Letter of HITRUST Risk-based, 2-year (r2) Certification

August 20, 2024

Chinstrap Penguin Corporation
123 Main Street
Anytown, TX 12345

HITRUST has developed the HITRUST CSF, a certifiable security and privacy framework which incorporates information protection requirements based on input from leading organizations. HITRUST identified a subset of the HITRUST CSF requirements that an organization must meet to be HITRUST Risk-based, 2-year (r2) Certified for a defined assessment scope. Chinstrap Penguin, Inc. ("the Organization") has chosen to perform a HITRUST CSF v11.4 r2 validated assessment utilizing a HITRUST Authorized External Assessor Organization ("External Assessor").

Scope

The following platforms of the Organization were included within the scope of this assessment ("Scope") which included a review of the referenced facilities and supporting infrastructure for the applicable information protection requirements:

Platform:

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

Facilities:

- CP Framingham Manufacturing Facility (Other) managed internally located in Framingham, Massachusetts, United States of America
- CP Headquarters and Manufacturing (Other) managed internally located in Las Vegas, Nevada, United States of America
- Pelican Data Center (Data Center) managed by Pelican Hosting located in Salt Lake City, Utah, United States of America

Certification

The Organization has met the criteria specified as part of the HITRUST Assurance Program to obtain a HITRUST r2 validated assessment report with certification ("Certification") for the Scope. Certification is awarded based on each domain's average maturity score meeting a minimum score. Within each domain the maturity scores for each requirement statement were validated by an External Assessor and the assessment was subjected to quality assurance procedures performed by HITRUST.

The Certification for the Scope is valid for a period of two years from the date of this letter assuming the following occurs. If any of these criteria are not met, HITRUST will perform an investigation to determine ongoing validity of the certification and reserves the right to revoke the Organization's certification.

- No security events resulting in unauthorized access to the assessed environment or data housed therein, including any data security breaches occurring within or affecting the assessed environment reportable to a federal or state agency by law or regulation

- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST r2 certification criteria specified as part of the HITRUST Assurance Program.

Users of this letter can contact HITRUST customer support (*support@hitrustalliance.net)* for questions on using this letter.

The Organization's Assertions

Management of the Organization has provided the following assertions to HITRUST:

- The Organization has acknowledged that, as members of management, they are responsible for the information protection controls implemented as required by the HITRUST.

- The Organization has implemented the information protection controls as described within their assessment.

- The Organization maintains the information security management program via monitoring, review, and periodic re-assessments of the information protection controls.

- The Organization has responded honestly, accurately, and completely to inquiries made throughout the assessment process and certification lifecycle.

- The Organization has provided the External Assessor with accurate and complete records and necessary documentation related to the information protection controls included within the scope of its assessment.

- The Organization has disclosed all design and operating deficiencies in its information protection controls of which is it aware throughout the assessment process, including those where it believes the cost of corrective action may exceed the benefits.

- No events or transactions have occurred or are pending that would have an effect on the assessment that was performed and used as a basis by HITRUST for issuing the report.

- There have been no communications from regulatory agencies concerning noncompliance with or deficiencies regarding the information protection controls that are included within the Scope of this assessment.

External Assessor Responsibilities

External Assessors are authorized by HITRUST based upon a thorough vetting process to demonstrate their ability to perform HITRUST CSF assessments, and individual practitioners are required to maintain appropriate credentials based upon their role on HITRUST assessments. In HITRUST r2 validated assessments the External Assessor is responsible for:

- Reviewing and gaining a detailed understanding of the information provided by the Organization.

- Performing sufficient procedures to validate the control maturity scores provided by the Organization.

- Meeting all HITRUST Assessment criteria described within the HITRUST Assessment Handbook.

HITRUST Responsibilities

HITRUST is responsible for maintenance of the HITRUST CSF and HITRUST Assurance Program against which the Organization and an External Assessor completed this assessment.

HITRUST performed a quality assurance review of this assessment to support that the control maturity scores were consistent with the results of testing performed by the External Assessor. HITRUST's quality assurance review incorporated a risk-based approach to substantiate the External Assessor's procedures were performed in accordance with the requirements of the HITRUST Assurance Program.

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

Limitations of Assurance

The HITRUST Assurance Program is intended to gather and report information in an efficient and effective manner. The assessment is not a substitute for a comprehensive risk management program but is a critical data point in risk analysis. The assessment should also not be a substitute for management oversight and decision-making but, again, leveraged as a key input.

HITRUST

Enclosures (2):

- Assessment Context
- Scope of Systems in the Assessment

Assessment Context

About the HITRUST r2 Assessment and Certification

The HITRUST r2 assessment provides the highest level of information protection and compliance assurance. It is the most comprehensive and robust HITRUST certification, and can be optionally tailored to include coverage for additional authoritative sources such as HIPAA, the NIST Cybersecurity Framework, and GDPR.

The HITRUST r2 assessment is an evolving, threat-adaptive assessment with an accompanying certification. HITRUST r2 assessments leverage threat intelligence data and best practice controls to deliver an assessment that addresses relevant practices and active cyber threats. To do this, HITRUST continually evaluates cybersecurity controls to identify those relevant to mitigating known risks using cyber threat intelligence data from leading threat intelligence providers. Therefore, the HITRUST r2 includes controls that exclusively address emerging cyber threats actively being targeted today.

Assessment Approach

An *Authorized HITRUST External Assessor Organization* (the "External Assessor") performed validation procedures to measure the control maturity of the HITRUST CSF requirements and corresponding evaluative elements included in this assessment for the scope of the assessment. These validation procedures were designed by the External Assessor based upon the assessment's scope in observance of HITRUST's CSF Assurance Program Requirements and consisted of inquiry with key personnel, inspection of evidence (e.g. access lists, logs, configuration, sample items, policies, procedures, diagrams), on-site or virtual observations, (optionally) utilization of the work of others (as described elsewhere in this report), and (optionally) reperformance of controls.

Each requirement in the HITRUST CSF contains one or more evaluative elements. For example, requirement 0322.09u2Organizational.12, which reads "Media is encrypted when onsite unless physical security can be guaranteed, and always when offsite.", contains the following two evaluative elements: "1. The organization restricts the use of writable, removable media in organizational systems" and "2. The organization restricts the use of personally owned, removable media in organizational systems". The implementation and operation of all evaluative elements associated with applicable HITRUST CSF requirements included in the assessment was evaluated by the External Assessor in reaching an implementation score.

Implementation Score	Description	Points Awarded
Not compliant- (NC)	Very few if any of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment. Rough numeric equivalent of 0% (point estimate) or 0% to 10% (interval estimate).	0

Implementation Score	Description	Points Awarded
Somewhat compliant (SC)	Some of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 25% (point estimate) or 11% to 32% (interval estimate).	25
Partially compliant (PC)	About half of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 50% (point estimate) or 33% to 65% (interval estimate).	50
Mostly compliant (MC)	Many but not all of the evaluative elements in HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 75% (point estimate) or 66% to 89% (interval estimate).	75
Fully compliant (FC)	Most if not all of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 100% (point estimate) or 90% to 100% (interval estimate).	100

Risk Factors

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

Assessment Type	
HITRUST Risk-based, 2-year (r2) Security Assessment	
General Risk Factors	
Organization Type	Service Provider (Information Technology, IT)
Entity Type	Healthcare - Business Associate
Do you offer Infrastructure as a Service (IaaS)?	No
Geographic Risk Factors	
Geographic Scope of Operations Considered	Multi-State
Organizational Risk Factors	

Number of Records that are currently held	Between 10 and 60 Million Records
Technical 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?	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
Is the system(s) publicly positioned?	No - The system is not publicly positioned
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 to 85,000
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No - There are no modems in the solution
Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - No fax machines used in the environment
Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - No Chinstrap personnel travel to locations deemed to be of significant risk.
Are hardware tokens used as an authentication method within the scoped environment?	No - There are no hardware tokens in use.
Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	Yes
Are wireless access points in place at any of the organization's in-scope facilities?	No - There are no wireless access points in the environment.
Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	No - There is no in-house or outsourced information systems development.
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 - There are no electronic signatures in use.
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	Yes

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 system allow users to access the scoped environment from an external network that is not controlled by the organization?	Yes
Regulatory Risk Factors (Optional)	
Subject to State of Massachusetts Data Protection Act	
Subject to 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 was established in 2005 and has grown to 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 Platform

The following table describes the platform that was included in the scope of this assessment.

Customer Central (a.k.a. "Portal")	
Description	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.
Application(s)	Penguin Nest, Penguin Analytics, South Pole Benefits Eligibility
Database Type(s)	Oracle

Customer Central (a.k.a. "Portal")	
Operating System(s)	HP-UX
Residing Facility	Pelican Data Center
Exclusion(s) from scope	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.

In-scope Facilities

The following table presents the facilities that were included in the scope of this assessment.

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. The “Consideration in this Assessment” column of the following table specifies the method utilized for each service provider relevant to the scope of this r2 assessment. HITRUST requires that the inclusive method be used on all r2 assessments but allows use of both the inclusive and exclusive methods on HITRUST Implemented, 1-year (i1) validated assessments. Confidential Page 11 of 27 © 2021 HITRUST Alliance Chinstrap Penguin Corp HITRUSTAlliance.net Organizations undergoing i1 validated assessments have two options of how to address situations in which a HITRUST CSF requir ement is fully or partially performed by a service provider (e.g. by a cloud service provider):

- The Inclusive method, whereby HITRUST CSF requirements performed by the service provider are included within the scope of the i1 assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing, and
- The Exclusive (or Carve-out), method, whereby HITRUST CSF requirements performed by the service provider are excluded from the scope of the i1 assessment and marked as N/A with supporting commentary that specifies that the HITRUST CSF requirement is fully performed by a party other than the assessed entity (for fully outsourced controls) or through commentary describing the excluded partial performance of the control (for partially outsourced controls).

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Seashore Office Data Storage	Seashore provides backup tape delivery and storage in a secure offsite facility. No unencrypted customer, covered, or otherwise confidential information is stored here.	Included
Pelican Hosting	Pelican Hosting provides a colocation facility where Chinstrap maintains a dedicated cage. Pelican Hosting personnel do not have logical access to any in-scope systems.	Included