

POLICY BULLETIN NO. 88



SUBJECT: PROTECTION AND DISPOSAL OF PERSONAL IDENTIFYING INFORMATION MAINTAINED BY GRAND VALLEY POWER

I. OBJECTIVE

To outline Grand Valley Power's ("GVP") policy for protection of Personal Identifying Information ("PII") that is stored or maintained by GVP, and disposition of PII when no longer needed. This policy is intended to meet requirements of applicable law, including Colorado Revised Statute Sections 6-1-713 and 6-1-713.5.

II. POLICY

GVP will (1) destroy or properly dispose of paper or electronic PII when it is no longer needed, and (2) implement and maintain reasonable measures to protect PII from unauthorized access, use, modification, disclosure or destruction through implementation and maintenance of reasonable security procedures and practices appropriate to the nature of the PII which take into account the nature and size of GVP.

III. IDENTIFICATION, DISPOSAL, AND PROTECTION OF PII

A. Definitions.

1. "Personal Identifying Information" (PII) means a social security number; a personal identification number; a password; a passcode; an official state or government-issued driver's license or identification card number; a government passport number; biometric data; an employer, student, or military identification number; or a financial transaction device. PII meeting the above requirements includes information in either paper or electronic form, and includes information about GVP consumers, board members, and employees.
2. "Biometric data" means unique data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account.
3. "Financial transaction device" means any instrument or device, whether known as a credit card, banking card, debit card, electronic fund transfer card, or guaranteed check card, or account number representing a financial account or affecting the financial interest, standing, or obligation of or to the account holder, that can be used to obtain cash, goods, property, or services to make financial payments, but shall not include a check, a "negotiable order of withdrawal," or a "share draft."

B. Stored Personal Identifiable Information.

With respect to GVP consumers, after verifying a person's identity using the name and social security number against a national credit check agency, GVP gathers data from consumers that includes PII. GVP also maintains PII regarding its employees and directors as part of Human Resources functions. In addition to names and dates of birth, GVP maintains the following items of PII:

1. Social Security Number;
2. Driver's License Number or Identification Card Number;
3. Financial Transaction Device (namely debit or credit card number, and/or banking account information); and
4. Password or Passcode

C. Destruction of GVP Personal Identifiable Information.

PII data is maintained on secured systems and paper files at GVP locations and with certain authorized third-party partners with whom GVP has a contractual relationship. When a consumer discontinues electric service with GVP or when an employee is no longer employed by GVP or a director no longer serves on the GVP board, PII will be protected and securely maintained until such time as the PII is no longer needed. When PII is no longer needed, and in accordance with applicable record retention requirements, policy, and related requirements, GVP shall destroy or arrange for the destruction of such documents within its custody or control that contain PII by shredding, erasing, or otherwise modifying the PII in the documents to make the PII unreadable.

D. Security and Protection of PII.

GVP shall secure and protect PII from unauthorized access, use, modification, disclosure, or destruction by utilizing reasonable security procedures and practices.

1. All electronic files that contain PII shall be stored within a secure, protected information system location specified and approved by GVP's Information Technology Manager. The following security measures shall be employed: provisioning and maintaining in-depth network security practices, including unique system user IDs with strong password requirements, network perimeter and internal protections utilizing firewall and intrusion detection equipment and/or software, malware protection on all endpoints, patch management, and data backup programs.

2. All physical files or documents that contain paper PII shall be stored in a locked room, drawer, cabinet, desk, or safe when not being actively viewed or modified. PII shall not be left unattended on a desk, network printer, fax machine, or copier.
3. Data Access. Access to PII is limited to GVP personnel and GVP partner companies with legitimate business need to know and who have agreed to comply with GVP's data privacy and security requirements. GVP consumers have access to their own data via an electronic application and may make changes to their GVP records by using the application. Otherwise consumer data can be changed when a consumer contacts a GVP employee who will first verify identity of the consumer using a PIN and/or last four digits of their social security number, or in person at GVP headquarters after presenting identification, e.g., driver's license, passport, work visa.
4. Unless GVP agrees to provide its own security protection for the information it discloses to a third-party service provider, GVP shall require that third-party service providers having access to PII implement and maintain reasonable security procedures and practices that are:
 - i. Appropriate to the nature of the PII disclosed to the third-party service provider; and
 - ii. Designed to protect the PII from unauthorized access, use modification, disclosure, or destruction.
5. Confidentiality of Social Security Numbers ("SSN"). As required by Colorado Revised Statutes Section 6-1-715, GVP shall not:
 - i. Publicly post or publicly display in any manner an individual's SSN. "Publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public;
 - ii. Print an individual's SSN on any card required for the individual to access products or services provided by GVP;
 - iii. Require an individual to transmit his or her SSN over the internet, unless the connection is secure or the SSN is encrypted;

- iv. Require an individual to use his or her SSN to access an internet website, unless a password or unique personal identification number or other authentication device is also required to access the internet website; or
- v. Print an individual's SSN on any materials that are mailed to the individual, unless state or federal law requires, permits, or authorizes the SSN to be on the document to be mailed. Notwithstanding this paragraph, SSNs may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend, or terminate an account, contract, or policy, or to confirm the accuracy of the SSN. A SSN that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

IV. RESPONSIBILITY

- A. The Board of Directors of Grand Valley Power is responsible for approval of this policy as well as changes and revisions to this policy.
- B. The CEO and Information Technology Manager shall be responsible for the overall administration of this policy. The CEO shall also be responsible for making delegations of authority to staff members for the implementation of the specific provisions of this policy.

Date Adopted: October 17, 2018
Date Revised: September 21, 2022

APPROVED: Jesse Mease
Board Secretary