**Template Instructions:**

This template must be completed as part of your HITRUST Validated Assessment and uploaded to the “Organizational Overview & Scope” section of your assessment within MyCSF

When completing the template please:

* Complete all sections of the template
* Do not modify or remove any section headers
* Do not alter the table format through the addition or removal of columns or alteration of column headers
* Review all content for spelling and grammar prior to uploading it to MyCSF

Assessed Entities should be aware that **all** content in this template will be included in your final HITRUST CSF Validated Assessment Report. Additionally, the ‘Organization Overview and Scope’ and ‘Overview of the Security Organization’ sections will also be included in the CSF Letter of Certification with Additional Scope Information. HITRUST recommends that Assessed Entities thoroughly review all information included in this template to avoid the disclosure of any information deemed confidential by the Assessed Entity.

**Organizational Overview and Scope:**

**Organization and Industry Segment Overview**

Please provide a paragraph that describe the organization and the industry segment they are servicing.

**Services/Products Provided**

Please provide a paragraph that addresses the specific products and services being provided by the entity being assessed. How do they differentiate themselves from the rest of the market?

**Primary Systems**

Please provide a paragraph that addresses the systems in scope, on what platforms they run, a description of their primary function, and whether PHI is involved. This should agree to the table at the end of this document.

**Services Outsourced**

Please provide a paragraph that lists the services (e.g. colocation data center, Security Operations Center (SOC), hardware leasing, Disaster Recovery (DR), sanitization and media destruction, etc.) that have been outsourced or moved to the cloud.

**Scope Overview**

The Scope Overview is designed to communicate in summary form what system(s) and process(es) were assessed as well as the components they are made of and the market-facing products and/or service lines they support. It will also communicate if the environment was assessed as a whole, or if partially assessed what exclusions, if any, were not assessed. Exclusions are only acceptable when there is a clear delineation. An example might be a portal that allows organizations to present content. The portal might be included but the content could be excluded.

| **System Name** | **Components** | **Service Offering** | **Full** | **Partial** | **With Exclusions** | **Description of Exclusions** |
| --- | --- | --- | --- | --- | --- | --- |
| Chinstrap Portal | Oracle DB v8.1VMWare v7.9 | Penguin Nest |  | X | X | Content & the underlying applications that provide it for delivery through Penguin Nest by customers were not assessed as part of the report |
| Penguin Analytics | X |  |  |  |
| South Pole Benefit Eligibility | X |  |  |  |

**Scope Description**

The scope description is a verbose description of the system(s) and process(es) that were assessed for the report. It should be written with as much detail about the system(s) and process(es) as possible and include descriptions of the service offering(s) and/or product(s) that they support. Items to include in the scope description would include component parts, internal vs. external development, connectivity, and interfaces.

**Scope Diagram**

High-level network diagram, system context diagram, or system architecture diagram.

**Overview of the security organization:**

[Narrative description]

**Additional information regarding [assessed entity’s] security program.**

|  |  |
| --- | --- |
| **Types of security tools deployed** | * Laptop Encryption
* Wireless Network Scanning
* Anti-Malware
* Anti-Spam and Web Filtering
* …
 |
| **3rd party assessments** | * Assessment Type — Date performed by – Report issuer
* SOC 2 Type II—Sept. 20XX performed by – Report issuer
* PCI Assessment—Feb. 20XX performed by – Report issuer
* …
 |

#

# Testing Summary:

**Below is a summary of the documentation reviewed and personnel interviewed for the controls outlined in this validated assessment.**

|  |  |
| --- | --- |
| **Testing Dates (Period of Assessment)** | * Start Date XX-Mon-XX – End Date XX-Mon-XX
 |
| **Documentation** | * PCI DSS v1.2 Report on Compliance: February 20XX
* SOC 2 Type II: Jan. 20XX to Sept. 20XX
* Acceptable Use Policies
* Information Protection Policies
* Perimeter Security Policies
* Remote Access Policies
* Physical Security Policies
* Personnel Security Policies
* …
 |
| **Interviews** | * John Smith – Internal Audit Manager
* James Taylor – Application Management Administrator
* Steve Buscemi – Security Administration/Verification Analyst
* Nathaniel Hawthorne – Windows Security Lead
* …
 |
| **Technical Testing** | * Penetration Test of Corporate Perimeter
* Client Vulnerability Scan: August 20xx
* Client System Server Configuration Audit: August 20xx
* Vendor Laptop Encryption Verification – Random Sample
* Additional technical testing or scanning
* …
 |