Application Threat Modeling

1. System Overview

Application Name: ________________________________

Application Description:

[Provide a brief description of the application's purpose and functionality]

1.1 Assets to Protect

- User credentials and authentication tokens
- Personal Identifiable Information (PII)
- Business-critical data and intellectual property
- [Add application-specific assets]

1.2 System Architecture

[Describe system components: Frontend, Backend, Database, APIs, Third-party Services]

[Insert architecture diagram here]

2. STRIDE Threat Analysis

STRIDE categorizes threats into six types: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

STRIDE Category	Threat Description	Affected Component	Severity
Spoofing Identity	[e.g., Attacker impersonates legitimate user]	[e.g., Authentication module]	[H/M/L]
Tampering	[e.g., Data modification in transit]	[e.g., API endpoints]	[H/M/L]
Repudiation	[e.g., User denies performing action]	[e.g., Audit logging system]	[H/M/L]
Information Disclosure	[e.g., Sensitive data exposure]	[e.g., Database layer]	[H/M/L]
Denial of Service	[e.g., Resource exhaustion attack]	[e.g., Web server/API]	[H/M/L]
Elevation of Privilege	[e.g., Unauthorized access escalation]	[e.g., Authorization module]	[H/M/L]

3. Mitigation Strategies

Threat	Mitigation Strategy	Implementation Status
[Threat from STRIDE]	[Detailed mitigation approach]	□ Not Started □ In Progress □ Complete

4. Attack Scenarios

Document specific attack scenarios based on identified threats:

Scenario 1: [Attack Name]

[Describe the attack vector, prerequisites, and potential impact]

5. Recommended Security Controls

- Implement multi-factor authentication (MFA)
- Enable comprehensive audit logging
- Deploy Web Application Firewall (WAF)
- Implement rate limiting and throttling
- [Add application-specific controls]