Garland County Personal Identity Information Security Notification and Confidentially Policy

Garland County recognizes its need to maintain the confidentiality of Personal Identity Information (PII) and understands that such information is unique to each individual. The PII covered by this policy may come from various types of individuals performing tasks on behalf of Garland County and includes employees, applicants, independent contractors, and any PII maintained on its customer base. The scope of this policy is intended to be comprehensive. It will include county requirements for the security and protection of such information throughout the county and its approved vendors both on and off work premises.

Garland County Elected Officials and department heads have delegated authority for developing and implementing procedural guidance for ensuring that their departmental responsibilities under this policy are communicated and enforced.

Key Elements

Personal Identity Information (PII): Unique personal identification numbers or data, including:

- Social Security Numbers (or their equivalent issued by governmental entities outside the United States).
- Taxpayer Identification Numbers (or their equivalent issued by governmental revenue entities outside the United States).
- Employer Identification Numbers (or their equivalent issued by government entities outside the United States).
- State or foreign driver's license numbers.
- Date(s) of birth.
- Corporate or individually held credit or debit transaction card numbers (including PIN or access numbers) maintained in organizational or approved vendor records.

PII may reside in hard copy or electronic records; both forms of PII fall within the scope of this policy.

Vendors: Individual(s) or companies that have been approved by the County Judges Office/Finance Office as a recipient of organizational PII and from which the Finance Department has received certification of their data protection practices conformance with the requirements of this policy. Vendors include all external providers of services to the county and include proposed vendors. No PII information can be transmitted to any vendor in any method unless the vendor has been pre-certified for the receipt of such information.

PII Retention: Garland County understands the importance of minimizing the amount of PII data it maintains and retains such PII only as long as necessary. Garland County follows the federal statutes regarding PII.

All new hires entering the county who may have access to PII are provided with a copy of this policy. Employees in positions with regular ongoing access to PII or those transferred into such positions are required to review the policy and procedures for the maintenance of PII data annually.

PII Audit(s): Garland County conducts audits of PII information maintained by the county in conjunction with fiscal year closing activities to ensure that this policy remains strictly enforced and to ascertain the necessity for the continued retention of PII information. Where the need no longer exists, PII information will be destroyed in accordance with protocols for the destruction of such records and logs maintained for the dates of destruction. The Finance and Human Resources departments under the auspices of the County Attorney will conduct the audits.

Data Breaches/Notification: Databases or data sets that include PII may be breached inadvertently or through wrongful intrusion. Upon becoming aware of a data breach, the county will notify all affected individuals whose PII data may have been compromised, and the notice will be accompanied by a description of the action being taken to reconcile any damage as a result of the data breach. Notices will be provided as expeditiously as possible and in no event be later than the commencement of the payroll period, after which the breach was discovered.

The County Attorney will handle breach notifications(s) to all governmental agencies to whom such notice must be provided in accordance with periods specified under these laws. Human Resources will communicate notices to affected individuals after consultation with the County Attorney and within the period specified under the appropriate law(s).

Data Access: Garland County maintains an IT system where PII data may reside; thus, user access to such IT systems is the responsibility of the IT department. The IT department has created internal controls for such systems to establish legitimate access for users of data, and access shall be limited to those approved by IT. Any change in vendor status or the termination of an employee or independent contractor with access will immediately result in the termination of the user's access to all systems where the PII may reside.

Data Transmission and Transportation

1. **County Premises Access to PII:** The Finance, Human Resources, and IT departments have defined responsibilities for on-site access of data that may include access to PII; IT has the oversight responsibility for all electronic records and data access capabilities. Finance and Human Resources have the operational responsibility for designating initial access and termination of access for individual users within their organizations and providing timely notice to IT.

2. **Vendors:** Garland County may share data with vendors who have a business need to have PII data. Where such inter-county sharing of data is required, the IT department is responsible for creating and maintaining data encryption and protection standards to safeguard all PII data that resides in the databases provided to vendors.

3. **Portable Storage Devices:** Garland County reserves the right to restrict PII data it maintains in the workplace. In the course of doing business, PII data may also be downloaded to laptops or other computing storage devices to facilitate company business. To protect such data, the county will also require that any such devices use IT department-approved encryption and security protection software while such devices are in use on or off county premises. The IT department is responsible for maintaining data encryption and data protection standards to safeguard PII data that resides on these portable storage devices.

4. **Off-Site Access to PII:** Garland County understands that employees may need to access PII while off-site or on business travel, and access to such data shall not be prohibited, subject to the provision that the data to be accessed is minimized to the degree possible to meet business needs and that such data shall

reside only on assigned laptops/approved storage devices that have been secured in advance by the IT department.

Regulatory Requirements: It is the policy of the county to comply with any international, federal, or state statute and reporting regulations. Garland County has delegated the responsibility for maintaining PII security provisions to the Elected Officials and department heads. The Garland County Attorney shall be the sole entity named to oversee all regulatory reporting compliance issues. If any provision of this policy conflicts with a statutory requirement of international, federal, or state law governing PII, the policy provision(s) that conflict shall be superseded.

Employee Hotline: If an employee has reason to believe that his or her PII (please refer to what constitutes PII) data security has been breached or that county representative(s) are not adhering to the provisions of this policy, an employee should contact the HR Department at 501-651-7766 or contact the county Human Resources representative.

Confirmation of Confidentiality: All county employees must maintain the confidentiality of PII as well as county proprietary data to which they may have access and understand that such PII is to be restricted to only those with a business need to know. **Employees with ongoing access to such data will sign acknowledgment reminders annually attesting to their understanding of the county requirement**.

Violations of PII Policies and Procedures: Garland County views the protection of PII data to be of the utmost importance. Infractions of this policy or its procedures will result in disciplinary actions under the county's discipline policy and may include suspension or termination in the case of severe or repeat violations. PII violations and disciplinary actions are incorporated in the county's PII training to enforce the county's continuing commitment to ensuring that this data is protected by the highest standards.