POLICY & PROCEDURES MANUAL

**MAPP Network Access Policy for International Travel**

To maximize our digital security and adhere to accepted best security practices, MAPP has implemented a conditional access policy (Geofence) which blocks account access outside of the United States.  This means that only connections from the United States are allowed into our network.

MAPP understands that having the ability to work and be connected to our network while traveling is necessary, so by creating this policy, we aim to keep employees connected to company resources, protect sensitive company data, and maintain a consistent level of network security while you are abroad. This policy outlines the guidelines and procedures for ensuring secure and uninterrupted access for employees traveling abroad.

This policy applies to all employees, contractors, and any other individuals who require access to MAPP's network or any IT related resources while traveling internationally.

**Notification Process:**

Employees must notify the IT department in advance of any planned international travel by emailing [helpdesk@mappbuilt.com](mailto:helpdesk@mappbuilt.com). The email should include the destination(s), travel dates, and duration of the trip. Please provide this information as soon as travel plans are confirmed.

**IT Department Responsibilities:**

Upon receipt of the travel notification, the IT department will assess the network access requirements for the destination(s) specified. Access will be granted for the specific countries and timeframes mentioned in the travel notification, provided there are no overriding security concerns.

**User Responsibilities:**

Employees must comply with the company's network security policies and guidelines while accessing the network abroad. Employees should adhere to any additional instructions or restrictions provided by the IT department for specific countries or regions.

**Compliance:**

Failure to comply with this policy will result in the inability to access your account while abroad. This includes, but is not limited to, your Microsoft account, your company email, Teams, and MAPP's Virtual Private Network (VPN). Employees are responsible for any violations of local laws or regulations pertaining to network access and data usage while abroad.

This policy will be reviewed periodically by the IT department to ensure its effectiveness and relevance. Updates and revisions will be communicated to all employees as necessary.