Software development plan

Introduction and Scope

Pitrix is a company which is going to be the manufacturer of advanced vehicle tracking and navigation systems for professional motor racing teams. The company aims to optimize vehicle performance, reduce lap times, and enhance overall racing experience through the creation of a mobile application which will provide real-time navigation data, vehicle telemetry and analytics. The end goal is to allow professional motor racing teams to gain a competitive edge to increase their chances of winning.

Objectives

The company aims to achieve a numerous number of objectives to mitigate the possibility of any risk from damaging the project when launched or active.

To reduce the **probability** of the risks which are identified in the risk treatment plan:

- Enforce frequent cybersecurity training for the employees which will allow for them to have increased awareness to lower the chances of security breaches.
- Enforce access level controls to prevent unauthorized data access and implement multi factor authentication to validate users.
- Enforce regular updates and security testing to lower the vulnerabilities of the mobile application.

To reduce the **impact** of the risks which are identified in the risk treatment plan:

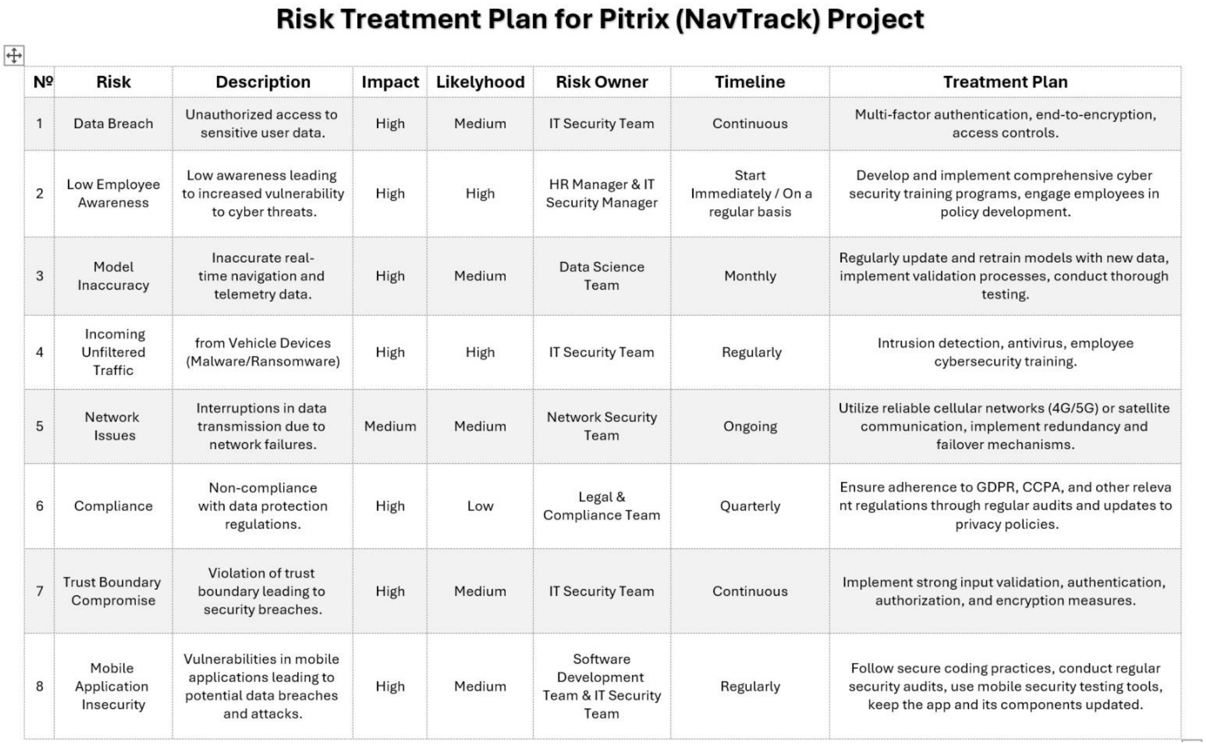
- Enforce data encryption measures to make compromised data unreadable when data breaches occur.
- Enforce network redundancy and failover mechanisms to provide a backup temporary solution to keep the mobile application running when network issues occur.

To completely **avoid** some the risks which are identified in the risk treatment plan:

- Ensure that there is compliance with data protection regulations through the adherence of GDPR and other privacy related regulations to avoid non-compliance issues.
- Ensure that after there is a deployment for the mobile application, any update or modifications are put through a new deployment as it will allow to have backups of past versions which may help identify when risks had impact and what the risk type is which helps to prevent them from happening in future deployments.

Risk Assessment and Treatment Plan

The diagram below shows the risk treatment plan for the company Pitrix which focuses on:



Risk Treatment Plan for Pitrix (NavTrack) Project

№	Risk	Description	Impact	Likelyhood	Risk Owner	Timeline	Treatment Plan
1	Data Breach	Unauthorized access to sensitive user data.	High	Medium	IT Security Team	Continuous	Multi-factor authentication, end-to-encryption, access controls.
2	Low Employee Awareness	Low awareness leading to increased vulnerability to cyber threats.	High	High	HR Manager & IT Security Manager	Start Immediately / On a regular basis	Develop and implement comprehensive cyber security training programs, engage employees in policy development.
3	Model Inaccuracy	Inaccurate real-time navigation and telemetry data.	High	Medium	Data Science Team	Monthly	Regularly update and retrain models with new data, implement validation processes, conduct thorough testing.
4	Incoming Unfiltered Traffic	from Vehicle Devices (Malware/Ransomware)	High	High	IT Security Team	Regularly	Intrusion detection, antivirus, employee cybersecurity training.
5	Network Issues	Interruptions in data transmission due to network failures.	Medium	Medium	Network Security Team	Ongoing	Utilize reliable cellular networks (4G/5G) or satellite communication, implement redundancy and failover mechanisms.
6	Compliance	Non-compliance with data protection regulations.	High	Low	Legal & Compliance Team	Quarterly	Ensure adherence to GDPR, CCPA, and other relevant regulations through regular audits and updates to privacy policies.
7	Trust Boundary Compromise	Violation of trust boundary leading to security breaches.	High	Medium	IT Security Team	Continuous	Implement strong input validation, authentication, authorization, and encryption measures.
8	Mobile Application Insecurity	Vulnerabilities in mobile applications leading to potential data breaches and attacks.	High	Medium	Software Development Team & IT Security Team	Regularly	Follow secure coding practices, conduct regular security audits, use mobile security testing tools, keep the app and its components updated.

- **Risk -** The identification of the risks involved when creating the mobile application
- **Description** – a summary of the risks which provide specific information on what happens if this risk is not addressed
- **Impact** – A rating which shows how much damage it can cause to the mobile application
- **Likelihood** – A review of how common this type of risk is likely to happen
- **Risk Owner** – This provides information on who will manage the risk when attempting to mitigate it
- **Timeline** – This is how frequent the treatments will occur to mitigate the risks of the project
- **Treatment Plan** – The treatment plan is the mitigation strategy used to prevent the risks from occurring