Customer Security Statement

ENGINEERING A DIGITAL FUTURE

INDIGO

Table of Contents

ENGINEERING A DIGITAL FUTURE

Customer Security Statement

PURPOSE

This document sets out the approach that Indigo takes to protecting the data of the organisation our people and our customers. We are committed to delivering secure services and being recognised as a trusted telecommunications and network service provider.

We have developed an embedded security culture through awareness, education and empowerment to ensure we deliver a great customer experience. Appropriate security controls are in place and operating effectively to deliver assurance in line with contractual agreements.

HOW DOES INDIGO MANAGE SECURITY?

Indigo operates an Information Security Management System (ISMS) based upon the requirements and recommendations of ISO27001:2013, including risk management, business continuity, incident management, physical security, security awareness training and much more.

The Indigo ISMS ensures that Security Governance is in place at the core of the organisation. Information Security reviews are conducted, with senior leadership engagement, on a monthly basis to monitor performance and reduce risk. These meetings include senior stakeholders from across the Information Security Team, IT and Services, Business Security, Security Operations, Health & Safety, Network Operations and Board level leadership.

Indigo have designed the external certifications so that our global customer operations and services are covered from end to end, with a dedicated assessment, by adopting a Three Line of Defence risk and assurance model.

The Indigo Information Security team's vision is to: *enable the business to achieve its goal as the customer partner of choice and become a premier global telecommunications service delivery partner through the delivery of secure products and services.*

This will be achieved by *managing threats, improving security culture and driving a risk reduction program across the Indigo business services to improve customer relationships, enabling business growth and opportunities*.

WHAT SECURITY POLICIES DO INDIGO HAVE IN PLACE?

Indigo's ISMS is managed by the internal Information Security Team – this team is responsible for managing and maintaining all security related policies as well as the ISO27001 certification and Statement of Applicability (SOA).

The ISMS documentation includes:

- Computer and Mobile Phone Use Policy
- Access Control Policy
- Business Continuity Policy
- Clear Desk Policy
- Cryptographic & Key Management Policy
- Cyber and Information Security Incident Management Policy

- GDPR Data Protection Policy
- GDPR Data Retention Policy
- Indigo Information Security Policy Statement
- Indigo Secure Development Policy
- Information Security Document Classification Scheme
- Indigo System & Network Administrators Policy
- IT and System Change Control Policy
- IT Back Up Policy.

How does Indigo Manage Risk?

We have a robust Information and Cyber Security Risk Management Framework and associated processes that are subject to regular review and continuous improvement. This ensures that risks are identified, recorded, managed and mitigated as appropriate throughout our business and including customer specific operational risks. Critical and Major risks are reported and escalated to Senior Leadership.

Our risk management framework methodically addresses risks that may pose a threat to Indigo, its infrastructure and services (both internal and external), its customers, staff, brand and assets. The risk management strategy provides a framework for the proactive management of risks to eliminate or minimise any impact.

How does Indigo Manage Information Classification?

All information is classified and protected to keep it safe. Our classification scheme identifies rules of how to handle and manage information at each level through our Data Classification and Handling Scheme and the implementation of data loss prevention tools. In addition, Indigo Security Policies detail what controls we implement to manage both Indigo and Customer data – including data retention and disposal.

The Classification Scheme adopted is as follows:

- **UNCONTROLED**: for example, third party documents that hold no formal classification
- **UNRESTRICTED**: Documents which do not contain information about any customer, employee or commercially sensitive activities
- **RESTRICTED**: Documents which are of commercial use to the Company. This includes internal documentation, procedures relating to both company internal activities and those associated with customers
- **CONFIDENTIAL**: Documents which contain specific information on any individual employee or contracting party. Document which contains specific customer information which is highly sensitive and can lead to substantial or unacceptable business losses. Indigo documentation which is commercially sensitive. All information processing equipment must be treated.

How does Indigo Manage Physical Security?

Indigo ensures that we provide a secure environment for all our colleagues and customers. We use live site monitoring and electronic protection systems to safeguard the integrity and security of Indigo's assts and our customer's infrastructure, applications and data.

We deploy a variety of controls, including but not limited to: identity cards, electronic access key fobs, biometric controls (facial recognition systems), CCTV, and role-based access control.

How Does Indigo Monitor IT System Use?

Indigo monitors user activity across all of its infrastructure, systems and applications 24/7 via its Security Operating Centre (SOC). All security incidents and events are investigated, triaged, contained, resolved and eradicated in accordance with the NIST aligned Incident Response plans and processes.

How does Indigo Manage Staff Screening & Vetting?

All Indigo colleagues and contractors are subject to a process of pre-employment screening that meets good commercial practice. Employee checks and vetting vary across the different countries in which we operate.

As standard, these checks include some or all of the following:

- Identity Checks (passport, driving licences, ID cards, Birth Certificates)
- Right to Work (if applicable)
- Business references from previous employers
- Academic checks along with personal qualifications
- Criminal history
- Where applicable (for example on government related contracts) Credit Checks
- Where applicable (for example working in the US) Social Security and / or Green Listing screening.

How does Indigo Manage Suppliers & Third Parties?

We effectively manage cyber and information security risks associated with Indigo suppliers through our procurement processes – ensuring that suppliers implement industry standard security policies and controls to safeguard Indigo customer data, systems, services and other assets that they are contracted to support.

We evaluate our suppliers using a series of assessments at on-boarding through life to service termination. Security is addressed in contractual arrangements and in accordance with our internal policies and regulations. Additionally, we request that suppliers have undertaken independent assurance certifications and reports (e.g., ISO27001).