IoT Device Threat Modeling Assessment Report

1. Executive Summary

[Provide a high-level overview of the assessment, key findings, and recommendations.]

2. Device Overview

Device Name	[Device Name]
Manufacturer	[Manufacturer]
Model	[Model]
Firmware/Software Version	[Version]
Intended Use	[Description]

3. Architecture Overview

- System Components
- Data Flows
- Connectivity (e.g., Wi-Fi, BLE, Cellular)
- Integration Points (cloud services, APIs)
- Users & Privileges

[Insert diagrams or summarize architecture here]

4. Threat Modeling Approach

[Brief description of methodology used, e.g. STRIDE, PASTA, custom approach]

- Scope
- Assumptions
- Tools Used

5. Identified Threats & Vulnerabilities

#	Threat/Vulnerability	Description	Potential Impact	Risk Level
1	[Threat Name]	[Description of the issue]	[Impact details]	[Low/Medium/High]

6. Risk Mitigation Recommendations

1. **[Threat Name]**: [Recommended mitigation action]
2. **[Threat Name]**: [Recommended mitigation action]

7. Conclusion

[Summary of overall risk posture, key takeaways, and next steps.]

8. Appendix

- Definitions & Acronyms
- Supporting Documents / References
- Assessment Date
- Assessment Team