Risk Plan

| Risk | Description | Severity | Likelihood | Mitigation |
|---|---|---|---|---|
| External data leaks | Unauthorised access to sensitive location data, on the database or interception during transit | High | Medium | Enforce encryption of data both in transit and in storage, alongside strong access control policies |
| Internal unauthorised tracking | Users with legitimate access to policy controls may try to enable tracking on certain devices | Medium | Low | Devices group policies will not be able to be edited once created, and the device cannot be remotely added to a device group |
| Legal compliance | Data being collected is to be considered sensitive and personal data if it can be linked to a person. | High | Low | Ensure that the data is kept secure in line with GDPR regulations. |
| Device goes offline | A device may be unreachable due to poor internet or loss of power | Low | Medium | Database will store last known locations of devices being tracked |
| Performance impact | Constantly communicating devices may experience lower battery longevity | Low | Low | Devices will only communicate back to the server after set time intervals, or after a geofence interaction |
| Encryption key compromise | Device side keys could be stolen, allowing attackers to forge location data | Low | Medium | Use android keystore to store keys which encrypt sensitive data |
| Device/app tampering | The device could be made to report falsified location data | Medium | Medium | Use map snapshot hashes alongside timestamps to verify if the distance/time is possible and flag suspicious “speeds” travelled. |
| Replay attacks | Attacker could replay old messages to make it seem like the device is still within a permitted area, while they steal the actual device | Medium | Low | All messages should use nonces and timestamps to prevent replay attacks. |