absolute AUTOMATIONS

**Delivery is the Difference.**

**Security Statement Document**

**RPA Networks, Inc (dba Absolute Automations)**

**Last Updated: July 1st, 2023**

## Purpose

This security statement serves to inform our valued customers about the robust measures RPA Networks, Inc has instituted to safeguard their data, including Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).

## 1. Introduction

At RPA Networks, Inc, our commitment to data security, confidentiality, and system availability is unwavering. Guided by our wide-ranging set of internal policies, from our Access Control Policy to our Information Security Policy, we work tirelessly to ensure a secure environment for our users' data and PHI.

## 2. Core Security Principles

Our security framework operates on the guiding principles of:

- **Data Security:** Safeguarding against unauthorized access and potential breaches.
- **Confidentiality:** Ensuring that user data, especially PHI, is treated with the utmost privacy.
- **System Availability:** Ensuring consistent and reliable access to our systems.

## 3. Security Measures

- Employing advanced security measures such as data encryption, firewalls, two-factor authentication (2FA), and role-based system access.
- Continuous system monitoring for potential malware and viruses.
- Conducting a comprehensive security assessment annually in line with our Risk Management Policy.

## 4. User Data Handling

- Encryption of user data at its source and during transmission, safeguarding its confidentiality and integrity.
- Regular backups, ensuring data availability and security.
- Sharing of data with third-party entities is strictly executed post the signing of a Business Associate Agreement (BAA) and after thorough security protocols assessment.

**5. Incident Response**

In the event of a security incident, our Incident Response Plan directs our actions and the communication with stakeholders, ensuring swift and effective resolution.

**6. Employee Training and Awareness**

- Mandatory Cyber Security & HIPAA compliance training for all employees and contractors in adherence to our Human Resource Security Policy.
- Dedicated efforts to ensure that employees remain updated about our security policies, practices, and potential threats.

**7. Third-party Vendors**

- For business-critical services and technology, we are in association with industry leaders like Microsoft and UiPath, both of which have undergone our rigorous security assessment as outlined in our Third-Party Management Policy.

**8. Review and Updates**

Our commitment to ongoing security improvement is reflected in our yearly review and update of this security statement, and other associated policies.

**9. Additional Policies**

Throughout our operations, we abide by and frequently reference a range of established policies, including but not limited to:

- Asset Management Policy
- Data Management Policy
- Operations Security Policy
- Access Control Policy
- Business Continuity and Disaster Recovery Plan
- And more.

**Contact Information**

For any queries or further information related to our security practices, kindly get in touch with: **Michael Yancon** *Chief Technology Officer* Email: michael.yancon@absoluteautomations.com