securityMETRICS®

PCI Security Standards Council®

Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Self Assessments - Merchants

Version 3.2.1

July 2021

Attestation of Compliance, SAQ A 3.2.1

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the merchant's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact your acquirer (merchant bank) or the payment brands for reporting and submission procedures.

Part 1. and Qualified Security Assessor Information

Part 1a. Organization Information

Company Name:	Permitium, LLC		DBA (doing business as):	Government Records	
Contact Name:	Paul Blake		Title:	Managing Member	
Telephone:	9495845766		E-mail:	paul.blake@permitium.com	
Business Address:	10617 Southern Loop Blvd		City:	Pineville	
State/Province:	NC	Country:	United States	Zip:	28134
URL:	www.permitium.com				

Part 1b. Qualified Security Assessor Company Information (Not applicable: self-attested)

Company Name:					
Lead QSA Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					

PCI Security Standards Council

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

☐ Retailer	☐ Telecommunication	☐ Grocery and Supermarkets
☐ Petroleum	☑ E-Commerce	☐ Mail order/telephone order (MOTO)

☐ Others (please specify):

What types of payment channels does your business serve?	Which payment channels are covered by this assessment?
☐ Mail order/telephone order (MOTO)	☐ Mail order/telephone order (MOTO)
☑ E-Commerce	☑ E-Commerce
☐ Card-present (face-to-face)	☐ Card-present (face-to-face)

Note: If your organization has a payment channel or process that is not covered by this assessment, consult your acquirer or payment brand about validation for other channels.

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?	N/A

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)

Part 2d. Payment Application

Does the organization use one or more Payment Applications? ☐ Yes ☑ No

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment. For example: • Connections into and out of the cardholder data environment (CDE) • Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable	All credit and debit card information is collected online through fields host directly by our processor - Authorize.net. No Credit or Debit card information is stored by Permitium.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☑ Yes ☐ No

securityMETRICS®

Part 2f. Third-Party Service Providers

Does your company use a Qualified Integrator & Reseller (QIR)?	☐ Yes ☑ No
Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?	☑ Yes ☐ No

Name of service provider:	Description of services provided:
Authorize.net	Web Host

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2g. Eligibility to Complete SAQ A

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:

☑	Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
☑	All payment acceptance and processing are entirely outsourced to PCI DSS validated third-party service providers
☑	Merchant has no direct control of the manner in which cardholder data is captured, processed, transmitted, or stored;
☑	Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
☑	Merchant has confirmed that all third party(s) handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
☑	Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically.
☑	*Additionally, for e-commerce channels* The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s).

PCI Security Standards Council

Section 2: Self-Assessment Questionnaire A

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying Self-Assessment Questionnaire (SAQ).

The assessment documented in this attestation and in the SAQ was completed on:	2021-03-18
Have compensating controls been used to meet any requirement in the SAQ?	☑ Yes ☐ No
Were any requirements in the SAQ identified as being not applicable (N/A)?	☑ Yes ☐ No
Were any requirements in the SAQ unable to be met due to legal constraint?	☐ Yes ☑ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the SAQ A dated (2021-03-18).
Based on results documented in the SAQ noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document **(check one):**

✓	**Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Permitium, LLC* has demonstrated full compliance with PCI DSS.
	Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or not all questions answered affirmatively, resulting in an overall **NON-COMPLIANT** rating; thereby *Permitium, LLC* has not demonstrated full compliance with PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4.*
	Compliant but with Legal exception: One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.

Part 3a. Acknowledgement of Status

Signatory(s) confirms:
(Check all that apply)

✓	PCI DSS Self-Assesment Questionnaire A, Version 3.2.1, was completed according to the instructions therein.
✓	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
✓	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
✓	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.
✓	No evidence of full track data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during this assessment.

Part 3b. Attestation

ELECTRONICALLY ATTESTED

Signature of Executive Officer ^	*Date:* 2021-03-18
Executive Officer Name: Paul Blake	*Title:* Managing Member

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

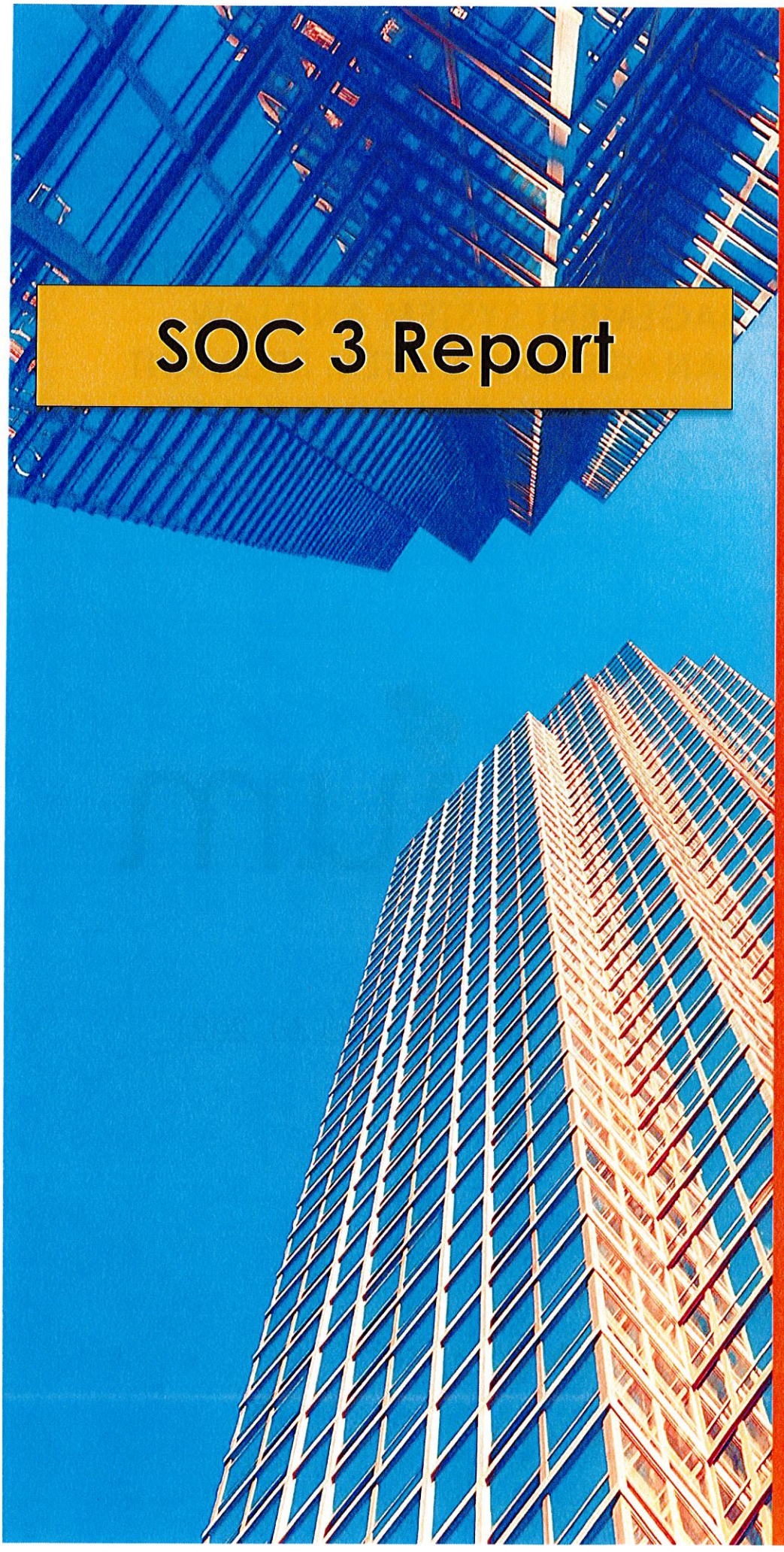
If a QSA was involved or assisted with this assessment, describe the role performed:	

N/A: Self-Attested only

Signature of Duly Authorized Officer of QSA Company ^	*Date:*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. Internal Security Assessor (ISA) Acknowledgement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	



SOC 3 Report

2021

Lazarus Alliance, Inc.

27743 N. 70th Street, Suite 100

Scottsdale, Arizona 85266 United States

http://www.lazarusalliance.com

REPORT ON PERMITIUM, LLC'S DESCRIPTION OF ITS SCHOOL MANAGEMENT SYSTEM AND LAW ENFORCEMENT MANAGEMENT SYSTEM RELEVANT TO SECURITY, AVAILABILITY, CONFIDENTIALITY, PROCESSING INTEGRITY, AND PRIVACY

Permitium, LLC

Assessment Dates: May 1, 2020 to April 30, 2021

Table of Contents

Section 1 - Assertion of Permitium, LLC Management

Permitium

(855) 712-PERM
support@permitium.com

10617 Southern Loop Blvd
Pineville, NC 28134

Assertion of Permitium, LLC Management

May 7, 2021

We are responsible for designing, implementing, operating, and maintaining effective controls within Permitium, LLC's ("Permitium", the "Company", or the "Service Organization") School Management System and Law Enforcement Management System throughout the period May 1, 2020, to April 30, 2021, to provide reasonable assurance that Permitium's service commitments and system requirements relevant to security, availability, processing integrity, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 1, 2020, to April 30, 2021, to provide reasonable assurance that Permitium's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Permitium's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period May 1, 2020, to April 30, 2021, to provide reasonable assurance that Permitium's service commitments and system requirements were achieved based on the applicable trust services criteria.

Permitium, LLC Management

Section 2 - Independent Service Auditor's Report

Lazarus Alliance Compliance
Proactive Cyber Security©

To: Permitium, LLC

Scope

We have examined Permitium, LLC's ("Permitium", the "Company" or the "Service Organization") accompanying assertion titled "Assertion of Permitium, LLC's Management" (assertion) that the controls within Permitium's School Management System and Law Enforcement Management System (system) were effective throughout the period May 1, 2020, to April 30, 2021, to provide reasonable assurance that Permitium's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Permitium is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Permitium's service commitments and system requirements were achieved. Permitium has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Permitium is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Permitium's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Permitium's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Permitium's School Management System and Law Enforcement Management System were effective throughout the period May 1, 2020, to April 30, 2021, to provide reasonable assurance that Permitium's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Lazarus Alliance Compliance, LLC

Scottsdale, AZ

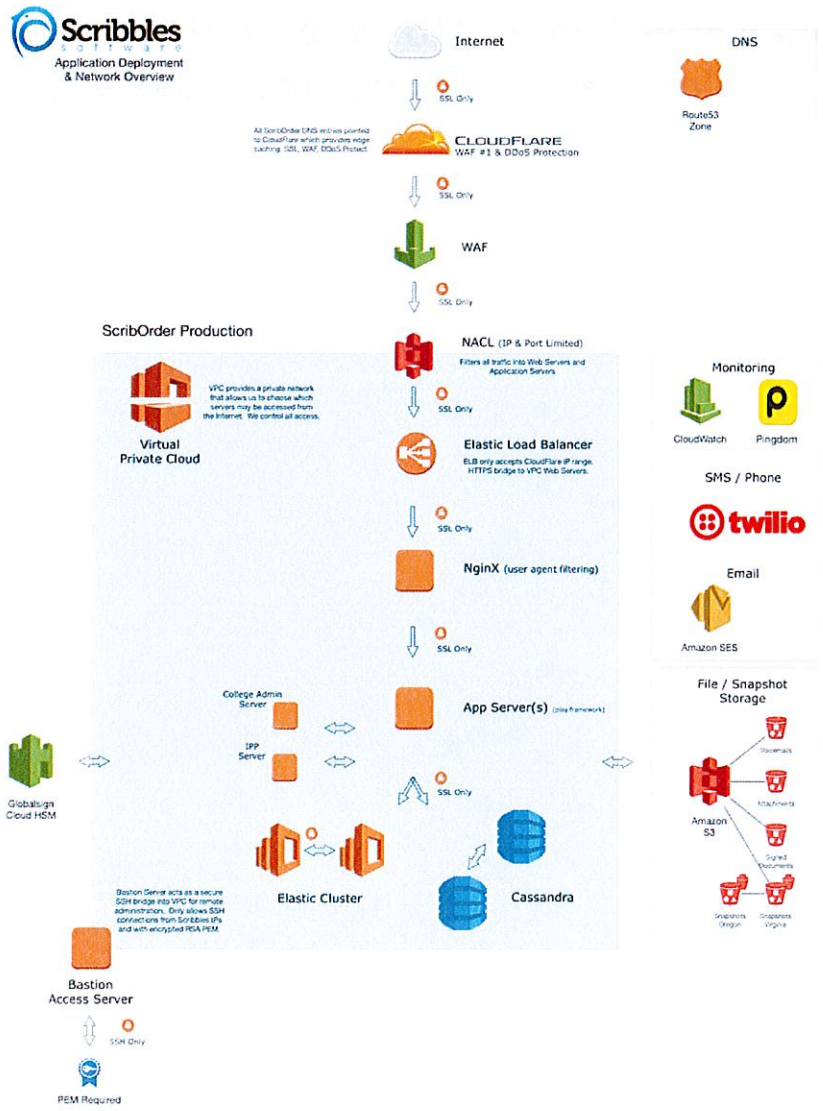
May 7, 2021

Attachment A - Permitium, LLC's Description of the Boundaries of Its School Management System and Law Enforcement Management System

Company Overview and Services Provided

Permitium provides a suite of Software as a Service (SaaS) document management solutions on a subscription basis. Clients contract to use organizational applications to enhance their business needs. Software offerings include the ability to provide electronic transcripts on request. There are also applications allowing students to choose which areas they wish to participate in as they progress through the school lifecycle. We are also able to help local law enforcement agencies with tasks they are mandated to perform such as Gun permit issuance and sex offender monitoring.

System Overview Illustration



Infrastructure

The Permitium, LLC application platform is hosted on the Amazon Web Services platform (AWS), a fully-managed Infrastructure as Service (IaaS) and Platform as a Service (PaaS) offering from Amazon, Inc. Amazon Web Service is developed and managed by the AWS team, and provides a cloud platform based on machine virtualization. This means that customer code deployed to the Web Service platform is securely delivered to the Permitium, LLC client community. Every physical node in AWS has one or more virtual machines, also called instances, that are scheduled on physical CPU cores, are assigned dedicated RAM, and have controlled access to local disk and network I/O.

Software

PermitDirector is a Software as a Service (SaaS) application developed and maintained by Permitium, LLC in-house software engineering group. The software engineering group enhances and maintains the Permitium platform to provide services to clients. Permitium software is not sold as an "on premises" solution. The Permitium web interface is a multi-user, web-based application that is used to collect inputs from users, process data and provide visual representations of key metrics to clients. It also provides some specific performance reports to help them manage their work with Permitium. To access the site, clients must complete the onboarding process and be provided credentials provisioned based on job duties.

People

Permitium, LLC organizational structure provides the framework for how organizational wide objectives are planned, executed, controlled, and monitored. A relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. Permitium, LLC develops an organizational structure contingent, in part, on its size and nature of activities.

The responsibilities of key positions within Permitium are clearly defined in documented job descriptions and communicated. Individuals that hold key positions are experienced, knowledgeable, and have lengthy tenure with the company. Permitium's organizational structure supports communication of information both up to leadership and down to support staff. Permitium's organizational structure comprises three primary business units and several groups that work together when delivering their SaaS platform.

The three business units consist of:

- Management Team is responsible for the oversight and monitoring of the organization's strategic direction and is responsible for making final decisions that are pushed down to the Leadership team and ultimately to Team members.
- Leadership Teams are responsible for the overall management, communications, direction, and implementation of the Management team's strategic direction. The

Leadership team is directly responsible for production and manages the quality of services.
- Team Members are responsible for executing on company tasks and managing the day-to-day service offerings of their respective departments.

Data

Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization. The data flow of Permitium's networks is restricted to their wide area network that consists of their internal network, hosted production systems, and certain site to site connections. The Permitium network is configured with Virtual Local Area Networks (VLANs) to provide increased segmentation between different customer environments. Remote access and administration is restricted via secure shell (SSH) connections and restricted to internal personnel of Permitium. Customers connect to their production site via Secure Sockets Layer (SSL) web connection.

- User organizations are responsible for defining the communications' method utilized to connect to Permitium's systems (e.g., direct connections, over public networks, etc.).
- User organizations are responsible for defining the communications' method that Permitium uses when connecting to their organization's internal network.
- User organizations are responsible for defining any encryption methodology utilized in relation to Permitium's services.

Processes and Procedures

Management has developed and communicated to clients procedures to restrict logical access to the Permitium platform and its data. Review of procedures is performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches. Selection, documentation, and implementation of security controls. Performance of annual management self-assessments to assess security controls. Authorization, changes to, and termination of information system access. Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

Attachment B - Permitium, LLC's Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Permitium, LLC designs its processes and procedures related to application development to meet its organizational objectives. Those objectives are based on the service commitments that applications contain the functional elements required by clients while maintaining maximum security controls adhering to the laws and regulations that govern student information services, and the financial, operational, and compliance requirements that Permitium, LLC has established for the services. Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the applications that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect client data both at rest and in transit

Permitium, LLC establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Permitium, LLC system policies and procedures, system design documentation, and contracts with clients. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Permitium, LLC application platform.

Criminal Justice Information Services (CJIS)

2021

PREPARED FOR Permitium, LLC.

Lazarus Alliance, Inc.
27743 N. 70th Street, Suite 10
Scottsdale, AZ 85266
888-896-7580 (p)
480-272-8846 (f)
www.lazarusalliance.com

Criminal Justice Information Services (CJIS) Security Policy Permitium, LLC.

04-15-2021

1 TABLE OF CONTENTS

04-15-2021

The Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy sets the minimum security requirements to provide an acceptable level of assurance to protect the full lifecycle of Criminal Justice Information. Agencies using cloud based services are required to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

This document outlines the specific security policies and practices for Permitium.com and how they are compliant with the CJIS Security Policy, version 5.8.

Permitium retains Lazarus Alliance, Inc., their independent auditors, 3PAOs, and CPAs, to continuously monitor and maintain their CJIS and SOC 2 Type 2 attestation reports. As the CJIS attestation is a confidential report, this Executive Summary will serve as affidavit to the completeness and compliance to the CJIS compliance requirements in their entirety.

Sincerely,

Michael D. Peters

eJD, MBA, C | CISO, CISSP, CRISC, CISA,

QSA, CMBA, CISM, SCPA, CCE, ISSA Hall of Fame

CEO Lazarus Alliance, Inc. - Proactive Cyber Security®

M: 1-762-822-4174 | O: 1-888-896-7580 x20

Lazarus Alliance is a proud veteran owned business.

SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) 800-53. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

CJIS

1. CONTACT INFORMATION AND REPORT DATE

1.1 CONTACT INFORMATION

Client	
▪ Company name:	Permitium, LLC.
▪ Company address:	P.O. Box 30012, #133 Laguna Niguel California 92607 United States
▪ Company URL:	https://www. permitium.com/
▪ Company contact name:	Jeff Maner
▪ Contact phone number:	910-722-9708
▪ Contact e-mail address:	jeff.maner@scribsoft.com
Assessor Company	
▪ Company name:	Lazarus Alliance, Inc.
▪ Company address:	27743 N 70th ST Suite 100 Scottsdale AZ 85266 United States
▪ Company website:	http://www.lazarusalliance.com
Assessor	
▪ Assessor name:	Dasharath Mane
▪ Assessor phone number:	1888-896-7580
▪ Assessor e-mail address:	Dasharath.Mane@lazarusalliance.com
Assessor Quality Assurance (QA) Primary Reviewer	
▪ QA reviewer name:	Jonathan Smith
▪ QA reviewer phone number:	1888-8967-580
▪ QA reviewer e-mail address:	Jonathan.Smith@lazarusalliance.com

1.2 DATE AND TIMEFRAME OF ASSESSMENT

▪ Date of Report:	04-15-2021
▪ Timeframe of assessment (start date to completion date):	05-01-2020 - 04-30-2021
▪ Identify date(s) spent onsite at the entity:	Remote Assessment
▪ Descriptions of time spent onsite at the entity and time spent performing remote assessment activities, including time spent on validation of remediation activities.	Lazarus Alliance, Inc. performs remote assessment activities with the client each month reviewing artifacts, collecting evidence, collaborating with employees and maintaining the overall assessment status. In addition, our review included the hosting companies System and Organization Controls 2 (SOC 2) Type 2 Report

2 CJIS OVERVIEW

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following detail provides an abstract representation of the information within scope and the categories of consideration.

2.1 CRIMINAL JUSTICE INFORMATION (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

- **Biometric Data**: data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
- **Identity History Data:** textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
- **Biographic Data:** information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
- **Property Data:** information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
- **Case/Incident History:** information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules.

2.2 CJIS PROGRAM OVERVIEW

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances.

The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security
- Policy Area 13—Mobile Devices

3 CJIS CONTROL SUMMARY

While the CJIS Security Policy has its genesis in federal guidelines, specifically the NIST Special Publication 800-53, those requirements have been shaped by the shared management philosophy of the APB process in which each local, state, tribal, and federal law enforcement agency are stakeholders. Additionally, noncriminal justice agencies (NCJAs) follow the same standard when accessing civil information for authorized purposes.

The following table illustrates each policy area and the corresponding NIST

Special Publication 800-53 control. All areas in green are considered compliant or out of scope and those in red to be considered not compliant.

CSP v5.8	Area Requirement Compliance Status	Compliance Status
5.1	Information Exchange Agreements Policy Area 1	
5.1.1	Information Exchange	**Compliant**
5.1.1.1	Information Handling	**Compliant**
5.1.1.2	State and Federal Agency User Agreements	**Compliant**
5.1.1.3	Criminal Justice Agency User Agreements	**Compliant**
5.1.1.4	Inter-Agency and Management Control Agreements	**Compliant**
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum	**Compliant**
5.1.1.6	Agency User Agreements	**Compliant**
5.1.1.7	Outsourcing Standards for Channelers	**Compliant**
5.1.1.8	Outsourcing Standards for Non-Channelers	**Compliant**
5.1.2	Monitoring, Review, and Delivery of Services	**Compliant**
5.1.2.1	Managing Changes to Service Providers	**Compliant**
5.1.3	Secondary Dissemination	**Compliant**
5.1.4	Secondary Dissemination of Non-CHRI CJI	**Compliant**
5.2	Security Awareness Training Policy Area 2	
5.2.1	Awareness Topics	**Compliant**
5.2.1.1	Level One Security Awareness Training	**Compliant**
5.2.1.2	Level Two Security Awareness Training	**Compliant**
5.2.1.3	Level Three Security Awareness Training	**Compliant**
5.2.1.4	Level Four Security Awareness Training	**Compliant**
5.2.2	Security Training Records	**Compliant**
5.3	Incident Response Policy Area 3	
5.3.1	Reporting Information Security Events	**Compliant**
5.3.1.1.1	FBI CJIS Division Responsibilities	**Compliant**
5.3.1.1.2	CSA ISO Responsibilities	**Compliant**
5.3.2	Management of Security Incidents	**Compliant**
5.3.2.1	Incident Handling	**Compliant**
5.3.2.2	Collection of Evidence	**Compliant**
5.3.3	Incident Response Training	**Compliant**
5.3.4	Incident Monitoring	**Compliant**
	Auditing and Accountability	

5.4	Policy Area 4	
5.4.1	Auditable Events and Content (Information Systems)	**Compliant**
5.4.1.1	Events	**Compliant**
5.4.1.1.1	Content	**Compliant**
5.4.2	Response to Audit Processing Failures	**Compliant**
5.4.3	Audit Monitoring, Analysis, and Reporting	**Compliant**
5.4.4	Time Stamps	**Compliant**
5.4.5	Protection of Audit Information	**Compliant**
5.4.6	Audit Record Retention	**Compliant**
5.4.7	Logging NCIC and III Transactions	**Compliant**
5.5	Access Control Policy Area 5	
5.5.1	Account Management	**Compliant**
5.5.2	Access Enforcement	**Compliant**
5.5.2.1	Least Privilege	**Compliant**
5.5.2.2	System Access Control	**Compliant**
5.5.2.3	Access Control Criteria	**Compliant**
5.5.2.4	Access Control Mechanisms	**Compliant**
5.5.3	Unsuccessful Login Attempts	**Compliant**
5.5.4	System Use Notification	**Compliant**
5.5.5	Session Lock	**Not Compliant**
5.5.6	Remote Access	**Compliant**
5.5.6.1	Personally Owned Information Systems	**Compliant**
5.5.6.2	Publicly Accessible Computers	**Compliant**
5.6	Identification and Authentication Policy Area 6	
5.6.1	Identification Policy and Procedures	**Compliant**
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	**Compliant**
5.6.2	Authentication Policy and Procedures	**Compliant**
5.6.2.1	Standard Authenticators	**Compliant**
5.6.2.1.1	Password	**Compliant**
5.6.2.1.2	Personal Identification Number (PIN)	**Compliant**
5.6.2.1.3	One-time Passwords (OTP)	**Compliant**
5.6.2.2	Advanced Authentication	**Compliant**
5.6.2.2.1	Advanced Authentication Policy and Rationale	**Compliant**
5.6.2.2.2	Advanced Authentication Decision Tree	**Compliant**
5.6.3	Identifier and Authenticator Management	**Compliant**
5.6.3.1	Identifier Management	**Compliant**
5.6.3.2	Authenticator Management	**Compliant**

5.6.4	Assertions	**Compliant**
5.7	Configuration Management Policy Area 7	
5.7.1	Access Restrictions for Changes	**Compliant**
5.7.1.1	Least Functionality	**Compliant**
5.7.1.2	Network Diagram	**Compliant**
5.7.2	Security of Configuration Documentation	**Compliant**
5.8	Media Protection Policy Area 8	
5.8.1	Media Storage and Access	**Compliant**
5.8.2	Media Transport	**Compliant**
5.8.2.1	Digital Media in Transit	**Compliant**
5.8.2.2	Physical Media in Transit	**Compliant**
5.8.3	Digital Media Sanitization and Disposal	**Compliant**
5.8.4	Disposal of Physical Media	**Compliant**
5.9	Physical Protection Policy Area 9	
5.9.1	Physically Secure Location	**Compliant**
5.9.1.1	Security Perimeter	**Compliant**
5.9.1.2	Physical Access Authorizations	**Compliant**
5.9.1.3	Physical Access Control	**Compliant**
5.9.1.4	Access Control for Transmission Medium	**Compliant**
5.9.1.5	Access Control for Display Medium	**Compliant**
5.9.1.6	Monitoring Physical Access	**Compliant**
5.9.1.7	Visitor Control	**Compliant**
5.9.1.8	Delivery and Removal	**Compliant**
5.9.2	Controlled Area	**Compliant**
5.1	Systems and Communications Protection and Information Integrity Policy Area 10	
5.10.1	Information Flow Enforcement	**Compliant**
5.10.1.1	Boundary Protection	**Compliant**
5.10.1.2	Encryption	**Compliant**
5.10.1.2.1	Encryption for CJI in Transit	**Compliant**
5.10.1.2.2	Encryption for CJI at Rest	**Compliant**
5.10.1.2.3	Public Key Infrastructure (PKI) Technology	**Compliant**
5.10.1.3	Intrusion Detection Tools and Techniques	**Compliant**
5.10.1.4	Voice over Internet Protocol	**Compliant**
	Systems and Communications Protection and Information Integrity (continued)	**Compliant**
5.10.1.5	Cloud Computing	**Compliant**

5.10.2	Facsimile Transmission of CJI	**Compliant**
5.10.3	Partitioning and Virtualization	**Compliant**
5.10.3.1	Partitioning	**Compliant**
5.10.3.2	Virtualization	**Compliant**
5.10.4	System and Information Integrity Policy and Procedures	**Compliant**
5.10.4.1	Patch Management	**Compliant**
5.10.4.2	Malicious Code Protection	**Compliant**
5.10.4.3	Spam and Spyware Protection	**Compliant**
5.10.4.4	Security Alerts and Advisories	**Compliant**
5.10.4.5	Information Input Restrictions	**Compliant**
5.11	Formal Audits Policy Area 11	
5.11.1	Audits by the FBI CJIS Division	**Compliant**
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	**Compliant**
5.11.1.2	Triennial Security Audits by the FBI CJIS Division	**Compliant**
5.11.2	Audits by the CSA	**Compliant**
5.11.3	Special Security Inquiries and Audits	**Compliant**
5.11.4	Compliance Subcommittees	**Compliant**
5.12	Personnel Security Policy Area 12	
5.12.1	Personnel Security Policy and Procedures	**Compliant**
5.12.1.1	Minimum Screening Requirements for Individuals Requiring Access to CJI	**Compliant**
5.12.1.2	Personnel Screening for Contractors and Vendors	**Compliant**
5.12.2	Personnel Termination	**Compliant**
5.12.3	Personnel Transfer	**Compliant**
5.12.4	Personnel Sanctions	**Compliant**
5.13	Mobile Devices Policy Area 13	
5.13.1	Wireless Communications Technologies	**Compliant**
5.13.1.1	802.11	**Compliant**
5.13.1.2	Cellular Devices	**Compliant**
5.13.1.2.1	Cellular Service Abroad	**Compliant**
5.13.1.2.2	Voice Transmissions Over Cellular Devices	**Compliant**
5.13.1.3	Bluetooth	**Compliant**
5.13.1.4	Mobile Hotspots	**Compliant**
5.13.2	Mobile Device Management (MDM)	**Compliant**
5.13.3	Wireless Device Risk Management	**Compliant**
5.13.4	System Integrity	**Compliant**
5.13.4.1	Patching/Updates	**Compliant**

5.13.4.2	Malicious Code Protection	**Compliant**
5.13.4.3	Personal Firewall	**Compliant**
5.13.5	Incident Response	**Compliant**
5.13.6	Access Control	**Compliant**
5.13.7	Identification and Authentication	**Compliant**
5.13.7.1	Local Device Authentication	**Compliant**
5.13.7.2	Advanced Authentication	**Compliant**
5.13.7.2.1	Compensating Controls	**Compliant**
5.13.7.3	Device Certificates	**Compliant**

For a more detailed technical review, please reference the CJIS-SSP-2021_1618462284-permitium.PDF CJIS SSP attestation report.