Security Report

ATTN:
Chief Technology Officer
Altamaha Tech, Inc.
313 East Seven Mile Road
Detroit, MI 48235

Dear Altamaha Tech, Incorporated,

This document contains a comprehensive report of Altamaha Tech cyber security posture. This report will provide a high-level overview of the operational details of the organization based on internal and external assessment methods. The assessment evaluated processes, procedures and technologies utilized for primary business functions. This includes the information technology infrastructure physical and logical configuration. This report will provide your organization with the required information to implement an improved cybersecurity posture, which will focus on securing future projects and programs. Our specific evaluation finding is listed below:

1. During a review of Altamaha Tech Inc. cybersecurity policies we found that the organization lacked most basic security policies. We recommend that the organization develop proper acceptable use, passwords, and mobile device management policies. Also, the organization will develop cybersecurity awareness training and education programs in order to supplement the administrative controls and written policies.

2. Altamaha Tech Inc. develop, manufacture, sell and service wearable medical devices. The medical devices collect sensitive data about the patients that utilize the devices. This information is considered PII and the organization has to ensure that this PII data is stored, and accessed in accordance with United States and international laws and regulations. Altamaha Tech Inc. is lacking some policies and procedures that address issues with compliance with information privacy laws and regulations.
    a. **Personally Identifiable Information:** Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
    b. **The General Data Protection Regulation (GDPR)** is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

c. **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)** is a federal law that requires the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. Investigators were unable to identify specific measures within the organization to maintain compliance with measures to protect information that is collected, processed and stored.

3. Altamaha Tech Inc. uses methods to process and accept payments for products and services. Payment methods used by customers utilizes credit cards (debit) or corporate cards for internal acquisitions. PCI DSS is an information security standard administered by the Payment Card Industry Security Standards Council that is for organizations that handle branded credit cards from the major card schemes. Altamaha Tech Inc. needs to ensure compliance with PCI DSS guidelines. Failure to do so may subject Altamaha Tech Inc. to penalty or sanction as outlined in the standard. Currently, a policy document or standardized procedure or other guidance is lacking to outline how Altamaha Tech Inc. accepts these payments in accordance with PCI DSS.

4. When assessing security controls both physical and logical to determine the organizations approach to cybersecurity risk management. The investigators reviewed a list of assets located with the company but failed to find an updated list of threats and vulnerabilities for all associated assets. We recommend developing a risk register to monitor, track and calculate risks within the organizations.

End of Report.