Data Protection Assessment

IT Cloud Provider | Cloud Hosting System

vendiligence™

Vendor Profile

IT Cloud Provider

Product
Cloud Hosting System

Assessment Date
09/12/2023

Service Description
The Vendor was noted as providing the following service(s): IT Cloud Provider - Cloud Hosting System

Domain URL
itcloudprovider.com

Vendor Type/Industry
Cloud Hosting

Vendiligence™ Overall Rating

SATISFACTORY

Vendor appears to maintain a partially well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear satisfactory.

Vendor Inherent Risk Profile Summary

Risk Summary Rating
HIGH

YES Personally Identifiable Information (PII)

YES Protected Health Information (ePHI)

YES Cardholder Data (CHD)

YES Client Data

Section Rating Summary

Data Privacy
LOW

Security Testing
LOW

Information Security Governance
MEDIUM

Sensitive Data Security
MEDIUM

Resiliency
LOW

Business Continuity
LOW

Report Comments and Recommendations

Vendor stated that Personally Identifiable Information (PII), Card Holder Data (CHD) and Protected Health Information (ePHI) is involved in the use of this product/service. Client is encouraged to request evidence that Vendor has a documented Third Party Vendor Management/Due Diligence program in place. Client is encouraged to request evidence that Vendor has a documented PII Retention Policy in place as well as someone in leadership acting in the capacity of a Chief Information Security Officer. Vendor did not provide adequate evidence that data is encrypted in transit or at rest. Client is encouraged to request documentation surrounding current encryption methods. Client is encouraged to request information surrounding the following data security controls we would expect to see: DDoS Mitigation, Wireless Access Controls, Data Classification, Media Sanitization, Breach Notification, Environment Segmentation, and MFA for administrative access. Client is encouraged to request evidence that environmental equipment is properly maintained and serviced regularly.

Data Protection Assessment

IT Cloud Provider | Cloud Hosting System

vendiligence™

Legend			
	A positive or affirmative response to the control category was provided by the vendor.	N/P	A response was not provided to the control category by the vendor.
	A negative or insufficient response to the control category was provided by the vendor.	N/A	The control category is not applicable to the scope of the assessment.

Risk Profile — Regulation Mapping — **HIGH**

Type of customer/consumer data involved in this product:

- YES Name
- YES Address
- YES Telephone Number
- YES Email Address
- YES Date of birth
- YES Social Security Number
- YES Drivers License Number
- YES Taxpayer Identification
- YES Account Number(s)
- YES Cardholder Data (CHD)
- YES Personally Identifiable Information (PII)
- YES Protected Health Information (ePHI)
- Other (please specify) NA

Type of client data involved with this product:

- NO Internal Policies/Documentation
- YES Non-Public Business Plans
- YES Non-Public Financial Information
- NO Non-Public Product/Service Information
- Other Types of Client Data (please specify): Employee Records

Experience with the function outsourced: 13 years

Critical Subservice Organizations and services provided:

ServiceCore - Provides call center and consumer services

- NO Client data stored outside the USA
- NO Services provided from outside the USA

Product hosted/installed: ☑ Vendor Location

Assessment Of Controls

This assessment identifies key risks to your organization's operations, assets, and customers, posed by current and potential vendors. Each control within this assessment ties back to relevant industry guidance and standards addressing vendor risk, allowing key decision makers to confidently weigh vulnerabilities introduced by vendors and respond to the resulting risks.

Data Protection Assessment

IT Cloud Provider | Cloud Hosting System

vendiligence™

Data Privacy

Regulation Mapping

LOW

- YES Provides notice to data subject about its privacy practices
- N/P Data Protection Officer
- YES Obtains consent from data subjects where required
- YES Collects Accurate, Up-to-Date, Complete, and Relevant PII
- YES Able to Display an Individual's Data and Who It's Shared With
- YES Able to Export an Individual's Data in a Common Format
- YES Able to Update/Correct an Individual's Data
- YES Able to Exempt an Individual's Data from Sharing/Selling
- YES Able to exempt an individual from automated decisions
- YES Able to delete an individual's data
- YES Able to delete or return all PII at contract termination
- YES Process in place for handling privacy requests (DSARS)
- YES Vendor maintains a data privacy code of conduct
- YES Persons interacting with sensitive data sign a confidentiality agreement
- YES Persons interacting with sensitive data receive privacy training
- YES Data is only used for contracted purpose
- YES Data is not shared with a fourth party without consent
- N/P Records of processing activities are maintained
- YES Vendor allows for full cooperation in audits for clients
- YES Data breach notification/unauthorized disclosures of PII are tracked
- YES Data is pseudonymized/de-identified
- YES Data is masked where appropriate

Security Testing

Regulation Mapping

LOW

- NO Penetration tests are performed by internal staff
- YES Penetration tests are performed by a third party
- YES Any Medium or higher findings identified during the penetration tests are remediated timely
- NO Application security tests are performed by internal staff
- YES Application security tests are performed by a third party
- YES Any Medium or higher findings identified during the application tests are remediated timely
- YES Vulnerability scans/tests are performed by internal staff
- YES Vulnerability scans/tests are performed by a third party
- YES Any Medium or higher findings identified during the vulnerability tests are remediated timely
- YES Social engineering or phishing performed

Frequency of social engineering tests

Monthly

Frequency of social engineering tests (other)

NA

Information Security Governance

Regulation Mapping

MEDIUM

Formal Programs or Policies

- YES Information Security
- YES Incident Management
- YES Change Management
- YES Risk Management
- YES Mobile Device/BYOD
- YES Asset Management - Hardware
- YES Asset Management - Software
- NO Vendor Management/Due Diligence
- YES Client Data Destruction Post-Contract
- YES Evidence of Insurance

Represented Practices

- YES Employee/Contractor Background Checks
- NO PII Retention Policy
- YES Employee/Contractor Security Training
- YES Board/Executive/Senior Management Involvement
- NO Designated Chief Information Security Officer (CISO)
- YES Patch Management

Sensitive Data Security	Regulation Mapping	MEDIUM

N/P Encryption at Rest	NO Wireless Access Control	NO Media Sanitization
N/P Encryption in Transit	YES Secure Device Baselining	YES Principle of Least Privilege
YES Logical Access Management	YES Remote Access Requires Multifactor Authentication	YES Separation of Duties
NO DDoS Mitigation	NO Data Classification	

Incident Detection and Response	YES IDS/IPS	NO Breach Notification
	YES Event Log Correlation and Analysis	YES Periodic Logical Access Review/Termination
	YES Network Segmentation	
	YES Antimalware	
Vendor Software/Application Security	YES Web application firewall	YES Third parties do not maintain access to dev/prod
	YES Designated security personnel involved in SDLC	NO Production and development environment segmentation
	YES Security testing is part of build verification	
Password Policy For Employee Access	NO Multifactor authentication for administrative access	
Password Policy For Client Access	YES Multifactor authentication available for client access	

Resiliency

Regulation Mapping | LOW

The following resiliency controls or better are in place for Vendor's primary data center	YES Generators (with redundancy)	YES Uninterruptable Power Supplies (with redundancy)
	YES Cooling & Conditioning System (with redundancy)	YES Redundant Internet Connectivity
The following system monitoring and supporting controls are in place	YES Fire Detection	YES Fire System Maintenance
	YES Fire Suppression	NO Cooling & Conditioning System Maintenance
	NO Generator Maintenance	YES Network Monitoring
	NO Uninterruptable Power Supply Maintenance	YES Temperature and Humidity
The following data resiliency controls are in place for production data	YES Primary Site Backups	YES Monitored Alerts on Failed Backups
	YES Offsite/Offline Backups	NO Backup Media Encrypted
	YES Backups Tested Annually	
Physical Security	YES Electronic Access Control	YES Visitor Tracking
	YES Multifactor Authentication for Physical Access	NO Security Guards
	YES Physical Access is Reviewed	YES Camera System

Business Continuity

Regulation Mapping | LOW

Overview

YES Vendor has documented Business Continuity Plan (BCP)

YES Vendor has documented Disaster Recovery Plan (DRP)

NO Board of Directors or Senior Management provides oversight of the BCP

YES Plans undergo ongoing maintenance

YES Are employees trained on Business Continuity and Disaster Recovery

Briefly describe documented process for service interruption or degradation

Vendor provided a documented step by step service interruption plan that includes a call tree, POCs and actionable steps to continue to deliver service through an interruption. The plan is distributed and available to all necessary groups and is review upon hiring (for applicable roles) and re-reviewed and signed off on annually. The plan also includes notification parameters as appropriate.

Business Continuity Plan Testing

YES A Business Impact Analysis is performed

YES RTO Tested & Met

Recovery Time Objective (RTO) and Comments: >72 hours

YES RPO Tested & Met

Recovery Point Objective (RPO) and Comments: >24 hours

	Frequency of testing	Last tested	Remediated
BCP	Annually	2/10/2023	5/3/2023
DRP	Annually	2/10/2023	5/3/2023

YES Distance between primary and alternate locations is appropriate

An alternative data center is available with the configuration of Warm

Disclaimer

It should be noted that it is the responsibility of the Board of Directors to determine whether the organization agrees with the opinion-based risk level expressed in this report.

All information contained in this assessment is the work product of the Venminder, Inc. Information Security Operations Team. Documents listed as Resources Utilized have been reviewed and assessed by an Information Security Subject Matter Expert and this assessment has been reviewed and approved for distribution. For more information on Venminder's Subject Matter Experts, please click here.

The objective of this Assessment is to assess a third party's general controls relating to their ongoing ability to protect data and deliver the products and services for which you have contracted. This assessment is not intended for, nor should it be used for, the purpose of assessing the third party's likelihood of suffering a data breach, attack, or other business impacting event causing the inability to provide contracted services, nor as a guarantee the vendor will follow any assessed plan or meet specified objectives. This Assessment is intended solely for the information and use by the client and is not intended to be and should not be used by anyone else other than the objectives listed herein.

Rating Explanation

LOW	Vendor appears to maintain a well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear appropriate.
MEDIUM	Vendor appears to maintain a partially well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear satisfactory.
HIGH	Vendor does not appear to maintain, or has provided insufficient evidence of, a well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear insufficient and/or introduce a cautionary level of risk.
SEVERE	Vendor does not appear to maintain, or has provided insufficient evidence of, a well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear insufficient and/or introduce a severe level of risk.

Industry Guidance and Standards Utilized

This assessment was developed using the following industry guidance and standards.

INDUSTRY GUIDANCE AND STANDARDS	MAPPING REFERENCE
AICPA Trust Services Criteria	TSC-*
California Consumer Privacy Act	CCPA-*
California Privacy Rights Act	CPRA.**
Canadian Personal Information Protection and Electronic Documents Act	PIPEDA.*
Center for Internet Security - Critical Security Controls v8	CSC-*
China Personal Information Protection Law	PIPL.*
Colorado Privacy Act	CPA.**
Connecticut Data Privacy Act	CTDPA.**
EU General Data Protection Regulation	GDPR-*
FFIEC IT Examination Handbook - Wholesale Payment Systems Booklet	WPS.**
FFIEC IT Examination Handbook - Audit Booklet	AUD.**
FFIEC IT Examination Handbook - Business Continuity Booklet	BCP.**
FFIEC IT Examination Handbook - Information Security Booklet	IS.**
FFIEC IT Examination Handbook - Management Booklet	MGT.**
FFIEC IT Examination Handbook - Operations Booklet	OP.**
FFIEC IT Examination Handbook - Outsourcing Technology Services	OT.**
FINRA Report on Cybersecurity Practices	FINRA-pg*
Health Insurance Portability and Accountability Act	HIPAA-*
Interagency Guidelines Establishing Information Security Standards	12CFR-**
Interagency Guidance on Third-Party Relationships (Board, FDIC, & OCC) 06.2023	TPRM.*
ISO/IEC 27001:2022	ISO.*
New York Department of Financial Services - 23 NYCRR 500	NYCRR-*
NIST Framework for Improving Critical Infrastructure Cybersecurity version 1.1	CSF.*
NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations	800-53-r5-**
NIST SP 800-63b Digital Identity Guidelines	800-63b.**
OCC 2021-36	OCC20**-**
SEC Regulation SCI reference to NIST 800-53 Rev. 4	800-53-**