology director.

13.4.3 SATE General Training Elements

1. A summary of the County's information security policies must be delivered to all employees, contractors, or third parties with access to PII and Liberty County Sensitive Information. A summary of information on these security policies, to the extent applicable, will be provided to Liberty County contractors.
2. The SATE program will include acceptable use training on PII and Liberty County Sensitive Information.
3. The SATE program will include physical security policies and procedures.
4. The SATE program will include general information security training such as log-on/off procedures, how to initiate a locked screen saver, password management, and other procedures for safeguarding against malicious software or threats.
5. The SATE program will include how to recognize and report a potential security incident or threat to the Liberty County Network.
6. The SATE program will provide updates on new or changes to security policies and procedures.

13.4.3 SATE training Course Plan

- Goal
- Scope
- Training participants (e.g., employees, consultants and contractors)
- Approach (i.e., train the trainer or train the end users)
- Methodology (i.e., face-to-face, web-based, audio, self-study)
- Deliverables (i.e., training plan, instructor's manual, video track, PowerPoint)
- Training Objectives
- Schedule
- Certification or Acknowledgement
- Course Review and Evaluation

Security training documentation shall be maintained through certificates or training or attendance rosters.

14.0 Incident Response Plan

14.1 Purpose

The purpose of this Incident Response Plan ("IRP") is to provide guidance on the appropriate steps to be taken in the event of a possible security incident or data breach, from the time of the suspected breach to the post-incident response closure, so that all incidents are handled in a consistent manner and the exposure to the potentially breached party is limited. It also provides a methodology for collecting evidence in the event of criminal activity. Documentation of response actions taken in connection with any security incident or data breach, as well as, documentation of the post-incident events and actions taken, is critical in making appropriate changes to business practices to improve the safeguarding and handling of Liberty County Sensitive Information and PII.

14.2 Applicability

This IRP process applies to all employees, elected officials, administrative consultants, temporary personnel, non-employees, interns, volunteers and the like who may experience or witness a security incident or possible data breach. After discovery, this process provides Information Technology with a checklist or outline for responding so that steps or information related to the incident are not missed. Liberty County is committed to protecting information and responding appropriately to a security incident or breach.

14.3 Scope

Protection of information and data is paramount. This IRP provides a checklist for responding to a security incident or potential data breach. An incident can be intentional or unintentional, and this IRP could be implemented in response to many events having an adverse effect on the Liberty County network.

14.4 Guidelines

This IRP describes safeguards to protect sensitive information, including PII. These safeguards are provided to:

- Protect the confidentiality, integrity and availability of data and the Liberty County network;
- Protect against a data breach that sound result in harm or inconvenience to a citizen or employee and meet any notification requirements that are required by Georgia Law;
- Protect against anticipated threats or hazards to the security and integrity of sensitive information including PII;
- Identify and assess the risk that may threaten PII;
- Conduct a responsible investigation to determine the likelihood of information that has been or will be misused;
- Conduct a post-incident investigation to capture lessons learned;

- Develop written policies and procedures to manage and control these identified risks or vulnerabilities;
- Adjust the Information Security Policy and program to reflect changes in technology, the sensitivity of data stored, and internal or external threats to Information Security.

The IRP will be tested annually by the Director of Information Technology to ensure all participants on the Incident Response Team ("IRT") know their roles in the event of an actual incident.

14.5 Process

1. Incident Response Process – Initial Discovery

a. Anyone suspecting or noting a security incident, data breach, potential system compromise, or malicious activity, must contact Information Technology and their supervisor and/or department head immediately.
b. Once reported, Information Technology will distribute Security Incident Reporting forms (**see *appendix A)*** to all involved parties to begin collecting information about the incident. Each party involved must complete as much information on this form as possible and MUST provide a narrative of what they saw or perceived to have happened.
c. Information Technology, working with the department in which the incident occurred, will determine if there has been a security incident and the nature and seriousness of the incident, by considering the following questions and discussing them with all involved parties.
    i. Does the system contain Liberty County Sensitive Information or PII?
    ii. Is there a chance outside law enforcement may need to get involved?
    iii. Is there a requirement or desire to perform a forensics analysis of the system compromise?
    iv. Are any funds or money stolen or missing?
    v. If the answer is "YES" to any of the above questions the Director of Information Technology shall contact the County Administrator to inform him/her of the security incident and they will determine the best way to proceed forward with the incident, which could include one or all of the following:
        1. Contact law enforcement (local, state or federal);
        2. Contact the County Attorney;
        3. Contact the County Cyber Security Insurance Agency;
        4. Contact the County's insurance carrier;
        5. Establish an Incident Response Team (IRT) to mitigate the incident.
    vi. Do preliminary analysis by isolation of the compromised system by disconnection of the network cable. If this is not feasible or desirable, Information Technology shall block access to the compromised system via the network.

d. Determine the security incident type by trying to determine the cause of the malicious activity and the level of system privileges attained by the intruder and implement appropriate remedial measures.
e. If a system is compromised:
    i. Disable any compromised account and terminate all processes owned by them.
    ii. Compile a list of IP addresses involved in the incident, including log entries if possible.
    iii. Determine if users need to change their passwords due to the compromise, as well as, whether or not they have accounts on other systems using the same credentials and initiate the password change.
    iv. Verify users have changed their passwords and encourage them to change personal passwords on other systems as a precaution to protect their personal information.
    v. Information Technology will perform a network vulnerability scan of the network and any other systems involved in the incident.

2. Security Incident After Action Review

a. Hold a meeting of the IRT within 48 hours of completion of the response.
b. Review chronology of the event.
c. Identify what went wrong and what went right. What measures or policies worked and didn't work.
d. Identify the threat or vulnerabilities that were exploited and determine whether it/they can be alleviated.
e. Review if intrusion detection or prevention was in place, and if it was active and up-to-date
f. Document After Action Review and request appropriate updates to the Information Security Policy and program as needed to the Liberty County Information Technology Authority.

15.0 Compliance

Violations of this policy may lead to the suspension of system privileges and/or disciplinary action up to and including termination of employment. Liberty County reserves the right to advise appropriate authorities of any violation of law.

16.0 Accountability

All users are accountable for reporting any suspected data breach for the Liberty County network to Information Technology.

Information Technology is responsible for ensuring compliance with all sections of this policy and the controls created to safeguard the Liberty County network.

The Liberty County Information Technology Authority is responsible for maintaining updates to this policy at least annually.

The Liberty County Cyber Security Insurance provider, their counsel, and the County Attorney are responsible for documenting the types of personal information that may have been breached, providing guidance throughout the investigation on privacy issues, and assist in developing the communications plan to impacted individuals.

17.0 Exceptions

Any exceptions to this policy must be approved at the Departmental level following review Liberty County Information Technology.

Appendix A – Liberty County Security Incident Reporting Form

Instructions: Please use the following form to document relevant security incident information as soon as the incident is reported or discovered. Please send via the most secure way possible the completed form to the contact listed below.

All information on this completed form is confidential and should not be discussed with anyone while the security incident is being investigated.

Please submit* completed form to: clint.stanley@libertycountyga.com
Clint Stanley
Liberty County IT
100-A Liberty St
Hinesville, GA 31313

Incident Case Information *(To be completed by IT Department)*	
Incident #:	Ticket #:

1. Contact Information	
Full name:	
Job title:	
Department:	
Division or office:	
Work phone:	
Mobile phone:	
E-mail address:	
Fax number:	
Additional contact information:	

2. Type of Incident *(Check all that apply)*	
☐ Account compromise *(e.g., lost password)*	☐ Social engineering *(e.g., phishing, scams)*
☐ Denial of service *(including distributed)*	☐ Technical vulnerability *(e.g., 0-day attacks)*
☐ Malicious code *(e.g., virus, worm, Trojan)*	☐ Theft/loss of equipment or media
☐ Misuse of systems *(e.g., acceptable use)*	☐ Unauthorized access *(e.g., systems, devices)*
☐ Reconnaissance *(e.g., scanning, probing)*	☐ Unknown/Other *(Please describe below)*
Description of incident:	

3. Scope of Incident *(Check one)*	
☐ Critical *(e.g., affects public safety or county-wide information resources)* ☐ High *(e.g., affects department's entire network or critical business or mission systems)* ☐ Medium *(e.g., affects department's network infrastructure, servers, or admin accounts)* ☐ Low *(e.g., affects department's workstations or user accounts only)* ☐ Unknown/Other *(Please describe below)*	
Estimated quantity of systems affected:	
Estimated quantity of users affected:	
Third-parties involved or affected: *(e.g., vendors, contractors, partners)*	
Additional scope information:	

4. Impact of Incident *(Check all that apply)*	
☐ Loss of access to services ☐ Loss of productivity ☐ Loss of reputation ☐ Loss of revenue	☐ Propagation to other networks ☐ Unauthorized disclosure of data/information ☐ Unauthorized modification of data/information ☐ Unknown/Other *(Please describe below)*
Estimated total cost incurred: *(e.g., cost to contain incident, restore systems, notify data owners)*	
Additional impact information:	

5. Sensitivity of Affected Data/Information *(Check all that apply)*	
☐ Confidential/Sensitive data/info ☐ Non-sensitive data/info ☐ Publicly available data/info ☐ Financial data/info	☐ Personally identifiable information (PII) ☐ Intellectual property/copyrighted data/info ☐ Critical infrastructure/Key resources ☐ Unknown/Other *(Please describe below)*
Quantity of data/information affected: *(e.g., file sizes, number of records)*	
Additional affected data information:	

6. Systems Affected by Incident*(Provide as much detail as possible)*	
Attack sources *(e.g., IP address, port)*:	
Attack destinations *(e.g., IP address, port)*:	
IP addresses of affected systems:	

Domain names of affected systems:	
Primary functions of affected systems: *(e.g., web server, domain controller)*	
Operating systems of affected systems: *(e.g., version, service pack, configuration)*	
Patch level of affected systems: *(e.g., latest patches loaded, hotfixes)*	
Security software loaded on affect systems: *(e.g., anti-virus, anti-spyware, firewall, versions, date of latest definitions)*	
Physical location of affected systems: *(e.g., state, city, building, room, desk)*	
Additional system details:	

7. Users Affected by Incident *(Provide as much detail as possible)*	
Names and job titles of affected users:	
System access levels or rights of affected users: *(e.g., regular user, domain administrator, root)*	
Additional user details:	

8. Timeline of Incident *(Provide as much detail as possible)*	
a. Date and time when Agency first detected, discovered, or was notified about the incident:	
b. Date and time when the actual incident occurred: *(estimation if exact date and time unknown)*	
c. Date and time when the incident was contained, or when all affected systems or functions were restored: *(use whichever date and time is later)*	
Elapsed time between the incident and discovery: *(e.g., difference between a. and b. above)*	
Elapsed time between the discovery and restoration: *(e.g., difference between a. and c. above)*	
Detailed incident timeline:	

9. Remediation of Incident *(Provide as much detail as possible)*	
Actions taken by Department to identify affected resources:	
Actions taken by Department to remediate incident:	
Actions planned by Department to prevent similar incidents:	
Additional remediation details:	

10. Incident Narrative *(Provide a narrative of the incident, use additional sheets if needed.)*
Incident Narrative:

Signature of person submitting Security Incident Report:

_____ _____

Signature *Date*

_____ _____

Printed Name *Title*

***PLEASE NOTE: All Security Incident Reporting Forms and accompanying documentation must be transmitted to IT in a safe and secure manner.**

Appendix B – Liberty County Hand Receipt

Liberty County
Information Technology
Hand Receipt Form

Department_____ **Date**

Issued _____

Name of Employee _____

Item(s) being issued:

_____
_____
_____
_____
_____

You have been issued Liberty County Information Technology equipment to aid in your job duties and assume full responsibility for said equipment from the date of delivery until returned as provided below. In the event the equipment is lost or stolen, it must be reported to the Information Technology Department immediately. This equipment is to be used as part of your job as a Liberty County employee only and must be surrendered, in good condition, upon termination or resignation of your employment and/or position, or upon the request of Liberty County, Georgia. This equipment should only be used by the employee it is issued to and not loaned or used by any non-employees, family, friends, or other unauthorized persons. Failure to return or properly account for the equipment as provided above in good condition will result in charges for a replacement, for which you will be liable.

By furnishing the equipment, neither Liberty County, Georgia nor the Liberty County Information Technology makes any warranties of any kind regarding the equipment, and any warranties, either express or implied, are hereby expressly disclaimed; it being understood and agreed that the equipment is made available and accepted "as is," where is," and "with all faults," in whatever condition it may be, without any guarantee or representation as to any matter whatsoever respecting the Equipment. **WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, LIBERTY COUNTY, GEORGIA AND THE LIBERTY COUNTY INFORMATION TECHNOLOGY EXPRESSLY DISCLAIM ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS OR ADEQUACY FOR ANY PARTICULAR PURPOSE OR USE, AND FURTHERMORE MAKE NO WARRANTY OR REPRESENTATION ABOUT THE PERFORMANCE, QUALITY, OR OPERATION OF SAID EQUIPMENT, OR ABOUT ITS PRESENT STATE OF REPAIR, CONDITION, OR MAINTENANCE.**

_____ _____
Employee's Signature **Issuer's Signature**

Date Returned_____ **Received by**_____

Appendix C – Liberty County Information Security & Usage Policy - Highlights

Liberty County Information systems collect, manage and store sensitive information on a regular basis to support County business is committed to preserving the confidentiality, integrity, and availability of its information resources.

The Liberty County Information Security and Usage Policy applies to all employees, elected officials, consultants, contractors, vendors and volunteers (Users) who receive create, store, handle or transmit Liberty County information in hard copy or electronic format. It is the responsibility of the user to read the full Liberty County Information Security and Usage Policy as condition of continued use of the Liberty County Information systems and the Liberty County Network.

Information Security

- Information Technology is responsible for Information Security and the Information Security Program;
- Users should have no reasonable expectation of privacy when using any computers, electronic devices or the Liberty County Network;
- Users are responsible for keeping Liberty County sensitive information and Personally Identifiable Information safe, secure and stored. Such information will only be transmitted to persons authorized to receive such information. Any information containing dates of birth or social security numbers must be sent encrypted;
- All mobile devices such as Laptops, iPhones, iPads, radios and any type of smart phones contain information as a computer and will be secured and handled like a computer when in use by a user or employee.
- Information Technology is responsible for issuing and maintain all computers, laptops, iPhones, iPads, radios and any type of smart phones. Also for maintaining the Liberty County network;
- Users are responsible for ensuring that all issued mobile devices are cared for and remain in like new condition;
- Access to any Liberty County computer system and the Liberty County network is restricted to Liberty County authorized users only;
- System usage, including email, is subject to monitoring, recording and auditing by Information Technology, and may be done so with or without notice;
- Any information that is transmitted through any means electronically that has sensitive personal information such as but not limited to date of birth or social security numbers will be sent through encrypted means.

Network User Account Security

- Users are issued a user name, password, and email address; they are responsible for the security of their accounts;
- Passwords must be changed **EVERY ninety (90) days** and must be complex, and at least 8 characters in length;
- Passwords cannot be changed to the last ten (10) passwords previously used;
- Users must lock or log off their computers when they leave their desk or office for extended periods of time and when they leave work at the end of the day they must shut down their computers;
- Users WILL NEVER share their passwords with anyone including their department head, supervisor, elected official, or Information Technology;
- All iPhones, iPads, Android devices, smart phones, and laptops MUST be secured with a pin code or password and all information will be encrypted whenever possible;
- Users will never alter, change or disable any virus protection or monitoring software installed on any Liberty County device for any reason

Security Incident Reporting and Response

- Users are responsible for reporting any suspected or observed security incident, data breach, systems compromise, or malicious activity to Information Technology as soon as it is suspected or observed;
- Users are required to document any suspicious or observances in writing as part of a security incident investigation;
- Information Technology will investigate any breach of our technology systems.

Security Awareness Training

- Users are required to attend Security Awareness and Education Training Classes.

Compliance

- Violations of the Liberty County Information Security and Usage Policy may lead to the suspension of system privileges and / or disciplinary action up to and including termination;
- Liberty County reserves the right to advise appropriate authorities of any violation of law.

Social Media

- All information transmitted that contains personnel information, SSN, or date of birth will be sent encrypted
- No department, or employee of Liberty County will open a social media account for the sole purpose of posting county / work related information without permission from the Information Technology;
- All departments that have a social media account will provide Information technology with information to edit, and have full administration rights to the social media site;
- All content is considered Open Records accountable.

Exceptions

- Any exception to the Liberty County Information Security and Usage Policy must be approved by the Liberty County Information Technology.

User Consent and Agreement

I the undersigned user have read the Liberty County Information Security and Usage Policy highlights presented above, and understand that it is my responsibility to fully read the entire Liberty County Information Security and Usage Policy as a condition of my continued use of Liberty County Information Systems. The Liberty County Network and any Liberty County mobile device, and that I do agree to comply with all the terms and conditions of the policy.

I agree that all network activity conducted while doing business on behalf of Liberty County and being conducted with Liberty County resources is the property of Liberty County, Georgia. I understand that the Liberty County Information Technology Department reserves the right to monitor, record, and log all network activity, including email, with or with notice, and therefore I have no expectations of privacy in the use of these resources.

User's Full Name: _____Department: _____

Supervisor/HR: _____Date: _____SSN (last 4): _____

Signed: _____Date: _____