DIVS

Privacy Policy

for

DIVS Vendors, Developers and Suppliers

Version 1.4

April 17, 2014

This Document was prepared under a grant from the Federal Emergency Management Agency's (FEMA) Grant Programs Directorate (GPD) United States Department of Homeland Security. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position of policies of FEMS/GPD or the U.S. Department of Homeland Security.

This document and associated work product were produced by Clerus Solutions, LLC as IProgram Manager to the DL/ID Verification Systems, Inc. program under contract to the Mississippi Department of Public Safety.

TABLE OF CONTENTS

1 DIVS PRIVACY POLICY

1.1 *Policy*

The privacy[1] of individuals will be protected and respected in all aspects of the Drivers License ID Verification (DIVS) systems, including the development environment, the support environment, and both the centralized and distributed components of the deployed system.

All companies and agencies involved in the development, operation, support and use of the DIVS systems[2] shall be required, contractually or via user agreements, to adhere to and implement this policy.

1.2 *Basis*

The privacy goals and requirements in this policy are based on and generally consistent with a blend of relevant federal and state guidelines and requirements. These include but are not limited to REAL-ID legislation; NIST Special Publications (SP) 800-122, SP 800-64 Rev. 2, and SP 800-53 Rev. 4; the Drivers Privacy Protection Act (DPPA); DHS' Handbook for Safeguarding Sensitive Personally Identifiable Information; the Fair Information Practice Principles (FIPP) used within DHS; and various state regulations.

2 PII IN DIVS

2.1 *Definition of PII in DIVS*

"Personally Identifiable Information", or PII, is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual.

2.2 *PII in DIVS*

PII that has been identified in DIVS includes, but is not necessarily limited to, the following.

Full legal name

Date of birth

SSN

Last 5 digits of the SSN

DL/ID number and State of Record

AKA names

AKA DOB

Driver photo

Driver signature

[1] For the purpose of this policy, "privacy" is the protection of information belonging to an individual through the use of controls to ensure that this information is not disseminated or accessed in an unauthorized manner.

[2] With the sole exception of the users, these will be referred to collectively as 'Vendors, Developers or Suppliers' or 'VDS'.

2.3 *Confidentiality Impact level of PII*

The overall Confidentiality Impact Level of the PII in DIVS is ***moderate***, based on the classification scale in SP 800-122. This is the level that should be used as the default by vendors, developers and suppliers except where an examination of the specific situation justifies deviation.

This ***moderate*** rating implies that while the harm resulting from inappropriate access, use or disclosure of PII in the DIVS systems, or from the compromise of the PII's integrity or availability, could be expected to have a serious adverse effect on agencies, or individuals, it is not likely to be life threatening to the individual(s) or to severely or catastrophically jeopardize the mission of any of the participating companies or agencies.

3 DIVS – PRIVACY PLAN

Every vendor, developer or supplier must document in a *privacy plan*[3] how it will address privacy concerns in its portion of DIVS. Each such privacy plan will be evaluated against the requirements in this and section 4.

3.1 *Fair Information Practice Principles*

Decisions affecting the privacy of individuals whose data is stored or processed as part of the DIVS systems, their development or operation, must be consistent with the Fair Information Practice Principles, as described in DHS Privacy Policy Guidance Memorandum number 2008-01, dated December 29, 2008.

DIVS VDSs are responsible for ensuring that their policies, local decisions and actions accurately implement the Fair Information Practice Principles as they apply to whatever aspects of the DIVS systems they are directly responsible for (e.g., a development environment, a data base, etc.), and also that they do nothing that would undermine the application of these principles to the deployed DIVS systems.

3.2 *NIST Privacy Controls*

VDS privacy policy should recognize privacy of PII as a core value that requires establishing appropriate privacy controls to ensure compliance with requirements. Appendix J in NIST SP 800-53 Rev. 4, states that "(p)rotecting the privacy of individuals and their PII that is collected, used, maintained, shared, and disposed of by programs and information systems, is a fundamental responsibility".

[3] It is acceptable, though not required, for the vendor, developer or supplier to create a single privacy/security plan instead of separate privacy and security plans.

DIVS VDSs are responsible for ensuring that their policies, local decisions and actions accurately implement the controls for protecting privacy specified in Appendix J of NIST SP 800-53, Rev. 4. These privacy controls are summarized below and address information privacy that is distinct from, but highly interrelated with, the information security controls that are addressed in DIVS Security Policy for DIVS Vendors, Developers, and Suppliers.

3.2.1 *Authority and Purpose (AP)*

To the extent that the VDS collects or conducts activities that affect the privacy of information, the VDS privacy policy should identify the legal basis that authorizes collection and performance of those activities. The VDS privacy policy should specify that the VDS privacy notice includes the purposes for which the PII is collected.

3.2.1.1 The VDS determines the legal basis and authority that permits it to collect, use, maintain, and share PII.

3.2.1.2 The VDS privacy policy and privacy compliance documentation specifies the purpose for which PII is collected.

3.2.1.3 The VDS privacy policy/plan must require that all use of PII be consistent with the original and authorized purpose.

3.2.2 *Accountability, Audit, and Risk Management (AR)*

The VDS privacy policy specifies controls implemented for the effective governance, monitoring, risk management, and assessment that enhance public confidence and demonstrate that the VDS complies with privacy protection requirements and minimizes overall privacy risk. The privacy plan must include a discussion of VDS practices and commitments with respect to violations of its policies, or breaches of trust that have privacy implications with significant consequences for violations and breaches.

3.2.2.1 The VDS develops and implements a comprehensive governance and privacy program, including a privacy plan, showing their accountability for and commitment to protecting individual privacy.

3.2.2.2 The VDS conducts a risk assessment of the privacy issues associated with DIVS systems and the VDS facilities that are used in support of DIVS. A Privacy Impact Assessment (PIA) along the lines of those required for federal systems may be used for this purpose. The VDS may add material required to address privacy issues specific to its facilities and functions that are not already addressed in the DIVS system PIA.

3.2.2.3 In contracts and other documents related to service acquisition, the VDS establishes privacy roles, responsibilities, and requirements for contractors and service providers.

3.2.2.4 The VDS uses on-going monitoring and audits to ensure the effective implementation of privacy controls and internal privacy policy.

3.2.2.5 The VDS develops, implements, and updates training and awareness strategies including a basic privacy training and certification program to ensure that personnel understand their privacy responsibilities and procedures. Personnel certify their acceptance annually, at a minimum.

3.2.2.6 The VDS privacy plan includes procedures to develop, disseminate, and update privacy reports.

3.2.2.7 The VDS designs information systems that automate controls to enhance privacy.

3.2.2.8 The VDS keeps an accurate accounting of disclosures of information held in systems under their control. The VDS retains this information as required and makes it available upon request to the person named in the record.

3.2.3 *Data Quality and Integrity (DI)*

The VDS privacy policy should specify implementation of privacy controls to ensure that PII collected and maintained by the VDS is accurate, relevant, timely, and complete for the purpose for which it is used, as specified in the VDS public notice.

3.2.3.1 To the greatest extent practicable, the VDS collects PII directly from the individual and confirms that the quality of the data it collects is accurate, relevant, timely, and complete.

3.2.3.2 The VDS corrects inaccurate or outdated PII used by its programs or systems.

3.2.3.3 The VDS issues guidelines to ensure and maximize the quality, utility, objectivity, and integrity of disseminated information.

3.2.4 *Data Minimization and Retention (DM)*

The VDS privacy policy should require implementation of data minimization and retention controls to ensure that the VDS collects, uses, and retains only PII that is relevant and necessary for the specified purpose for which the data was originally collected. The policy should specify that the VDS retains PII for only as long as necessary and in accordance with approved record retention schedules. Additional specification is for the VDS to destroy PII according to documented schedules and procedures.

3.2.4.1 The VDS identifies, collects, and retains only the minimum PII elements needed to meet its legally authorized purpose for collection. The VDS periodically reviews and evaluates its holdings of PII.

3.2.4.2 The VDS only retains PII for the period required to fulfill its purpose as identified in the notice or as required by law. The VDS disposes of, destroys, erases, and/or anonymizes PII regardless of storage method in a manner consistent with preventing loss, theft, misuse, or unauthorized access.

3.2.4.3 The VDS will not use PII for development or testing.

3.2.4.4 The VDS protects PII that it retains through de-identification or anonymization where doing so improves privacy while still supporting necessary functionality.

3.2.4.5 In some cases, DIVS requires full database and column-level encryption of SSNs and DOBs in deployed systems. Similar measures may be appropriate at other points in the development and testing environments and should be considered by the VDS in its security plans for DIVS.

3.2.5 *Individual Participation and Redress (IP)*

The VDS privacy policy should specify that individuals are provided access to their PII and the ability to correct or amend their PII, as appropriate. As a result, individuals become active participants in decision-making processes concerning the collection and use of their PII.

3.2.5.1 Where feasible and appropriate, the VDS provides the individual the ability to authorize the collection, use, maintenance, and sharing of PII prior to collection. The consequences of decisions by the individual to approve or decline authorization are explained. Individuals are given the opportunity to provide their consent to new uses or disclosure of their PII before the new use or disclosure is implemented. The VDS ensures that individuals are aware of and consent to all uses of PII not initially described in the public notice.

3.2.5.2 The VDS provides access to individuals to their PII maintained by VDS systems in order to determine if the PII requires correction or amendment. The VDS publishes rules and regulations that govern requests to access records. The VDS publishes access procedures in System of Records Notices (SORNs).

3.2.5.3 The VDS provides a process by which individuals can correct or amend inaccurate PII as well as establishes a process to disseminate corrections or amendments of PII to other authorized users of the PII.

3.2.5.4 The VDS implements a process to receive and respond to complaints, concerns, or questions from individuals regarding the VDS privacy practices.

3.2.6 *Security (SE)*

The VDS coordinates with information security personnel to ensure that the VDS privacy policy supplements the security policy. This coordination includes the implementation of administrative, technical, and physical safeguards to protect PII against loss, unauthorized access, or disclosure and includes privacy incident planning and response. The privacy plan indicates how access is protected at all times, with controls that are adequate to prevent easy breaches of PII by unauthorized individuals.

3.2.6.1 The VDS establishes, maintains, and updates an inventory of its programs and systems in which it collects or conducts activities involving PII.

3.2.6.2 The VDS privacy plan includes an incident response plan used in privacy-related incidents. This may be contained within a general information security incident response plan.

3.2.6.3 Incident notification procedures must meet the most stringent notification standard of any state involved in the DIVS systems.

3.2.6.4 The privacy plan should indicate how privacy tenets and requirements are met throughout the entire System Development Life Cycle.

3.2.7 *Transparency (TR)*

The VDS privacy policy should require the VDS to issue public notice of its information practices and the privacy impact of their programs and activities.

3.2.7.1 The VDS provides and updates effective notice to the public and individuals regarding its activities that impact privacy and its authority for collecting PII. The notice should specify choices, if any, individuals have regarding how the VDS uses PII and consequences of exercising or not exercising those choices. The notice documents the ability to access and have PII amended.

3.2.7.2 The VDS keeps its public notice current with information on the PII collected, the purpose for that collection, and how PII is protected. In addition, the notice describes how PII is used internally by the VDS and if PII is shared with external entities including the purpose for such sharing. Through the VDS public notice, individuals are informed of their ability to consent to specific uses or sharing of PII and how they can access PII for the purpose of amendment or corrections.

3.2.8 *Use Limitation (UL)*

The VDS privacy policy should stipulate that the scope of PII use is limited. The privacy plan should indicate to whom and in what situations PII will be shared with other parties, any special arrangements or contract clauses that will be used in those situations, and provisions for approval of emergency sharing in exigent circumstances.

3.2.8.1 The privacy plan should forbid any sharing not specifically included in the documented situations.

3.2.8.2 The VDS uses PII internally only for the authorized purposes allowed by the Privacy Act or specified in public notices.

3.2.8.3 Information sharing with third parties is only for authorized purposes under a specific third party agreement (e.g., Memoranda of Understanding) with VDS staff monitored, audited, and trained on the authorized uses and sharing of PII including consequences violations.

4 DIVS - GENERAL SECURITY CONTROLS RELEVANT TO PRIVACY

General security controls that have special relevance for privacy must be considered from the perspectives of general system/data security and privacy.

The following controls are from SP 800-53 Rev 4 (April, 2013). The controls are identified in SP 800-122 as having particular value in protecting PII or for privacy in general. The control names and references (e.g., "AC-3") correspond to security controls as listed in SP 800-53 Rev 4.

Note: The security controls listed below may also appear in the *DIVS Security Policy*. The *DIVS Security Policy* focuses on all sensitive data[4] and functionality, whereas this *DIVS Privacy Policy* is specifically concerned with PII and privacy-related functionality. The implementation of the following security controls must satisfy both purposes.

4.1 *Access Enforcement (AC-3)*

Access to PII must be positively controlled at all times, only permitted with prior authorization, and based on the Principle of Least Privilege.

4.2 *Separation of Duties (AC-5)*

Situations where a separation of duties can reduce the risk of privacy incidents should be identified and, where practical, implemented.

4.3 *Least Privilege (AC-6)*

When assigning privileges to access or handle PII, parties – as individuals or by role – should be granted no more than the minimum access privileges that are needed to perform their duties and carry out their roles, consistent with maintaining an appropriate level of granularity with respect to ACL sets.

[4] "Sensitive Information" is defined as "Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act); that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy." (Source: National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, p.b-23.)

4.4 *Remote Access (AC-17)*

A clear policy with respect to remote access to systems or files containing PII needs to be promulgated.

Remote access should be prohibited where not essential, and where allowed, needs to be well protected, for example with strong encryption.

4.5 *Access Control for Mobile Devices (AC-19)*

There must be a clear policy with respect to the use of portable devices in situations where PII is accessed, processed, or stored.

The devices covered by the policy must include but need not be limited to laptop computers, smart phones and personal digital assistants (PDAs).

The policy must cover remote access, local storage, and use of applications that process PII, and must reflect the relative risks of devices and situations.

4.6 *Information Sharing (AC-21)*

Automated mechanisms can be provided to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.

4.7 *Audit Events (AU-2)*

Logs shall be used to maximum effect to protect PII during development, deployment, operation and support of the DIVS systems.

Situations where access or manipulation of PII can be accomplished without being subject to reliable logs or audit must be identified and compensating controls considered.

4.8 *Audit Review, Analysis, and Reporting (AU-6)*

Effective audits, oversight and reviews are central to the security of PII in the development and operational environments and must be included in every VDS privacy plan.

4.9 *Identification and Authentication (Organizational Users) (IA-2)*

Each user accessing PII should be uniquely identified and individually authenticated.

The strength of the authentication method and session management should favor strong controls (e.g., two-factor authentication, session timeouts) wherever practical.

4.10 *Media Access, Marking, Storage, Transport, Sanitization (MP-2 to MP-6)*

Best practices must be used to provide for the security of PII on media.

Controls should address PII in digital and non-digital forms, and on any type of device or media including, but not limited to, electronic storage devices, tape, film and paper.

4.11 *Transmission Confidentiality and Integrity (SC-8)*

PII must be protected during all types of transmission, whether across physical (e.g., wires, cables, optical fibers) or wireless data links.

4.12 *Protection of Information at Rest (SC-28)*

Confidentiality of PII at rest must be protected, including PII information stored on secondary devices such as hard drive or backup tape and is usually accomplished through encryption.

4.13 *Information System Monitoring (SI-4)*

Automated tools, such as data loss prevention technologies, shall be utilized to monitor PII internally or at network boundaries for unusual or suspicious transfers or events.