Course

**IFSC 76003-9U1 – Data Protection and Privacy**

Submitted to

**Prof Jennifer Davis**

**Prof Timothy Holthoff**

Submitted by

**Deepak Singla**

Assignment 1

**CPO Plan – Quantum Leap, Inc**

College

**University of Arkansas Little Rock,**

**Little Rock, Arkansas**

# Table of Contents

## Introduction

As a new CPO of Quantum Leap, Inc, I would like to first know what is already working in the company and what is already implemented, company policies, what rules and regulations company already has been following. Once the existing system is understood then plan for the new future enhancements to the existing system. On approval from the stakeholders, new measures will be put in place such as creating a first-year plan, drafting privacy policies, developing a Privacy Impact Assessment (PIA) template, and creating a Data Breach Incident Response Plan. Finally, there will be an after-action report detailing the response, findings, and necessary notifications, with the incident spreading from the West Memphis data center to a data center in Paris. Following sections details the various phases of the process

## First 30 days plan – Meet the team/What already working

A CPO role is an ever-evolving role. As the technology is advancing every day so as the risk of data being compromised.

- First challenge would be to find out the pain points of the organization. And set expectations for the privacy measurements. This should be done by meeting one on one leadership (CEO, CIO, CFO, HR, EWS Support, SME, Innovation leads) and other senior managers in the company and meet other stakeholders.

- Need to find out the how much cybersecurity awareness does every single employee have and how are they prioritizing staying ahead of cyber threats?

- Meet different teams understand the culture of the company especially with Security, HR, Legal Team and other teams as and when required. Understand the awareness level of the teams, how receptive teams when a change is implemented organization wide.

- Review the company's existing privacy policies (Privacy, Security, Subscribers), procedures, and compliance frameworks such as EWS Handling, Third Parties, FedRAMP implications and Quantum leaps. Audit key documents such as Privacy Impact Assessments (PIAs), Records of Processing Activities (ROPAs) and/or Incident response plans

## First 60 days plan – Review and plan

- After the initial review Develop the initial draft of a comprehensive privacy policy for Quantum Leap and a specific privacy notice for Enterprise Web Services (EWS.com), as required by the course.

- Create a privacy roadmap that addresses identified gaps (Privacy, Retention and Third-Party Risk) and aligns with overall business objectives. These gaps should have been identified in the first 30 days.

- After meeting with leadership, create a formal structure on privacy governance outline. Work with legal team, HR and security teams and find the right set of people to do the groundwork. Prepare and present an overview of the privacy program's initial findings and the proposed roadmap to the board or executive leadership

## First 6 months plan – Implement new policies

This is the time to rollout the plan, get the teams together and execute the plan as prepared in last phase.

- Awareness of the members of the organization towards old and new policies is paramount. Make sure enough training sessions have been conducted so that there is no deficit of knowledge about these new measures being implemented. Members awareness is one of the major problems in many organizations. Conduct regular phishing and cybersecurity awareness trainings

- Finalize the quantum leap and publish privacy policies and data-handling procedures across the organization such as Access Controls, Encryption, EWS System, review updates and EWS.com privacy notice based on internal feedback and publish them. This should include a formalized process for conducting Privacy Impact Assessments (PIAs).

- Take advantage of Artificial Intelligence tools available today to make sure organization put its resources to the best use.

- Launch a program to periodically review and audit the company's data processing activities and ensure compliance with internal policies and external regulations.

- A tracking system like some kind of review board for this new privacy program is to be implemented. Key performance indicators would help measure the effectiveness of the new rules and regulations. This will help prioritize the areas where modifications are required.

## First 1 year plan – Review/Optimize/Scale

- This is the phase of retrospection, maturing the privacy program, scaling efforts, and establishing the CPO as a key strategic partner for business growth.

- Review and update the privacy roadmap based on lessons learned, regulatory changes, and evolving business needs. Privacy by design Framework (Quantum and EWS Focused)

- Work with marketing and public relations to strategically communicate the company's commitment to data privacy as a way to build customer trust and gain a competitive advantage.
- After round the years efforts, by now organization should have a strong base and a framework to follow for future organizational expansions and projects. This framework should be revisited every quarter to make sure that the rules and regulations, privacy policies are still valid in ever evolving world of Artificial Intelligence.

## References


https://www.spencerstuart.com/research-and-insight/the-chief-privacy-officers-new-priorities-from-risk-manager-to-strategic-partner

https://trustarc.com/resource/top-10-priorities-privacy-leaders/

Used google and AI search.

https://thedataprivacygroup.com/blog/the-role-of-a-chief-privacy-officer-cpo-a-strategic-overview/