Infosec FAQs

**Q1: What are the minimum-security requirements for developing an application with GenAI integrations?**

A: The application should support SAML 2.0 and OAuth 2.0 for Single Sign-On (SSO) integration and external application integrations. No local authentication is allowed. It should have network-level controls such as restricted access to application endpoints including APIs, IP range restrictions, and secure admin/support workstation setup.

Q2**: How should the application handle authentication and network-level controls?**

A: The application should have a robust system for login and connection to other applications. It should implement IP restrictions and have its own security management system for network and application levels. Access to GenAI should be controlled through API Management Services with IP whitelisting.

Q3: **What are the requirements for storing secrets and keys in the application?**

A: Any secrets and keys should not be stored in Application config/databases in clear text. A secure vault solution should be used for credentials storage and rotation.

Q4: **What are the requirements for authorization and access controls?**

A: Use SAML for user provisioning and deprovisioning with no manual user creation or deletion allowed. Role-based access controls should be properly documented and shared for InfoSec review.

Q5**: What are the requirements for data storage in DB?**

A: No user or credentials data should be stored in the DB. Only Request - GenAI response data will be stored in DB. Users do not have direct access to DB & tables. The DB should be encrypted in storage.

Q6: **How are audit logs getting maintained?**

A: Application logs should record sensitive user activity and GenAI responses, have timestamps, identity name / id, activity details, and should be reported to a centralized log management system.

Q7: **How is the generated code tested for vulnerabilities?**

A: The generated code should be subjected to automated vulnerability scanning or Static Application Security Testing (SAST) to catch potential security flaws.

**Q 8: How is sensitive information handled?**

A: Application should have measures in place to identify and appropriately handle sensitive information. This could include redacting or encrypting sensitive data or ensuring it doesn't get written into the code in the first place.

**Q 9: How is the generative AI model secured?**

A: TBD

**Q 10: How are usage limits enforced?**

A: GenAI applications can be resource intensive. Therefore, there should be measures in place to enforce usage limits and prevent abuse of the system, such as rate limiting or quotas.

**Q 11: How is data privacy ensured?**

A: All data used by the generative AI application should be handled in accordance with data privacy laws and regulations. This includes collecting only the necessary data, anonymizing data where possible, and providing users with clear information about how their data is used.