Indigo Information Security Requirements for Suppliers

Version 1.0

Indigo partners with a variety of third-party service providers (aka Suppliers) to support its business operations. As part of these strategic business relationships the suppliers have access to wide ranges of information, representing a spectrum of risk to the company. To appropriately manage the risks, it is important to understand the nature of the services being provided, inventory the type of information the suppliers have access to and assess the controls/processes they have in place to appropriately safeguard the sensitive information.

The minimum Information Security requirements outlines the principles and minimum controls necessary for protecting Indigo's information and IT systems exposed during a supplier's service lifecycle and are aligned with industry best practices. The minimum Information Security controls are controls that Indigo expects to exist as part of a mature Information Security program which includes, but are not limited to:

1. Information Security Policy and Standards

Information security polices and standards should be review and assessed for relevance at least annually. Based upon the results of that assessment, the policy and standards should be updated. Suppliers are also expected to provide its personnel with Information Security Awareness training. Suppliers personnel should a clear understanding of the rules and guidelines for dealing with the protection of information.

2. Access Control and Unauthorized Access

Suppliers should ensure that only authorized personnel are accessing the systems and applications that host Indigo information with such access based on the 'least privileged' principle. Suppliers should use best efforts to prevent, secure and defend its systems against hackers, unauthorized users, viruses, malware, or others who seek to breach the security or integrity of such systems. Industry standard complex password parameters should be deployed for all applications hosting Indigo data.

3. Encryption

Suppliers should work with Indigo in order to ensure that proper encryption requirements for confidential data transmission and storage, including storage of backups and archives, are in place and satisfactory to Indigo, including encryption on mobile devices, encryption of information transmitted across trusted/untrusted networks, encryption of data at rest and strong authentication controls guarding access to the information.

4. Incident Management and Disaster Recovery

Suppliers should have a process for managing security incidents. Suppliers should have a process to handling Indigo's emergency inquires outside of normal business hours. Suppliers are expected to have a program/processes to ensure continuation of business in case of disaster or pandemic. There should be a notification process in place to inform Indigo of an incident or security breach.

5. Secure Software Development Lifecycle

Suppliers that supply software related products to Indigo are expected to have Secure Development Practices deployed to ensure that all software written by or on behalf of the suppliers and utilized by Indigo has been automatically scanned (when possible) for vulnerabilities and corrected before being released into production. At a minimum, all critical/high and medium level risks (i.e. OWASP Top 10) vulnerabilities are expected to have been fixed or remediated by other means prior to being used in production for use by Indigo.

6. Physical Security

Suppliers are expected to have policies and procedures designed to ensure physical environmental protection of Indigo assets, data or property in the supplier's possession. Physical and environmental controls should be consistent with industry best practices and include physical access controls to areas of critical/sensitive information processing.

7. Vulnerability Management

Suppliers should have a vulnerability management program in place to monitor and review vulnerabilities in its environment. Penetration tests should be conducted on at least an annual basis. The penetration test reports should detail the scope, methodology and confirmation that the sites and applications in use by Indigo were included in the testing. Web application vulnerability assessments should be conducted on at least a quarterly basis. Vulnerabilities identified must be remediated.

8. Change Control

The suppliers should have change control policies and procedures. The suppliers should have a process to deal with third party software security updates and patches. The suppliers should have a process for handling emergency changes.

9. Third Party Assurance

Suppliers are expected to have a third-party assurance program of their own which helps validate that any of their Third-Party suppliers have a comparable security program and control environment to protect Indigo's sensitive information in accordance with expectation of a mature information security program.

10. Compliance

Suppliers are expected to comply with all applicable privacy laws and regulation requirements related to maintaining security, confidentiality, and protection of Indigo’s information.