WEST VIRGINIA
OFFICE OF
ENERGY

PRIVACY AND SECURITY RISK ASSESSMENT

State of West Virginia
Home Efficiency Rebates
Inflation Reduction Act
(50121)

Executive Summary

The West Virginia Office of Energy places the highest priority on the privacy and security of consumer data. The state's privacy and risk assessments are meticulously designed to protect the sensitive information entrusted to the office, ensuring robust safeguards against unauthorized access, data breaches, and associated risks. These protocols reflect the state's unwavering commitment to maintaining the highest standards of data protection, ensuring that all personal and utility data is managed with the utmost diligence and integrity.

Contents

System Categorization Rationale

The state will utilize system categorization as a critical first step in risk assessment to determine the level of protection required for the Rebate Program and the data it handles. The categorization rationale is based on the sensitivity, confidentiality, and integrity of the data processed, stored, or transmitted within the boundaries of the Rebate Program. The state's rationale for categorization is as follows:

- *Sensitivity of Data*: The Rebate Program collects Personally Protected Information (PPI) such as names, addresses, utility information, dates of birth (DOB), and phone numbers. The sensitivity of this data is high because its unauthorized disclosure or misuse can result in identity theft, financial fraud, and other serious consequences.
- *Confidentiality*: Given the nature of the PPI involved, the Rebate Program requires a high level of confidentiality. Unauthorized access to this information could lead to privacy violations and legal liabilities.
- *Integrity*: The integrity of the data is crucial to ensure that information remains accurate and unaltered. Any corruption or manipulation of this data could lead to incorrect decisions and undermine the effectiveness of the Rebate Program.
- *Availability*: Information and data collected must be available to authorized users as needed, as any disruption in availability could impact the ability to deliver services, leading to operational and reputational risks.

Method for Determining Risk Impacts

The following steps are used to assess risk impacts:

Identifying Potential Risks

The state has identified the potential risks associated with the Rebate Programs data collection:

- *Data Sharing Risks*: Unauthorized access or misuse of shared data by third-party entities.
- *Data Corruption Risks*: Inaccurate or altered data due to system errors, cyber-attacks, or malicious activity.
- *Data Loss Risks*: Loss of data due to hardware failures, accidental deletion, or cyber-attacks.
- *Loss of Confidentiality Risks*: Unauthorized access to sensitive information leading to privacy breaches.

Assessing the Impact of Each Risk

The impact of each identified risk is assessed based on the following criteria:

- *Severity*: The potential harm or damage caused by the risk event, including financial, operational, legal, and reputational impacts.
- *Exposure*: The extent to which the Rebate Program or organization is exposed to the risk, including the number of users or systems affected.

- *Likelihood*: The probability of the risk event occurring based on historical data, industry trends, and system vulnerabilities.

Determining Risk Level
The state will determine the overall risk level by evaluating the severity, exposure, and likelihood of potential risks. Based on these assessments, the risk level will be classified as low, medium, or high, guiding the state's prioritization and implementation of appropriate mitigation strategies.

Risks Associated with Data Sharing

The state has identified the following risks associated with data sharing within the Rebate Program.

- *Unauthorized Access*: Third-party entities with access to the data may misuse or share the information without proper authorization.
- *Data Breach:* Weaknesses in the security controls of third-party entities could lead to breaches, exposing sensitive data.
- *Non-compliance*: Failure of third-party entities to adhere to data protection regulations and agreements could result in legal penalties and reputational damage.

Risks of Data Corruption, Loss, and Confidentiality Breaches

Data Corruption

- *Impact:* Corruption of data can lead to inaccurate or misleading information, affecting decision-making and program outcomes. In the case of PPI, corrupted data could misrepresent individual identities, leading to wrongful actions or denial of services.
- *Causes:* Data corruption can occur due to software bugs, hardware malfunctions, cyber-attacks (e.g., ransomware), or human error.
- *Mitigation*: Regular data integrity checks, robust error detection mechanisms, and maintaining secure backups are essential to mitigating the risk of data corruption.

Data Loss

- *Impact*: The loss of data, especially PPI, may disrupt program operations, erode trust, and result in significant legal and financial penalties.
- *Causes:* Data loss can occur due to accidental deletion, hardware failure, cyber-attacks, or natural disasters.
- *Mitigation:* Implementing redundant data storage, regular backups, disaster recovery plans, and access controls will help the state and its partners in preventing data loss.

Loss of Confidentiality

- *Impact:* Unauthorized disclosure of data may lead to identity theft, financial fraud, and other privacy violations. It may also damage the state's reputation and result in legal consequences.
- *Causes*: Confidentiality breaches may occur due to inadequate access controls, insider threats, cyber-attacks, or data sharing with untrustworthy third parties.
- *Mitigation*: Employing strong encryption, access controls, continuous monitoring, and employee training on data protection best practices will help safeguard confidentiality.

Factors Considered in Determining Risk Impact

West Virginia will consider the following factors when determining risk impact:

- *Data Sensitivity*: The more sensitive the data, the greater the potential impact of a breach or loss.
- *Regulatory Requirements*: Compliance with laws and regulations that mandate specific protections for data collected through the Rebate Program including but not limited to: The E-Government Act of 2002 and SP 800-171. Additionally the state will follow standards set forth in the ISO/IEC 27002.
- *Operational Dependency*: The extent to which program operations rely on the availability, integrity, and confidentiality of the data.
- *Stakeholder Impact:* The potential harm to individuals, customers, partners, and the state itself.
- *Threat Environment:* The current landscape of cybersecurity threats, including emerging risks and known vulnerabilities.

7. Conclusion

West Virginia's Privacy and Security Assessment underscores the state's unwavering commitment to safeguarding consumer information while ensuring the effectiveness of the Rebate Program. By rigorously protecting sensitive data through comprehensive risk management strategies, the state not only upholds the highest standards of privacy and security but also enhances the overall success of initiatives. The state's dedication to these principles ensures that consumers can trust in the integrity of the Rebate Program and maintain confidence in knowing that their information is secure and that the state's efforts are driving meaningful, measurable outcomes.

Links / References

https://technology.wv.gov/our-departments/cyber-security

https://code.wvlegislature.gov/email/5A-6B/

https://privacy.wv.gov/privacyimpactassessment/Pages/default.aspx

FIPS Publication 199: Establishes standards for security categorization of federal information and information systems (Section 3, p. 1-4).

NIST SP 800-53: Provides detailed security controls for continuous monitoring and incident response (Sections 3 and 4, p. 25-53).

NIST SP 800-61: Guide for Computer Security Incident Handling provides guidelines for developing and maintaining an effective incident response plan (Sections 2 and 3, p. 7-18).