TECHNOLOGY SERVICES
PERSONALLY IDENTIFIABLE INFORMATION POLICY

POLICY NO. 39-01

I. **PURPOSE**:

This policy and supporting procedures are designed to provide Hernando County BOCC with a documented and formalized Personally Identifiable Information (PII) policy that is to be adhered to and utilized throughout the organization at all times. The subsequent policies and procedures relating to PII initiatives for Hernando County BOCC strive to ensure the overall *confidentiality, integrity, and availability* of highly sensitive and privileged information.

II. **POLICY**:

Personal Identifiable Information or PII, is any information that permits the identity of an Individual to be directly or indirectly inferred, including information that is linked or linkable to that individual, regardless of whether the individual is a U.S. Citizen, legal resident, visitor to the U.S. or employee or contractor to the County. Examples of PII include: social security numbers, driver's license numbers, passport number, Alien Registration number, or financial account number.

The County is aware of the necessity to take reasonable measures to safeguard protected personally identifiable information (PII) and other information the Federal awarding agency or pass-through entity designates as sensitive or the non-Federal entity considers sensitive consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality.

The County will exercise care when handling all PII by limiting the sharing of PII with other County employees, contractors and auditors and only shared when related to official duties of the County. When possible, all PII will be redacted prior to transmission and will only provide specific data elements needed to perform the task at hand. If copies of the PII are created to perform a particular task or project, all duplicate copies will be deleted or destroyed when they are no longer needed.

When handling, processing, transmitting, transporting and or storing PII, the County will limit the potential for unauthorized disclosure by educating personnel to be aware of their surroundings during the preparation of personal identifiable information.

If the PII is to be transmitted in electronic form, it will only be accessed via County approved devices such as laptops, USB flash drives and external hard drives. Personally owned USB flash drives may not be used. In addition, the County will avoid the use of personally owned computers and will disallow access to PII unless logged in through the secure virtual desktop. All personnel are directed to contact County Technology Services personnel for secure access prior to utilizing any personal devices.

Precautions will be taken when removing PII from the work place. No information should ever leave the workplace without proper authority. All paper documents must be under the control of the employee or locked in a secure receptacle when not in use. Personnel will be instructed to secure PII when in transit and to never leave PII unattended and unsecured.

When PII is transmitted via email, personnel should take steps to encrypt the information with passwords, sent separately from the PII and/or redact sensitive information. Information regarding PII stored on a shared network computer drive will have access limited to those personnel on a need to know by permission settings or passwords.

In the event of a loss of control, compromised, unauthorized disclosure, unauthorized acquisition, unauthorized access or similar incident, whether the incident is intentional or unintentional, it must be reported immediately to management who will in turn notify the proper legal authorities.

Adopted: June 26, 2018