Attachment III

Information and Security Requirements and Procedures

DEFINITIONS:

County Data or Non-public Information: any information classified as Internal Use, Confidential, or Restricted and therefore requires protection.

Information Asset: without limitation, digital Information and any item that processes, stores, or transmits digital information and supporting infrastructure owned, leased, managed, operated, or maintained by, or in the custody of, the County or non-County entities and used for County purposes.

REFERENCE:

Board of Supervisors Policy 6.100 – Information Security Policy
Board of Supervisors Policy 6.101 – Use of County Information Assets
Board of Supervisors Policy 6.103 – Information Security Incident Reporting and Response
Board of Supervisors Policy 6.104 – Information Classification Policy

GUIDELINES:

- Approved Teleworkers must protect the confidentiality, integrity, and availability of the County's Information Assets from unauthorized disclosure, modification, or destruction.
- Approved Teleworkers must use County approved remote access (i.e., Zscaler, MyApps) and teleconference (i.e., Teams, Cisco WebEx) tools.
- Approved Teleworkers are permitted to use their personally owned desktop/laptop. At a minimum, the personally owned device must meet the following requirements (Employee must agree to allow the County to use automated methodologies to ensure requirements are met.):
  - Operating system software and application software, including web browsers, are kept up to date
  - Antivirus/Anti-malware software is installed and up to date
  - Full disk encryption if the personal device stores County Non-public information
  - Use of password protection
  - Compliance with all County Information Technology standards and procedures.
- Remote access login credentials must be kept confidential and not shared with others.
- Printing while teleworking must be authorized by the manager.
  - Printed or hard copy documents must be kept separate and secure when not in use.
  - Printed or hard copy documents must be disposed of securely using a cross-cut shredder or returned to County facilities and disposed of in secure shredding bins.
- County Data must NOT be saved on personally owned devices (e.g., desktop/laptop/tablet, USB flash drives) or public online storage (e.g., Google Docs, iCloud).
- When there is a business need to save County Non-public information to a USB flash drive, only a County-issued encrypted flash drive may be used.
- Utilize approved County file sharing systems to securely collaborate with other departments or approved external entities (SharePoint Online, OneDrive for Business, Microsoft Teams, or Managed File Transfer). Avoid using email to share such Information.
- When email must be used for sending County Data/Non-public Information, the message must be sent securely by inserting '[Secure]' in the email subject line.
- Non-County e-mail systems (e.g. personal e-mail accounts) must NEVER be used to conduct County business.
- Immediately report security and privacy incidents, including lost or stolen computing devices used for County business, regardless if County or personally owned, to your Departmental Information Security

Officer (DISO) or another employee in charge of information security for your department. After hours, the incident should be reported to the County’s Information Security Hotline at 562-940-3335.

ACKNOWLEDGEMENT:

I agree to abide by the preceding Information Security and Privacy Guidelines and understand, agree and will comply with the Board of Supervisors Policies on Information Technology and Security. Any violation of said guidelines and Board policies can result in the removal of Telework privileges as well as disciplinary action.