Exhibit 2: High-Level Cybersecurity & Data Protection Information Requested

This section outlines the **high-level cybersecurity information** requested from Suppliers as part of the Travel System **Request for Information (RFI)**. Since this is not an RFP, detailed evidence, certifications, or documentation are **not required** at this stage. Potential Suppliers should provide concise descriptions of capabilities, architecture, and security practices.

1. System Hosting & Data Location

- High-level description of where the system is hosted (cloud/on-prem, U.S.-based or international).
- General location of production and disaster recovery environments.
- Whether any data is stored, accessed, or processed outside the United States.

2. Access Control & Authentication

- Overview of authentication methods supported (SSO, MFA, identity provider compatibility).
- Summary of access control approach (role-based access, admin access structure).
- Whether any foreign nationals may have access to the system or its data.

3. Data Protection Practices

- High-level description of data protection methods (encryption in transit/at rest, anonymization, or data minimization practices).
- General approach to securing sensitive travel information.

4. Incident Response & Monitoring

- Overview of how the vendor detects and responds to security incidents.
- Description of available system logging and monitoring capabilities.

5. Business Continuity & Disaster Recovery

- Summary of DR/COOP approach.
- High-level RTO/RPO targets.
- Confirmation that DR environments apply equivalent security controls.

6. Data Retention & Post-Contract Handling

- General data retention policies for customer data.
- High-level process for returning or deleting data after contract termination.
- Whether system logs or backups persist after customer offboarding.

7. Third-Party Integrations & Supply Chain

- High-level list of major third-party services integrated into the system.
- General approach to vendor's supply-chain risk management.

8. Compliance & Security Standards

- Summary of relevant security certifications or frameworks followed (e.g., SOC 2, ISO 27001, FedRAMP).
- High-level overview only; no documentation required at this time.

9. Foreign National Access Considerations

- High-level disclosure of countries where vendor staff or support may be located.
- Whether any support, development, or operations functions are performed outside the U.S.
- Summary of controls to prevent access from restricted/sensitive countries.

10. Optional: Additional Security Features

Vendors may provide high-level descriptions of any other security capabilities that differentiate their system (e.g., zero-trust architecture, advanced threat detection, privacy-by-design features).

Note to Suppliers

At this RFI stage, **broad descriptions** are sufficient. Detailed technical documentation, certifications, penetration test reports, or policy documents will be requested during a later RFP phase if applicable.