Third Party Risk Management Policy

1. Introduction

1.1. The purpose of this policy is to establish the methods by which Globespan Travel Management will manage security risks that are introduced by third parties, including contracted vendor service providers and members/participants. The intent is to ensure that the security of Globespan Travel Management information and information assets are not reduced when sharing information with third parties or by the introduction of third party products or services into the Globespan Travel Management environment. This policy applies to all third party arrangements, including those with Business Associates.

2. Policy statement

2.1. Globespan Travel Management shall establish third party risk management functions with the purpose of governing security risks of third party organizations that have access to enterprise data, or provide products or services for Goway.

Responsibilities for the third party risk management function shall include:

- Identifying all Globespan Travel Management Business Associates
- Vetting the security controls of third parties before establishing a third party contract relationship.
- Ensuring an approved and up-to-date Globespan Travel Management Business Associate Agreement (BAA) is in place and has been signed by every third party.
- Maintaining a current and accurate listing of all Globespan Travel Management business associates.
- Monitoring third parties for adherence to provisions within BAAs (where applicable), Service Level Agreements (SLAs), and contractual security requirements.
- Performing on-going or continuous reviews of security measures implemented by third party service providers.
- Ensuring the adherence to all other provisions within this policy.

3. **Third Party Risk Identification**

3.1. The potential risks to Globespan Travel Management information assets from business processes involving third parties shall be identified, and appropriate controls shall be implemented to mitigate these risks before granting access.

3.2. Third parties shall only be granted access to Globespan Travel Management information assets after due diligence has been conducted, appropriate controls have been implemented, and a written contract defining the terms of access has been signed.

3.3. Due diligence by Globespan Travel Management to determine risk shall include interviews, and reviews of documents, checklists, and certifications.

4. **Third Party Security Requirements**

4.1. If appropriate, a risk assessment shall be conducted of the third party to determine the specific security requirements necessary to secure their systems to a level of risk acceptable to Goway.

4.2. All identified third party security requirements shall be addressed and validated before granting third party access to Globespan Travel Management information or information assets.

5. **Third Party Agreements**

5.1. Agreements with third parties involving accessing, processing, communicating or managing Globespan Travel Management information assets, or adding products or services to information assets must cover all relevant security requirements and shall include all required security and privacy controls in accordance with Globespan Travel Management security and privacy policies.

5.2. The specific limitations of access, arrangements for compliance auditing, penalties, and the requirement for notification with respect to relevant third party personnel transfers and terminations shall be identified in the third party agreements.

5.3. A standard Business Associate Agreement (BAA) shall be defined.

5.4. The BAA shall include provisions for breach notification and termination upon breach.

6. **Third Party Access Control Requirements**

6.1. Globespan Travel Management shall only allow third parties to create, receive, maintain, or transmit on its behalf after the organization obtains satisfactory written assurance that the third party will appropriately maintain and enforce the privacy and security of the enterprise data

6.2. Third party access shall be based on the principles of need-to-know and least privilege.

6.3. Third party access shall be granted only for the duration required.

6.4. Remote access connections between Globespan Travel Management and third parties must be encrypted.

6.5. Remote access connections with third parties shall be monitored on an ongoing basis.

7. **Third Party Service Delivery**

7.1. Globespan Travel Management shall require that third parties meet industry best practices and regulatory requirements for security and privacy controls and that they are implemented, operated and enforced.

7.2. SLAs, or contracts with an agreed service arrangement, shall address liability, service definitions, security controls, and other aspects of services management.

7.3. Globespan Travel Management shall develop, disseminate and update at least annually a list of current service providers.

7.4. Globespan Travel Management shall address information security and other business considerations when acquiring systems or services including maintaining security during transitions and business continuity following a failure or disaster.

8. **Third Party Service Providers Monitoring and Review**

8.1. The services, reports and records provided by the third party Service Provider shall be monitored and reviewed on an annual basis, and audits shall be carried out to ensure compliance with the third party Service Provider agreements is maintained.

8.2. The results of monitoring activities of third party Service Provider services shall be compared against the SLA or contracts at least annually.

8.3. Regular progress meetings shall be conducted as required by the SLA or contract to review reports, audit trails, security events, operational issues, failures and disruptions, and ensure identified issues are investigated and resolved accordingly.

8.4. Network connections with third party Service Providers shall be periodically audited to ensure that they have implemented any required security features and meet all requirements agreed to with Goway.

9. **Third Party Change Management**

9.1. Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking into account the criticality of business systems and processes involved and re- assessment of risks.

9.2. Third parties shall be required to coordinate, manage and communicate changes that will have an impact to Globespan Travel Management information, systems or processes.

9.3. Third party changes shall be evaluated to identify the potential impacts before implementation.

10. **Enforcement**

10.1. Globespan Travel Management IT General Manager department shall be responsible for enforcing compliance with this policy under the direction of the Vice President of IT & Operations..

Review and update of this document will take place when changes require revising the **Third Party Risk Management Policy**. Such modifications may relate to changes in roles and responsibilities, release of new legislation or the identification of a new policy area, in consultation with appropriate members and their approval on all revisions to this Third Party Risk Management Policy. When approved a new version of the policy will be issued and all affected departments will be informed of the changes.

Document Configuration Control

Version No	Page No	Details of Change	Change Date	Prepared By	Approved By
1	All			Scott Duncan	Peter Lacy
1.1	All	Review	01 Nov 2020	Scott Duncan	Peter Lacy
1.2	All	Review	10 Nov 2020	Scott Duncan	Peter Lacy