NO.DG-II/Cyber. Advisory/4/111/2023

GOVERNMENT OF SINDH
INFORMATION SCIENCE & TECHNOLOGY DEPARTMENT

Karachi, Dated: 26th November, 2024

To

1. The Chairman, Enquires, Anti-Corruption, Establishment of Sindh, Karachi.
2. The Chairman Sindh HEC Karachi.
3. The Senior Member Board of Revenue (BOR)Sindh, Karachi.
4. The Additional Chief Secretary, Govt of Sindh_____
5. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
6. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
7. The Administrative Secretary, Government of Sindh (All).
8. The Provincial Ombudsman,Sindh.
9. The Inspector General of Police Sindh,Karachi
10. The Divisional Commissioner (All) in Sindh_____.
11. The Deputy Commissioner, District _____

Subject: - **CYBER SECURITY ADVISORY- CYBER SECURITY IMPLICATIONS OF WEARABLE DEVICES (ADVISORY NO.21001).**

Context. In light of increasing concerns regarding the security risks associated with workable smart devices, extreme vigilance and caution must be exercised when personal are permitted wear such devices in environments where classified or sensitive information is discussed or handled potential for data leakage through wearable devices, particularly in high-security offices, meetings other critical locations, presents a significant threat to organizational cybersecurity.

2. **Case Studies.** Some cases in point are as under:

a. In 2018, exposure of Fitbit user location data raised concerns about the unauthorized tracking of key personnel, as fitness data from the device's GPS inadvertently disclosed the whereabouts of secret locations

b. Known vulnerabilities in Apple Watch have allowed third-party apps to exploit insufficient permissions, enabling them to bypass authentication safeguards and gain unauthorized access.

c. The 2020 ransomware attack on Garmin led to the encryption of Garmin's data, causing significant operational downtime and loss of services, including aviation and fitness tracking. The company incurred financial losses estimated to be in the millions of dollars to restore its systems

3. **Need for Prior Formal Auditing and Approval of Devices.** Before any wearable devices are authorized for use (if required) in sensitive locations, a formal evaluation and auditing process must be conducted. This evaluation should include a comprehensive review of the device's security architecture, encompassing data encryption standards, vulnerability to external threats, and the adequacy of user authentication mechanisms. Any device found to have insufficient security controls or vulnerabilities must not be approved for use until these concerns are fully addressed. Once a device passes this formal evaluation, explicit approval is to be obtained, ensuring that the device meets all organizational security standards.