CYBERSECUITY

IN ACCORDANCE WITH THE FEDERAL COMMUNICATIONS COMMISSION REGULATIONS (47 U.S.C. § 1601), I HEREBY ATTEST THAT OUR ORGANIZATION DOES NOT UTILIZE ANY EQUIPMENT PROHIBITED BY THE FCC.

SZ DJI TECHNOLOGY CO LTD IS NOT ON THE LISTED OF THE SECURES NETWORKS ACT AS OF FCC.GOV LAST UPDATED SEPTEMBER 2023

ATTACHED IS OUR CYBERSECURITY PLAN OUTLINING THE MEASURES IN PLACE TO ENSURE COMPLIANCE.

1. RISK ASSESSMENT
   A. Identify potential cyber threats specific to drone operations
   B. Evaluate vulnerabilities in the drone spraying system
   C. Assess potential impact of cyber threats on business operations

2. SECURITY POLICIES AND PROCEDURES
   A. Develop and implement a cybersecurity policy
   B. Establish procedures for secure drone deployment and maintenance
   C. Define roles and responsibilities for employees involved in drone operations

3. NETWORK SECURITY
   A. Secure communication channels between ground control and drones
   B. Implement encryption protocols for data transmitted during spraying
   C. Regularly update and patch software to address security vulnerabilities

4. PHYSICAL SECURITY

A. Protect drones and associated equipment from unauthorized access

B. Implement measures to prevent physical tampering or theft of drones

C. Secure storage and transportation of drones to prevent compromise

5. DATA PROTECTION

A. Ensure secure storage and handling of sensitive data collected during operations

B. Implement backup and recovery procedures for critical data

C. Comply with relevant data protection regulations

6. EMPLOYEE TRAINING

A. Provide cybersecurity training for employees involved in drone operations

B. Raise awareness about social engineering threats and phishing attacks

C. Regularly update employees on cybersecurity best practices

7. COMPLIANCE

A. Stay informed about and comply with relevant aviation and cybersecurity regulations

B. Regularly audit and assess cybersecurity measures for compliance

C. Collaborate with regulatory bodies to ensure adherence to industry standards

8. CONTINUOUS MONITORING AND IMPROVEMENT

A. Implement continuous monitoring systems for cybersecurity threats

B. Regularly review and update cybersecurity measures based on emerging threats

C. Foster a culture of cybersecurity awareness and improvement within the organization