**Canadian Immigration, Refugees & Citizenship Department**

***Passport Automation System***

* **1.0 Purpose of the Document**

This Risk Management Plan identifies potential risks in the **Passport Automation System** project and outlines strategies to mitigate them. It ensures project stability, compliance, and successful execution.

* **2.0 Risk Assessment Approach**

The risk management approach follows these key steps:

1. **Identify Risks**: Analyze potential threats to project success.
2. **Assess Probability & Impact**: Classify risks based on severity.
3. **Mitigation Strategies**: Develop plans to minimize impact.
4. **Monitor & Control**: Continuously track and update risk factors.

* **3.0 Risk Identification**

| **Risk ID** | **Category** | **Risk Description** | **Probability** | **Impact** | **Mitigation Strategy** |
| --- | --- | --- | --- | --- | --- |
| R-01 | Security | Unauthorized access to sensitive passport data | High | Critical | Implement **AES-256 encryption**, enforce **multi-factor authentication** |
| R-02 | Compliance | Failure to meet **GDPR & Canadian Privacy Act** standards | Medium | High | Regular **compliance audits**, engage **legal team** for validation |
| R-03 | Budget Overruns | Unexpected costs exceeding allocated funds | Medium | High | Maintain **10% contingency reserve**, conduct **monthly financial reviews** |
| R-04 | Data Integrity | Corrupt or missing user data during processing | High | High | Implement **automated daily backups**, perform **routine data integrity checks** |
| R-05 | System Downtime | Application downtime due to high traffic | Medium | High | Scale infrastructure using **AWS auto-scaling**, implement **load balancers** |
| R-06 | Cyber Threats | DDoS attacks, phishing, malware | High | Critical | Deploy **firewalls, intrusion detection systems (IDS)**, conduct **regular security audits** |
| R-07 | User Adoption | Low engagement due to usability issues | Medium | Medium | Conduct **usability testing**, improve **UI/UX design** |
| R-08 | Vendor Dependencies | Third-party service failures (Cloud, APIs) | High | High | Ensure **backup service providers**, negotiate **SLAs with vendors** |
| R-09 | Regulatory Delays | Approval delays from **government agencies** | Medium | High | Engage **regulatory bodies early**, provide **periodic compliance reports** |
| R-10 | Technical Debt | Accumulation of poorly managed code and dependencies | Medium | High | Implement **code review processes**, schedule **regular refactoring sessions** |

* **4.0 Risk Monitoring & Control**
* Risks will be **continuously monitored** throughout project phases.
* Weekly **risk review meetings** will be held with project stakeholders.
* Risk mitigation actions will be **documented and updated** as required.
* **4.1 Risk Escalation Process**
* **Low Impact Risks**: Managed at the **team level** with immediate fixes.
* **Medium Impact Risks**: Reviewed in **bi-weekly management meetings**.
* **High Impact Risks**: Escalated to **executive-level decision-making**.
* **5.0 Contingency Plan**
* **Data Security**: Regular **penetration testing**, **incident response plan**.
* **Budget Control**: Implement **cost tracking dashboards**.
* **Regulatory Delays**: Maintain **early regulatory engagement**.
* **System Failures**: Utilize **cloud-based failover architecture**.
* **6.0 Conclusion**

The Risk Management Plan ensures proactive identification, analysis, and resolution of risks that could impact the Passport Automation System. Ongoing reviews and timely interventions will ensure project success.

* **7.0 Appendices**
* Compliance Documentation
* Incident Response Procedures
* Cybersecurity Measures Checklist
* Risk Review Reports