Subject: **Cyber Security Advisory – Cyber Security Implications of Wearable Devices (Advisory No. 21)**

Context. In light of increasing concerns regarding the security risks associated with wearable smart devices, extreme vigilance and caution must be exercised when personal are permitted to wear such devices in environments where classified or sensitive information is discussed or handled. The potential for data leakage through wearable devices, particularly in high-security offices, meetings or 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 addresses. Once a device passes this formal evaluation, explicit approval to be obtained, ensuring that the device meets all organizational security standards.

4. **Guidelines for Use of Approved Devices**

   a. **Device Prohibition in Critical Areas**. Wearable smart devices should be prohibited in areas where sensitive discussions, decisions or operations occur.

b. **Mandatory Security Assessments**. Wearables approved for use, shall undergo through security assessments, including vulnerability testing of the device's operating system, applications, connectivity protocols (e.g. Bluetooth, Wi-Fl) and encryption standards, prior to deployment.

c. **Disabling of Non-Essential Features**. GPS, Near Field Communication (NFC), Bluetooth Low Energy (BLE) and any other communication features which are not explicitly required for the device's operation in the sensitive environment should be completely disabled to minimize attack vectors.

d. **Regular Firmware and Software Updates**. All devices should be maintained with up-to-date firmware and security patches to mitigate known vulnerabilities. Devices failing to meet these criteria should not be permitted.

e. **Restricted Network Access**. Wearable devices should not be allowed to connect to the organization's internal networks or systems unless rigorous security measures, including network segmentation and encryption are in place.

f. **Secure Authentication Mechanisms**. Personnel must ensure that wearable devices are protected with strong, multi-factor authentication (MFA) mechanisms. Devices lacking such mechanisms should not be used in sensitive locations.

g. **Periodic Security Audits**. Security audits of wearable devices, both in terms of software integrity and data transmission, should be conducted regularly to ensure continued compliance with organizational security policies.