Category: 400
Number: 404
Subject: DATA PROTECTION POLICY

1. **PURPOSE:** Establish a policy to identify protected data and to establish procedures for employees, contractors, vendors or other individuals who have access to protected data through Gratiot County systems, programs, databases or other information technology.
2. **AUTHORITY:** The Gratiot County Board of Commissioners.
3. **APPLICATION:** This Policy applies to Elected Officials, Department Heads, employees and any contractor, vendor or individual with access to Gratiot County systems or data.
4. **RESPONSIBILITY:** The Board of Commissioners shall be responsible for the authorization of this Policy. The Administrator shall be responsible for the administration of this policy.
5. **DEFINITIONS:**
    - 5.1 Data to be protected includes, but is not limited to:
        - 5.1.1 Personally Identifiable Information (PII): Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. Examples include: Full Name (if not common), National Identification Number, IP address (in some cases), Vehicle Registration Plate Number, Driver's License Number, Face, Fingerprints, or Handwriting, Credit Card Numbers, Digital Identity, Date of Birth, Birthplace, Social Security Number, and Genetic Information.
        - 5.1.2 Sealed Court Records: Records that have been sealed by a court or other non-public court records.
        - 5.1.3 Financial: County banking information or individuals' banking information used for direct deposit of wages, reimbursements, or vendor payments.
        - 5.1.4 Juvenile Court Records
        - 5.1.5 Ongoing Criminal Case Investigations
        - 5.1.6 Protected Health Information: Protected Health information as defined under Health Insurance Portability and Accountability Act (HIPAA)
        - 5.1.7 Usernames and Passwords: Usernames, passwords, Personal Identification Number (PIN) or account codes that allow employees to gain access to systems where County data is contained.
    - 5.2 Employee: An individual who is not an independent contractor and was hired and paid by Gratiot County to provide specific services for the County.
6. **POLICY:** Gratiot County (County) must protect the types of data listed in Section 5 from unauthorized modification, loss, leaks, and theft.
    - 6.1 The protection of data listed in Section 5 is a critical business requirement. However, the ability to access protected data to complete certain County work is critical to County operations.
    - 6.2 It is not anticipated that this technology control can alone effectively deal with the malicious theft scenario, or that it will reliably detect all data loss or theft. Its primary objective is employee awareness and to avoid accidental loss scenarios.

6.3 This policy serves as a County-wide minimum. In instances where a Department needs to meet more stringent industry compliance standards, the Department will adhere to those specific requirements. Examples of industry compliance standards include but are not limited to: Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA) Payment Card Industry Data Security Standards (PCI DSS), United States Internal Revenue Service Publication 1075 (IRS 1075), Michigan Social Security Number Privacy Act (SSNPA).

6.4 All county staff which may have access to data types listed in Section 5 (as defined) shall have a criminal history check run on their date of hire by the County.

6.5 All County Elected Officials, Department Heads and staff, employees, or any contract workers with access to data listed in Section 5 will need to complete Gratiot County's security awareness training and agree to uphold the Information Technology policies in the Non-Economic Personnel Manual.

- 6.5.1 Security awareness training must be completed within 30 days of hire date, and then annually thereafter.
- 6.5.2 Throughout the year, security awareness exercises may be conducted. If an employee fails a security exercise, the employee must complete an additional security awareness training session within 14 days of failing a security exercise.
- 6.5.3 If an employee does not complete security awareness training, he or she will have their network and email access suspended until training is successfully completed.

6.6 Each employee shall be provided a unique County-Issued User ID by the Gratiot County Information Technology Department that will grant employees access to the Gratiot County computer network.

6.7 Visitors to Gratiot County locations where data listed in Section 5 is contained must always be escorted by an employee who is authorized to be in that area.

6.8 If an employee should identify an unknown, unescorted, or otherwise unauthorized individual in County Courthouse locations where data listed in Section 5 is contained, he or she must immediately notify Court Security at ext. 4228. When unknown, unescorted, or otherwise unauthorized individuals are identified in areas where data listed in Section 5 is contained in any other County building, he or she should call 911.

6.9 Data listed in Section 5 of this policy may not be transmitted publicly, or via systems or communication channels not controlled by the County. For example, the use of external email systems or cloud services not paid for by the County and approved by Gratiot County IT to store or distribute data increases risk of data leaks and therefore is not allowed.

6.10 To maintain information security, employees must ensure that data listed in Section 5 is not left on one's desk unattended or otherwise in plain view.

6.11 Employees must use a secure password on all County systems or other systems used to conduct County business. Secure passwords must meet the following requirements:

- 6.11.1 Must be a minimum length of eight characters
- 6.11.2 Cannot be a dictionary word or proper name
- 6.11.3 Must include a special character or number
- 6.11.4 Cannot be the same as the user ID
- 6.11.5 Must be changed every 90 days
- 6.11.6 Cannot be the same as one of the 10 passwords previously used on the account

6.11.7 These credentials (username and password combination) must be unique, must not be shared with other employees or non-employees and must not be used on other external systems or services. A secure password may be shared with identified IT staff as needed for user support.

6.12 Employees separating from County service under any circumstances are required to relinquish and identify all data records, in any format, to their immediate supervisor.

6.13 Employees must immediately notify IT if a device containing data listed in Section 5 of this policy is lost (e.g., cell phone, laptop, flash drive, etc.)

6.14 Any Employee who finds a system or process which the Employee suspects is not compliant with this policy has a duty to inform IT so that appropriate action may be taken.

6.15 Employees assigned to work remotely must take extra precaution to ensure that data is appropriately handled. Employees should seek guidance from a supervisor and IT if they are unsure as to their responsibilities.

6.16 Employees must ensure that assets holding data listed in Section 5 of this policy are not left unduly exposed or vulnerable, for example, visible in the back seat of a vehicle.

6.17 Data that must be moved within the County is to be transferred only via business-provided secure transfer mechanisms (e.g., encrypted USB keys, network shares, Gratiot County email, etc.) The County will provide employees with systems or devices that fit this purpose. You must not use other mechanisms to handle data. If an employee has a question regarding use of a transfer mechanism, or it does not meet his or her business purpose, he or she should raise this with IT.

6.18 Any confidential information being transferred on a portable device (e.g., USB stick. laptop, cell phone) must be encrypted in line with industry best practices and applicable law and regulations. If there is doubt regarding requirements, employees must seek guidance from IT.

6.19 **Specific Procedures:**

6.19.1 All IT devices that require disposal such as Hard Disk Drives, Solid State Drives, USB Keys, CDs and DVDs, PDAs and Mobile Computing Devices must be turned into IT to be properly wiped or destroyed. Paper documents containing data listed in Section 5 must be shredded.

6.19.2 All other devices unable to be sanitized will be destroyed or will have the medium storing the data removed and destroyed by IT staff.

7. ADMINISTRATIVE PROCEDURES:

7.1 The County Administrator is authorized to adjust this policy where necessary to meet administrative responsibilities and to ensure the purpose of this policy is achieved.

7.2 Employees found to have violated this policy may be denied future access to data systems.

8. CONFLICT WITH STATE OR FEDERAL LAW: This Policy is subject to all applicable State and Federal laws and regulations regarding data protection and disclosure of information. Should this Policy conflict with any State or Federal law or regulation, the State or Federal law or regulation will control.

9. ADMINISTRATOR/LEGAL COUNSEL REVIEW: The Administrator has determined that this policy as submitted to the Board of Commissioners contains the necessary substance in order to carry out the purpose of the policy. The County Civil Counsel has determined that this policy as submitted complies with all applicable laws, rules and regulations.

Approved as to Substance:

Gratiot County Administrator (Signed)

Tracey Corder

Gratiot County Administrator (Printed)

12/16/2021

Date

Approved as to Legal Content:

Gratiot County Legal Counsel (Signed)

Sarah K. Osburn

Gratiot County Legal Counsel (Printed)

Cohl, Stoker & Toskey, P.C.

Name of Law Firm

12/16/21

Date

Board of Commissioners adoption:

Chair, Gratiot County Board of Commissioners (Signed)

1-4-2022

Date

Chuck Murphy

Chair, Gratiot County Board of Commissioners (Printed)

Date