# GEO Blocking Policy

## 1. Purpose

The purpose of this GEO Blocking Policy is to enhance the security of (COMPANY NAME) IT infrastructure by restricting access to our systems and data from specific geographic regions. This policy aims to minimize the risk of unauthorized access and cyber threats originating from regions not relevant to our business operations.

## 2. Scope

This policy applies to all employees, contractors, and third-party service providers who access (COMPANY NAME) information systems, networks, and data. The policy also covers all devices, including but not limited to laptops, desktops, mobile devices, and servers.

## 3. GEO Blocking Implementation

(COMPANY NAME), in collaboration with our Managed Service Provider (MSP), (COMPANY NAME), have implemented GEO blocking measures to restrict access to our systems and data from specified geographic regions. Regions that are deemed high-risk or irrelevant to our business operations will be blocked from accessing our IT infrastructure.

## 4. Employee Travel Notification

Employees who plan to travel outside the country or to a region that is typically blocked under this policy must provide the IT department with at least one week's notice prior to their departure. This notice must include:

* The travel destination(s)
* The dates of travel
* The expected return date

This information is necessary for the IT department to temporarily adjust the GEO blocking settings to allow access from the specified region during the travel period.

## 5. Return Notification

Upon returning from travel, employees are required to notify the IT department of their return. This allows the IT department to revert the GEO blocking settings to their standard configuration, re-blocking the regions previously allowed during the travel period.

## 6. Compliance

Employees who fail to provide adequate notice of travel or who do not inform the IT department of their return may experience access restrictions to (COMPANY NAME) systems and data while traveling. These restrictions will be enforced as part of our commitment to maintaining a secure IT environment.

## 7. Exceptions

Any exceptions to this policy must be approved by the IT department in consultation with the MSP and management.

Date of Policy Implementation: (DATE)

Policy Owner: (COMPANY NAME)