August 20, 2021

Chinstrap Penguin Corp
1234 Beach View Avenue
Las Vegas, NV 89103

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an Authorized External Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST® CSF Assurance Program requirements, the following platform, facilities and supporting infrastructure of the Organization ("Scope") meet the HITRUST CSF® v9.1 certification criteria:

Platforms:

- Customer Central (a.k.a. "Portal") residing at Pelican Data Center

Facilities:

- Pelican Data Center located in Salt Lake City, Utah, United States of America
- CP Headquarters and Manufacturing located in Las Vegas, Nevada, United States of America
- CP Framingham Manufacturing Facility located in Framingham, Massachusetts, United States of America

The certification is valid for a period of two years assuming the following occurs:

- A monitoring program is in place to determine if the controls continue to operate effectively over time
- Annual progress is being made on areas identified in the Corrective Action Plan(s) (CAPs)
- No data security breach reportable to a federal or state agency by law or regulation has occurred
- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST CSF certification criteria
- Timely completion of the interim assessment as defined in the HITRUST CSF Assurance Program Requirements

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail, and clarity relating to information protection. With input from leading organizations, HITRUST identified a subset of the HITRUST CSF control requirements that an organization must meet to be HITRUST CSF Certified. For certain HITRUST CSF control requirements that were not being met, the Organization developed a CAP that outlined its plans for meeting such requirements.

HITRUST performed a quality assurance review to ensure that the control maturity scores were consistent with the results of testing performed by the Authorized External Assessor. Users of this letter can refer to the document Leveraging HITRUST CSF Assessment Reports: A Guide for New Users for questions on interpreting this letter and can contact HITRUST customer support at support@hitrustalliance.net. Users of this letter are assumed to be familiar with and understand the services provided by the organization listed above and what specific services are being used by the user organization.

A full HITRUST CSF Validated Assessment Report has been issued by HITRUST and can be requested from the organization listed above. Additional information on the HITRUST CSF Assurance Program can be found on the HITRUST website at https://hitrustalliance.net.

HITRUST

HITRUST

Enclosures (2):

- Assessment Context
- Scope of the Assessment

Assessment Context

The assessed entity completed the following tailoring questionnaire to derive this assessment's customized set of HITRUST CSF requirements based on organizational, geographical, systematic, and regulatory risk factors.

Assessment Type
HITRUST CSF Security Assessment

General Factors	
Organization Type	Service Provider (Non-IT)
Entity Type	Non-Healthcare

Geographic Factors	
Geographic scope of operations considered	Multi-State

Organizational Risk Factors	
Number of Records that are currently held	Between 10 and 60 Million Records

Systematic Risk Factors	
Is the system(s) accessible from the Internet?	Yes
Is the scoped system(s) (on-premise or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?	No - The systems are only accessible by internal resources. Data is not shared and there is no direct third party access.
Does the system(s) transmit or receive data with a third party/business partner?	Yes
Is the system(s) accessible from a public location?	No - There are no publicly positioned systems in the environment or on Chinstrap's devices. Data is not shared and there is no third party access.
Number of interfaces to other systems	25 to 75
Number of users of the system(s)	Fewer than 500
Number of transactions per day	6,750 - 85,000
Is any aspect of the scoped environment hosted on the cloud?	No – No aspect of the scoped environment is hosted on the cloud.
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No - There are no dial up options in the environment or on any Chinstrap devices.
Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - There are no fax machines in the environment or fax capabilities on any Chinstrap devices.

Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - All Chinstrap employees work in the identified facilities and none of them travel to areas considered to be of significant risk.
Are hardware tokens used as an authentication method within the scoped environment?	No - There are no hardware tokens used within Chinstrap's in-scope environment.
Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	Yes
Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	Yes
Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)?	No - None of the in-scope systems leverage or require the use of e-signatures.
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	Yes
Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?	Yes
Are wireless access points in place at any of the organization's in-scope facilities?	Yes
Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	Yes

Regulatory Risk Factors
Subject to State of Massachusetts Data Protection Act
Subject to the State of Nevada Security of Personal Information Requirements

Scope of the Assessment

Company Background

Chinstrap Penguin Corp is a manufacturer, retailer, and distributor of widgets for use in the care, feeding, and housing of all Antarctic Chinstrap Penguins. Chinstrap Penguin Corp, established in 2005, has grown to be one of the largest widget producers in the world and now offers a number of specialized widgets to its customers and third-party distributors. In 2014 Chinstrap Penguin Corp entered the gadget market by acquiring Gadget Group and is now the third largest gadget manufacturer in the United States.

In-scope Platforms and Facilities

The following tables present the platforms and facilities that were included in the scope of this assessment.

Platform	Application(s)	Database(s)	Operating System(s)	Residing Facility	Exclusions from Scope
Customer Central (a.k.a. "Portal")	Penguin Nest, Penguin Analytics, South Pole Benefits Eligibility	Oracle	HP-UX	Pelican Data Center	Content and applications from customer systems that are delivered via the Portal are outside the scope of this assessment. This includes customers who choose to leverage the embedded credit card processing page, which is offered as an add-on service. The embedded credit processing page is provided and managed by a third-party service provider.

Description of the Platform

The Portal is a platform that allows numerous applications and service offerings to be accessed by customers via a single web-based interface via a browser. It does this for numerous customers and allows their customers to obtain information in a single location. Chinstrap Penguin personnel access the Portal through a secure VPN to a bastion host. From the bastion host systems administrators connect via VDI to an administrative console for management of all in-scope applications and supporting infrastructure.

The Portal is developed by Chinstrap Penguin personnel. It is built in Java and .Net. The solution leverages VMWare for scalability. The applications/service offerings that make up the Portal are Penguin Nest, Penguin Analytics, and South Pole Benefit Eligibility.

- Penguin Nest is an application that delivers content and applications from customer systems via the Portal. The application collects and feeds critical metrics to Penguin Analytics.
- Penguin Analytics is an application that delivers reporting and analytics capability to customers. It allows them to develop dashboards and reports and track KPIs with their information that is stored within the Portal.
- South Pole Benefits Eligibility allows our customers to provide benefit eligibility information so that users of the system have a single place to go to get the eligibility information from multiple customers. Meta data from the application is fed to Penguin Analytics for further analysis by customers.

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
Pelican Data Center	Data Center	Yes	Pelican Hosting	Salt Lake City	UT	United States of America
CP Headquarters and Manufacturing	Office	No	N/A	Las Vegas	NV	United States of America
CP Framingham Manufacturing Facility	Other	No	N/A	Framingham	MA	United States of America

Services Outsourced

The following table presents outsourced services relevant to the scope of this assessment.

Third-party Provider	Relevant Service(s) Provided
Pelican Hosting	Pelican Hosting provides a colocation facility where Chinstrap Penguin maintains a dedicated cage. Pelican Hosting personnel do not have logical access to any in-scope systems.

Overview of the Security Organization

Chinstrap's information security function is housed under the larger information technology department. The information security function is led by the CISO who reports to the CIO. The information security function has developed a robust information security program focused on managing information security risk. Key elements of the program include:

- Risk management
- Network security
- Application security
- Physical security
- Business continuity and disaster recovery
- Incident management
- Identity and access management
- Compliance management
- Security training and awareness