WINTER HAVEN POLICE DEPARTMENT

GENERAL ORDER 82.4

Information Technology Security

ACCREDITATION STANDARDS: N/A

EFFECTIVE DATE: September 12, 2013

RESCINDS: G.O. 82.4, November 21, 2018 and all applicable Amended/Temporary Orders prior to December 10, 2019

LAST REVISED DATE: December 10, 2019

This General Order contains the following numbered sections:

CONTENTS

POLICY

It shall be the policy of the Winter Haven Police Department (Department) and the City of Winter Haven Technology Services Department (IT) to ensure that sensitive information is secure and is in compliance with the Federal Bureau of Investigation (FBI) Criminal Justice Information Services Security Policy.

PURPOSE

The purpose of this General Order is to provide security measures that shall ensure sensitive information maintained or processed by the Department and IT is protected, and to establish uniform guidelines and accountability for the utilization of the information systems.

SCOPE

This General Order shall apply to all members of the Department and Technology Services.

DISCUSSION

This General Order applies to all computer systems (including those that are dedicated elements, subsystems, components of more extensive systems, or mobile/remote systems), regardless of the manner in which the systems were acquired. The mobile laptop computer communicates by using wireless network technology to transmit data from a mobile unit to the secure City of Winter Haven and Polk County Sheriff's Office network. Wireless network technologies allow for instant transmission of data through the cellular or wireless switching stations and provides mobile units with remote access to all City of Winter Haven information services.

PROCEDURE

I. Security

A. The security policies and procedures provided in this General Order shall be required to protect sensitive information, which includes criminal justice information and personally identifiable information (as defined in the FBI Criminal Justice Information Services Security Policy). Personally identifiable information extracted from criminal justice information shall only be used for official business. This General Order shall adhere to Florida State Statute 815, which pertains to computer-related crimes and to the FBI Criminal Justice Information Services Security Policy.

B. The IT Department Director shall be tasked with the planning, economics, and management of the Department's information technology security program and establishing related procedures. The IT Department Director shall:

1. Provide for the development, coordination, dissemination, and maintenance of Department's objectives, concepts, policies, procedures, and standards for managing information technology security; and

2. Provide for, or assist with, the development, coordination, maintenance, and implementation of information technology security documents related to:

a. Administrative procedures and members;

b. Physical and virtual environments;

c. Network and other communications mediums;

d. Hardware and software; and

e. Special testing/evaluation.

C. The internal security is the responsibility of the IT Department Director, who shall appoint an Information Technology Security Officer. The Information Technology Security Officer shall be the designated Local Agency Security Officer. The Information Technology Security Officer shall provide the IT Department Director with the information and assistance required to:

1. Establish and document specific information technology security requirements;

2. Create new and improved policies, techniques, and procedures as needed to fulfill information technology security requirements;

3. Develop practical guidelines that can be easily understood and used to economically protect sensitive information at the level required;

4. Establish an information technology security test and evaluation policy, procedures, and techniques, including a test and evaluation program;

5. Investigate any reported security incidents;

6. Provide after hours support for the Department's data center facilities;

7. Identify who is using the Criminal Justice Information Services Systems Agency approved hardware, software, and firmware, and ensure no unauthorized individuals or processes have access to the same;

8. Identify and document how the equipment is connected to the state system;

9. Along with the Department's Terminal Agency Coordinator Ensure that personnel security screening procedures are being followed as stated in this policy;

10. Ensure the approved and appropriate security measures are in place and working as expected; and

11. Support policy compliance and ensure the Criminal Justice Information Services System Agency Information Security Officer is promptly informed of security incidents.

D. All authorized Department and IT members shall be responsible for carrying out these information technology security policies and procedures including:

1. Safeguarding sensitive information in their custody;

2. Making sure members who receive sensitive information are authorized members who have proper need and access; and

3. Informing users of published security policies and procedures.

E. Only Department/City-issued information systems (laptops, workstations, servers, portable devices, tablets, smartphones, etc.) that meet the information technology security standards shall be authorized to access the secure City network.

F. Personally owned information systems/devices (smartphones, tablets, etc.) shall not be authorized for accessing, processing, storing, or transmitting sensitive agency information and shall not be allowed to access the secure City network. Personally owned information systems/devices shall be authorized to access City

e-mail only to view, create, and respond to e-mails containing non-sensitive information. Precautions shall be taken to prevent unauthorized access to personally owned devices with access to City e-mail.

G. The Department shall follow the secure password attributes listed to authenticate a member's unique identification. A member's password shall:

1. Be a minimum length of eight (8) characters on all systems;

2. Not be a dictionary word or proper name;

3. Not be the same as the user identification;

4. Expire within a maximum of ninety (90) calendar days;

5. Not be identical to the previous ten (10) passwords;

6. Not be transmitted in the clear (unencrypted) outside the secure location; and

7. Not be displayed when entered.

H. If a Department member forgets their password, they shall contact the Information Technology Security Officer to reset their password.

I. Passwords shall not be saved on any computer (desktop or laptop).

J. The information system shall prevent further access to the system by initiating a session lock after a maximum of thirty (30) minutes of inactivity. The session lock shall remain in effect until the user reestablishes access to the system using appropriate identification and authentication sign-on procedures.

K. Any City of Winter Haven computer that can access CJIS information and is not in a secure facility as specified in CJIS Security Policy shall have advanced authentication in accordance with CJIS Security Policy.

1. All City of Winter Haven laptop computers shall have advanced authentication in accordance with CJIS Security Policy.

II. Terminal Agency Coordinator

A. The Terminal Access Coordinator serves as the point of contact at the Department for matters relating to Criminal Justice Information Services information access.

B. The Terminal Agency Coordinator administers Criminal Justice Information Services systems programs within the Department and oversees the Department's compliance with Criminal Justice Information Services systems policies.

III. Personnel Screening for Contractors and Vendors

A. Support personnel, contractors, and vendors with access to physically secure locations or controlled areas (during criminal justice information processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

B. The Terminal Agency Coordinator shall ensure background investigations are completed on all facility contractors/vendors/workers, in accordance with the Federal Bureau of Investigation Criminal Justice Information Services Security Policy, prior to being issued a facility access card or being allowed on facility premises unescorted. This shall be accomplished by:

1. A state of residency and national fingerprint-based record check/computerized criminal history check.

C. Contractors and vendors shall meet the following requirements:

1. Prior to granting access to criminal justice information and/or the facility, the contracting government agency on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint-based record check.

2. If a record of any kind is found, the contracting government agency shall be formally notified and system access shall be delayed pending review of the criminal history record information. The contracting government agency shall, in turn, notify the contractor-appointed security officer.

3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the contracting government agency or the criminal justice agency (if the contracting government agency does not have the authority to view criminal history record information) shall review the matter.

4. A contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified from access.

5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.

6. The contracting government agency shall maintain a list of personnel who have been authorized access to criminal justice information and shall, upon request, provide a current copy of the access list to the Criminal Justice Information Services systems officer.

7. Applicants with a record of misdemeanor offense(s) may be granted access to criminal justice information if the Chief of Police determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification.

8. The contracting government agency may request the Criminal Justice Information Services systems officer to review a denial of access determination.

IV. Information Technology Users

A. All members shall be responsible for:

1. Protecting sensitive information and information systems received at their functional area;

2. Protecting devices located in their respective areas that are used to input and output sensitive information or which are connected to the secure City network when it is processing sensitive information;

3. Returning any unexpected or unrecognizable output products to the Information Terminal Agency Coordinator. If any unexpected or unrecognizable data is inadvertently displayed on a monitor or printed from a copier/printer, this fact shall be reported to the Terminal Agency Coordinator; and

4. Reporting all security incidents to the Information Technology Security Officer.

5. Members shall be responsible for the proper usage of the Department-issued mobile laptop computers and the accountability of all associated accessories assigned to them.

6. Routine National Crime Information Center/Florida Crime Information Center (NCIC/FCIC) inquiries shall be conducted by the member using their mobile laptop computer, unless officer safety is an issue.

7. All NCIC/FCIC queries that indicate a positive hit, such as wanted person, stolen article, domestic violence, or missing person, should be confirmed to assure the proper interpretation of the hit is valid and confirmed through NCIC/FCIC procedures. A member shall not take action solely on the information obtained through the mobile laptop computer until it is confirmed by the Crime Information Center.

V. Accessing and/or Processing Sensitive Information

A. Each user's identity shall be positively established. A user's access to the system, as well as activity in the system (including material accessed and actions taken), shall be controlled and open to scrutiny. This requirement is, as a rule, met by applying a combination of administrative procedures and hardware and software controls. When an automated audit trail is available, data should be collected on accesses made to files; how and from where such accesses were initiated; the identity of the person or process initiating the access; and a record of all unauthorized access attempts. System access controls shall be in place and operational to prevent multiple concurrent active sessions for one (1) user identification, for those applications accessing criminal justice information. System access controls shall ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and add, remove, or alter programs.

B. Measures shall be taken to make sure that the Technology Services Department is externally protected against unauthorized access to the City's data center

facilities, unauthorized access to the system from remote terminals, and unauthorized access to electronic media.

C. All Technology Services Department components shall operate so that system hardware and software malfunctions are automatically or administratively detected and reported in time to detect or prevent unauthorized disclosure.

D. Each database, file, or data set shall have an identifiable origin and use, and an explicitly defined set of access controls based on sensitivity, user identity, and established need-to-know. The system shall function so that each user has access to only the information to which they are entitled.

E. As required by the FBI Criminal Justice Information Services Security Policy, information systems with access to criminal justice information outside of physical secure locations shall be secured utilizing advanced authentication methods.

F. It shall be the responsibility of all members to ensure the protection of sensitive information from unauthorized disclosure, alteration, or misuse.

G. The Technology Services Department shall restrict access to wireless networks to allow only authorized agency-issued information systems/devices access to the secure City network. The wireless network systems shall control authorization, access, and monitoring of the use of wireless networks that access the secure City network. Specific methods for securing the wireless network shall be part of the information security plan and shall comply with the FBI Criminal Justice Information Services Security Policy. The Technology Services Department shall ensure that a monthly review of the wireless networks is completed.

H. The Technology Services Department shall authorize, monitor, and control all methods of remote access to the secure City's network and the information systems. The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The Technology Services Department shall control access through managed access control points. Remote access for vendors shall only be authorized for compelling operational needs and the rationale for such access shall be documented in the information security plan for the information system.

I. The Chief Information Officer shall be responsible for the development of a comprehensive information security plan to protect the secure City network and all information systems that access the secure City network and its information. The information security plan shall be considered confidential and exempt from disclosure pursuant to Florida State Statute 119.071(3)(a).

VI. Computer Hardware and Software

A. Purchase of any hardware or software shall be in accordance with the City's purchasing policy.

B. The City and the Department purchases and licenses the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Unless authorized by the software

developer, the City does not have the right to reproduce such software for use on more than one computer.

C. Members may only use software on local area networks or on multiple machines according to the software license agreement. The Department prohibits the illegal duplication of software and its related documentation.

D. The Information Technology Department (IT) is responsible for the installation of software on Department computers. IT may authorize selected members to assist in the installation of computer software.

E. All computer software must be inspected for viruses prior to installation on any Department computer.

1. The Technology Services Department shall ensure each Department computer is protected against unauthorized external/internal access and equipped with an anti-virus program.

F. Only computer software that is related to Department business or operations shall be installed on any Department computer.

VII. Back-Up, Storage, Security, and Use of Central Records Computer Files:

A. The Technology Services Department shall complete a full backup of the data center files on a routine basis

B. All back-up data shall be maintained at a secure off-site location.

C. The security of all back-up data shall be restricted for use by the Information Technology Department as needed for restoring the information system.

D. The Chief Information Officer shall be responsible for authorizing the disposal/destruction of any back-up data and/or media. The back-up data and/or media shall be disposed of in a manner to ensure the information cannot be replicated by any unauthorized persons. A written log shall be maintained by the IT Network Supervisor to record the date and time of any back-up data and/or media destruction.

VIII. Computerized Criminal History Records:

A. User profiles and passwords shall be required to access the City's data center NCIC, and FCIC.

B. Routine criminal history inquiries shall only be accomplished by those agency members who are NCIC/FCIC certified.

C. All criminal history requests shall be completed in accordance with NCIC/FCIC instructions. The receipt and dissemination of criminal history information from the City's data center shall be governed by the NCIC/FCIC regulations, Florida Public Records Statutes, and the FBI Criminal Justice Information Services Security Policy.

D. The receipt and dissemination of criminal history information from the NCIC/FCIC information systems shall only be for law enforcement purposes and shall only be released to other criminal justice agencies except as delineated in this General Order. Criminal history information released to another criminal justice agency, verbally or physically, shall be documented on a Computerized Criminal History Secondary Dissemination log, retained for six (6) years, and be available for review by NCIC and/or FCIC auditors.

E. Criminal history record information shall only be used for the purpose for which it was originally obtained. When criminal history record information is no longer useful, it shall be shredded and shall not be retained in case files.

F. The destruction of NCIC/FCIC documents shall be governed by the Florida Public Records Statutes and NCIC/FCIC regulations.

G. NCIC/FCIC Certified Members:

1. Members shall not use or disseminate any information generated by NCIC/FCIC, except as provided by the NCIC/FCIC Manuals and Florida Statutes.

2. For specific instructions regarding the entry/inquiry of information from the NCIC or the FCIC, refer to the NCIC/FCIC Manuals which are available to members via the Florida Criminal Justice Network (CJNET).

IX. Incident Response

A. The Chief Information Officer and the Information Technology Security Officer shall respond to suspected computer security incidents by identifying and controlling the incidents and immediately reporting the findings to the Chief of Police or their designee.

1. The Chief of Police may assign a Department member to assist in the investigation of a security incident.

B. The Department's computer security incident response process shall include notification procedures to be followed for incidents where the investigation determines non-encrypted personal information was, or is reasonably believed to have been, accessed by an unauthorized person, as required by Florida State Statute 817.5681.

C. The Chief Information Officer or Information Technology Security Officer shall determine the appropriate response required for each suspected computer security incident.

D. Department members shall notify their supervisor of computer security incidents, including suspected or confirmed breaches, immediately upon discovery. The supervisor shall notify their bureau commander, the Chief Information Officer or Information Technology Security Officer of computer security incidents, including suspected or confirmed breaches, immediately upon discovery. The bureau commander shall immediately notify the Chief of Police of each suspected computer security incident. Each suspected computer security incident, including findings and corrective actions, shall be documented in writing and

maintained for a minimum of three (3) years or until legal action (if warranted) is complete. These documented findings shall be considered confidential and exempt from disclosure pursuant to Florida State Statute 119.071(3)(a).

E. The Information Technology Security Officer or Terminal Agency Coordinator shall be responsible for the prompt reporting of a computer security incident to the Florida Department of Law Enforcement (FDLE) Criminal Justice Information Services Information Security Officer, the FDLE Customer Support Center, or the FDLE Network Administrator, in accordance with the FBI Criminal Justice Information Services Security Policy.

F. Members shall report loss of mobile devices immediately, according to agency reporting procedures.

G. Members shall immediately report lost security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes, according to agency reporting procedures.

H. The method(s) and area(s) of storage for policies and procedures applicable to maintaining the Department/City's security system shall be considered confidential and exempt from disclosure pursuant to Florida State Statute 119.071 (3)(a).

X. Security Alerts and Advisories

A. The Information Technology Security Officer shall:

1. Receive information system security alerts/advisories on a regular basis.

2. Issue alerts/advisories to appropriate members.

3. Document the types of actions to be taken in response to security alerts/advisories.

4. Take appropriate actions in response, for all devices on the secure City network.

XI. Electronic and Physical Media Protection

A. The City shall take measures to ensure that all electronic and physical media is properly protected at all times.

B. The City shall securely store electronic and physical media within physically secure locations or controlled areas. The City shall restrict access to electronic and physical media to authorized members. If physical and personnel restrictions are not feasible then the data shall be encrypted using City approved data encryption methods.

C. The City shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

1. Electronic Media in Transport: Controls shall be in place to protect electronic media containing sensitive information while in transport (physically moved from one location to another) to prevent data from being comprised.

2. Physical Media in Transport: The controls and security measures shall also apply to sensitive information in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

D. The City shall sanitize (overwrite at least three (3) times), or destroy electronic media by physical means prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed. Members shall ensure the sanitization or destruction of electronic or physical media containing sensitive information is either witnessed by authorized members or carried out by authorized members.

E. Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information being compromised by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

XII. Data Encryption

A. Encryption shall be a minimum of one hundred twenty-eight (128) bit.

B. When sensitive information is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).

C. When sensitive information is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).

D. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

XIII. Software Patch Management

A. The City shall identify applications, services, and information systems containing software or components affected by software flaws and potential vulnerabilities when they are announced by software vendors.

B. The City (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall ensure prompt installation of newly released security relevant patches, service packs and hot fixes.

C. The City's patch management strategy shall include:

1. Testing of appropriate patches before installation;

2. Rollback capabilities when installing patches, updates, etc;

3. Automatic updates without individual user intervention; and

4. Centralized patch management.

D. Patch requirements discovered during security assessments, continuous monitoring, or incident response activities shall also be addressed expeditiously and be included in the information security plan.

XIV. Violations of Information Technology Security Requirements

A. Any violation of the security requirements (e.g. use of information for non-law enforcement purposes, dissemination of information, etc) of this General Order, NCIC/FCIC, FBI Criminal Justice Information Services Security Policy or other secure data resources shall be a Group III Offense as outlined in General Order 26.1

1. A Group III Offense is punishable by up to termination on the first offense.

2. Disciplinary procedures outlined in General Order 26.1 shall be followed.

B. Investigations of violations or suspected violations of security requirements shall be assigned by the Chief of Police.

1. Violations or suspected violations of a non-criminal nature shall be in accordance with General Order 52.1.

2. Violations or suspected violations of a criminal nature shall be in accordance with General Order 42.1.

XV. Definitions

A. *Access* – The ability of a user to communicate with (input to or receive output from) the Technology Services Department or have entry to a specified area. This definition does not include those persons (customers) who simply receive products created by the system and who have no communication or interface with the Technology Services Department or its members.

B. *Advanced Authentication* – Verification of a user's identity utilizing two (2) or more authentication methods, i.e., Username/Password, Biometrics (fingerprint, iris scan), Proximity Card, Secure Tokens, etc.

C. *Application Software (functional)* – Those routines and programs designed by or for the Technology Services Department users and customers to complete specific, mission-oriented tasks, jobs, or functions, using available Technology Services Department equipment and basic software. Application software may be either general purpose packages, such as demand-deposit accounting, payroll, etc., or specific application programs tailored to complete a single or limited number of user functions. Except for general purpose packages acquired directly from software vendors or from the original equipment manufacturers

(OEM), this type of software is generally developed by the user, either with in-house resources or through contract services.

D. *Basic Software (nonfunctional)* – Those routines and programs designed to extend or facilitate the use of particular Technology Services Department equipment. As a rule, the Technology Services Department vendor provides this software which is usually essential for the systems' operation. Examples of basic software are executives and operating systems, diagnostic programs, compilers, assemblers, utility routines such as sort, merge and input or output conversion routines, file management programs, and data management programs. Data management programs are commonly linked to, or under the control of, the executive or operating system programs.

E. *Computer* – Any internally programmed automatic device that performs data processing.

F. *Computer Network* – A set of related, remotely connected devices and communication facilities including more than one (1) computer system with capability to transmit data among them through communication facilities.

G. *Computer Program* – An ordered set of data representing coded instructions or statements which, when executed by a computer, cause the computer to process data.

H. *Computer Software* – A set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

I. *Contained* – Refers to a state of being within limits, as within system bounds, regardless of purpose or functions, and includes any state of storage, use, or processing.

J. *Controlled Access* – The process of limiting access to the resources of an information technology system only to authorized members, users, programs, processes, or other information technology systems (as in computer networks).

K. *Controlled Area* – An environment, considered in part or as a whole, where all types and aspects of access are checked and controlled.

L. *Criminal Justice Information* – The abstract term used to refer to all of the FBI Criminal Justice Information Services provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property, and case/incident history data. In addition, criminal justice information refers to the FBI Criminal Justice Information Services provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions.

M. *Data Center Facilities* – One (1) or more information systems with their peripherals and communications equipment located in a single area. This does not include remote terminal equipment located outside the single area, even though such equipment may be electrically connected to the data center facilities.

N. *Dedicated Security Mode* – A mode of operation where information technology and its peripherals and remotes are exclusively used and controlled by specific users, or groups of users, for processing a particular type and category of classified or otherwise sensitive information. All users of the system have clearances and need-to-know for all material in the Technology Services Department.

O. *Electronic Media* – Electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory cards.

P. *Financial Instrument* – Any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

Q. *Information System* – A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

R. *Information Technology Security* – Includes all hardware and software functions, characteristics, and features; operational procedures, accountability procedures, and access controls at the data center facilities and remote terminal facilities; the management constraints; the physical environment; emanations security (EMSEC); and members and communications security needed to provide an acceptable level of protection for hardware, software, and sensitive information or material in the system.

S. *Intellectual Property* – Data, including programs.

T. *Internal Security Controls* – Hardware and software features within the Information Technology Department which restrict access to objects (hardware, software, and data) to only authorized subjects (persons, programs, or devices).

U. *Material* – Refers to data processed, stored, used, or generated by an information technology system, regardless of form or medium; for example, programs, reports, data sets, files and records.

V. *Mobile Laptop Computer* – The laptop computers used by field personnel to transmit data/information to and from the servers or secure City network.

W. *Multilevel Security* – A mode of operation which provides a capability that permits various levels and categories or compartments of data to be concurrently stored and processed in information technology and permitting selective access to such material concurrently by members (users) who have differing security clearances and need-to-know. Internal controls, as well as members, physical, and administrative controls, separate users and data on the basis of security clearance and need-to-know. The internal security controls shall be thoroughly demonstrated to be effective in preventing deliberate, malicious attempts to gain unauthorized access to classified information.

X. *Operating System* – An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in operating a computer system. Operating systems may perform input or

output, accounting, resource allocation, storage assignment tasks, and other system-related functions (synonymous with monitor, executive control program, and supervisor).

Y. *Password* – A protected word or string of characters which identifies or authenticates a user for access to a specific resource such as a data set, file, record, etc.

Z. *Personally Identifiable Information* – Any information about an individual maintained by the agency, including any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, driver’s license numbers, state resident/personal identification numbers, passport numbers and alien registration numbers, health insurance identification numbers provided by insurance carriers, Military ID number, date and place of birth, mother‘s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

AA. *Physical Media* – Any printed or written document, or printed imagery.

BB. *Physically Secure Location* – A facility or an area, a room, or a group of rooms within a facility, or the secure space within an agency vehicle, with both the physical and personnel security controls sufficient to protect sensitive information and associated information technology systems.

CC. *Property* – Anything of value as defined in Section 812.012, F.S., and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine readable or human readable form, and any other tangible or intangible item of value.

DD. *Remote Access* – Any temporary access to the secure City network and/or information systems by a user (or information system) communicating temporarily through an external, non-agency controlled network (e.g., the Internet).

EE. *Secure City Network* – The secure City network facilitates the transmission of sensitive and non-sensitive information from terminal to terminal within the City/Department.

FF. *Security Incident* – Any act or circumstance that involves sensitive information in which there is a deviation from the requirements of governing security regulations. For example: compromise, inadvertent disclosures, need-to-know violations, and administrative deviations.

GG. *Sensitive Information* – Agency generated or captured data, including, but not limited to information pertaining to the security of facilities, employees, and information, all personally identifiable information, digitized signatures (ink signatures that have been digitized), ongoing investigation information, and investigative technique information.

HH. *System Access Controls* – Access control mechanisms to enable access to sensitive information shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects.

II. *User* – Any person(s) or organization(s) who has access to an information technology via communication through a remote device or who is allowed to submit input to the system through other media, for example, tape or diskettes.

JJ. *User Identification* – A plain text or computer language set of characters that uniquely identifies any authorized person, office, or staff agency who may directly use and receive products or services from a computer system.

KK. *Vulnerability* – A weakness in information technology security procedures, administrative controls, internal controls, etc., that could be exploited to gain unauthorized access to classified information.

LL. *Wireless Network* – A wireless network that enables one or more information systems/devices to communicate without physical connections, without requiring network or peripheral cabling. Wireless network technologies include, but are not limited to: 802.11x, cellular networks, Bluetooth, satellite and microwave. Wireless network technologies shall require at least the minimum security applied to wired technology and, based upon the specific technology, may require some additional security controls.

APPROVED 

Charles E. Bird
CHIEF OF POLICE