1.0 Introduction and Purpose

The Information Security Rules of Behavior Handbook describes the rules associated with user's responsibilities and certain expectations of behavior using Information Systems and while connected to the County network, as required by Administrative Procedure 6–7. This handbook makes users aware of their role in safeguarding Information Systems and applies to all County employees, volunteers, interns, contractors, and business partners at all times, regardless of how or where they are accessing the Information Systems.

2.0 Definitions

2.0 Compliance–Mandated Departments or Information Systems – Departments or Information Systems that process, store, and/or transmit data subject to security restrictions imposed by the Federal and State governments, Health Insurance Portability and Accountability Act (HIPAA), FBI Criminal Justice Information Services Division (FBI CJIS), and the Payment Card Industry Data Security Standard (PCI–DSS).

2.1 Department of Technology Services (DTS) – An Executive Branch department responsible for County Government enterprise information systems and telecommunications.

2.2 Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

2.3 Sensitive Information – Any information that by law or County policy cannot be publicly disclosed, including without limitation:

A. Non–Public criminal justice information;
B. Credit or debit card numbers;
C. An individual's first name or first initial and last name, name suffixes, or unique biometric or genetic print or image, in combination with one or more of the following data elements;
   a) A Social Security number;
   b) A driver's license number or state identification card number, or other individual identification number issued by a State or local government;
   c) Passport number or other identification number issued by the United States government;
   d) An Individual Taxpayer Identification Number; e) A financial or other account number that in combination with any required security code, access code, or password, would permit access to an individual's account;
   f) Medical records; or
   g) Health insurance information.

2.4 Users – Individual, or (system) process acting on behalf of an individual, authorized to access a system.

3.0 Information Security Rules of Behavior

3.1 General

3.1.1 Any Information that is contained in, or stored on Information Systems, or transmitted, or received using Information Systems, is the property of the County and, therefore, is not private.

3.1.2 All activities performed on Information Systems may be monitored or logged.

3.1.3 Users teleworking at any alternate workplace must follow security practices that are the same as or equivalent to those required at the primary workplace.

3.1.4 Users must only use County provided and approved infrastructure or cloud solutions for conducting County business and storing County information.

3.1.5 Users must use only the County-provided email / calendaring / collaboration solution (Office 365) for County work; forwarding of a County business email to a User’s personal email system is prohibited.

3.2 When accessing or using Information Systems, Users must comply with the following:

3.2.1 Users must only access Information Systems and Information that is required in the performance of their official duties.

3.2.2 Users must promptly report any observed or suspected security problems/incidents, including loss/theft of Information Systems, or persons requesting that user to reveal their password.

3.2.3 Users must protect Sensitive Information per departmental procedures and report access, copying, or use of Sensitive Information that is not necessary to perform the User's County-assigned responsibilities.

3.2.4 Users must protect Information Systems from theft, destruction, or misuse.

3.2.5 Users must abide by software copyright laws.

3.2.6 Users must promptly change a password whenever it is compromised or suspected to be compromised.

3.2.7 Users must maintain the confidentiality of passwords and are responsible for actions performed with their accounts.

3.2.8 Users must lock Information Systems with a password when away from the work area (on–site and off–site), including for meals, breaks, or any extended period.

3.2.9 Users must physically protect Information Systems when used for teleworking and even when not in use.

3.2.10 Users must report unauthorized personnel that appear in the work area.

3.2.11 Users must protect Sensitive Information stored on electronic media, or in any physical format, such as paper, must lock the information in a secure area when not in use, and must delete, reformat, or shred Sensitive Information when it is no longer needed.

3.3 When accessing or using Information Systems, Users must not engage in the following activities:

3.3.1 Users must not write, display, or store passwords where others may access or view them.

3.3.2 Users must not download software or code from the Internet while connected to the County's network, unless explicitly approved and authorized by the County, as such downloads may introduce malware to the County's network.

3.3.3. Users must not obtain, install, replicate, or use unlicensed software unless authorized by their Department.

3.3.4 Users must not open emails from suspicious sources.

3.3.5 Users must not use peer-to-peer networking unless approved by the County or required for vendor support. Users must not conduct software or music piracy, hacking activities, or participate in online gaming.

3.3.6 Users must not acquire, possess, or use hardware or software tools that defeat software copy protection, discover passwords, identify security vulnerabilities, or circumvent encryption.

3.3.7 Users must not attempt unauthorized access to an Information System, including attempt to access the information contained within the system.

3.3.8 Users must not use copyrighted or otherwise legally protected material without permission.

3.3.9 Users must not transmit chain letters, unauthorized mass mailings, or intentionally send malware.

3.3.10 Users must not use any personal computers/devices for County business or Information System that show signs of being infected by a virus or other malware.

3.3.11 Users must report any suspected information security incident to the IT Help Desk.

3.3.12 The County will determine and provide approved and authorized hardware or peripheral devices to documented, authorized Users. General Users may not add any devices to the County network without permission from County management.

3.3.13 Users must not alter hardware or software settings on any Information Systems without permission.

3.3.14 Users must not authorize or make a ransom payment.