11.5. Personal Wearable Devices

Objective

11.5.1. Wearable devices are prevented from unauthorised communication or from compromising secure areas.

Context

Scope

11.5.2. This section covers information relating to the use of personal wearable devices, fitness devices, smart watches, devices embedding in clothing and similar wearable devices.

11.5.3. These devices can use RF in various parts of the spectrum to communicate including Wi-Fi, cellular, satellite, RFID, NFC and Bluetooth frequencies as well as providing data storage capability, audio and video recording and USB connectivity. All such wearable or mobile devices are considered to be transmitters.

11.5.4. Personal wearable devices can be equipped with a variety of capabilities including smart phone pairing, internet connectivity, cameras, speakerphones, audio and video recording and remote control. Some devices (for example Narrative and Autographer) will automatically take snapshots at intervals during the day. In some cases the snapshots are geotagged.

11.5.5. Such devices are also susceptible to Internet malware and exploits. All risks related to the use of the Internet will apply to these devices.

11.5.6. Merely disabling the capabilities described above is not a sufficient mitigation and is not acceptable, posing a high risk of compromise, whether intentional or accidental. The device MUST NOT have such capabilities installed if the device is to enter a secure area.

11.5.7. There is a wide variety of devices now available with upgrades and new models appearing frequently. There are many hundreds of models with a variety of custom operating systems and programmes and other applications. Some industry surveys and predications are forecasting explosive growth in the use of wearable devices, reaching over 100 million devices by 2020. Checking the capabilities and vulnerabilities of each device and subsequent security testing or validation will be an onerous task for agencies and may be infeasible.

Key Risk Areas

11.5.8. Personal wearable devices are not only about the technological aspects, the human factor is equally important. Users often forget about personal information security and their own safety, which enables social engineering attacks on the devices. The main protective measure for users is awareness, but even the *trust-but-verify* rule is not completely reliable in this situation. Accordingly, the information gathered by wearable devices should be appropriately secured to maintain privacy and personal security.

11.5.9. There are four important risk groups to be considered when managing personal wearable devices:

1. Data leaks and breaches;
2. Network security compromises;
3. Personal information leaks; and
4. Privacy violations.

Personal Information

11.5.10. In most cases, the protection of personal information will be the responsibility of the individual. In cases where the use of devices is permitted under a medical exemption, agencies MAY be required to ensure that devices that collect and store data comply with relevant regulation and guidance, such as the Privacy Act.

PSR references

11.5.11. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Physical security (PHYSEC) | Protective Security Requirements

References

11.5.12. Further references can be found at:

Reference	Title	Publisher	Source
ITL bulletin for April 2010	**Guide to protecting personally identifiable information**	NIST	https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul2010-04.pdf [PDF, 50 KB]
SP 800-122	**Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) - Recommendations of the National Institute of Standards and Technology**	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf [PDF, 800 KB]
	Privacy Act 2020	Office of The Privacy Commissioner	https://privacy.org.nz/ https://legislation.govt.nz/
	The Health Insurance Portability and Accountability Act of 1996 (USA)	US Congress	https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm https://www.hhs.gov/hipaa/index.html
	Health Information Technology for Economic and Clinical Health Act (HITECH Act) (USA)	US Congress	https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf [PDF, 881 KB] http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html
	Technology, Media and Telecommunications Predictions, 2014	Deloitte	https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-predictions-2014-interactive.pdf [PDF, 1.05 MB]
	Technology, Media and Telecommunications Predictions, 2015	Deloitte	https://www2.deloitte.com/au/en/pages/technology-media-and-telecommunications/articles/tmt-predictions.html
	Study: Wearable Technology & Preventative Healthcare	Technology Advice Research	http://technologyadvice.com/
	Security Analysis of Wearable Fitness Devices (Fitbit)	Massachusetts Institute of Technology	https://courses.csail.mit.edu/6.857/2014/files/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf [PDF, 630 KB]
	Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device	School of Computing and Information Sciences, Florida International University	https://arxiv.org/pdf/1304.5672.pdf [PDF, 541 KB]
	Survey of Security and Privacy Issues of Internet of Things		http://arxiv.org/ftp/arxiv/papers/1501/1501.02211.pdf [PDF, 548 KB]

Rationale & Controls

Personal Wearable Device usage policy

11.5.13.R.01. **Rationale**

Any device that uses part of the RF spectrum to communicate is subject to interception. The required level of expertise to conduct intercepts needed varies greatly. Other capabilities of Personal Wearable Devices can be used for malicious purposes, including the theft of classified information and revealing the identities of personnel. Accidentally or maliciously revealing classified information through Personal Wearable Devices can lead to a security breach.

11.5.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2736]

Agencies MUST develop a policy governing the use of personal wearable devices, including fitness devices.

Personnel awareness

11.5.14.R.01. **Rationale**

There is a high risk of unintended disclosure of classified information when using personal wearable devices. It is important that personnel are aware of the level of classified information they discuss, the environment in which they are operating as well as the wide range of security risks associated with the use of mobile and personal wearable devices.

11.5.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2750]

Agencies MUST advise personnel of the maximum permitted classification for conversations where any personal wearable or mobile device may be present.

11.5.14.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2752]

Agencies SHOULD advise personnel of all known security risks posed by using personal wearable devices in secure areas or other areas where classified conversations can occur.

Mobile Device Physical Security

11.5.15.R.01. **Rationale**

Personal wearable devices are invariably software controlled and can be infected with malware or other means of compromise. No “off-hook” or “power off” security can be effectively provided, creating vulnerabilities for secure areas. Secure areas are defined in Chapter 1 at 1.1.36.

11.5.15.C.01. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must Not** [CID:2758]

Personal wearable devices MUST NOT be allowed to enter secure areas.

11.5.15.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2759]

Agencies SHOULD provide a storage area or lockers where personal wearable devices can be stored before personnel enter secure or protected areas.

Medical Exemptions

11.5.16.R.01. **Rationale**

In some isolated cases personal wearable devices are necessary for the medical well-being of the individual. In such cases personal wearable devices MAY be permitted with the written authority of the Agency’s Accreditation Authority. Such devices MUST NOT have any of the following capabilities:

- Camera;
- Microphone;
- Voice/video/still photograph recording;
- Cellular, Wi-Fi or other RF.

Merely disabling such capabilities is not acceptable. The device MUST NOT have such capabilities installed. Permitted device capabilities are:

- Accelerometer;
- Altimeter;
- Gyroscope;
- Heart Activity monitor;
- Vibration feature for the personal notification purposes.

11.5.16.R.02. **Rationale**

Personal wearable devices may contain personal information of the individual using the device. This may be on the device itself in printed or electronic form, and also in the registers of tested, permitted or rejected devices in use within the agency. It is important that relevant legislation and regulation pertaining to the protection of personal information is followed.

11.5.16.C.01. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must Not** [CID:2763]

Any personal wearable devices approved on medical grounds MUST NOT have any of the following capabilities:
Camera;
Microphone;
Voice/video/still photograph recording;
Cellular, Wi-Fi or other RF means of transmission.

11.5.16.C.02. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:2765]

Where personal wearable devices are exempted on medical grounds and used in secure areas agencies MUST ensure that:

- the agency networks in secure areas have been certified and accredited for the purpose; and

- users are aware of the area, surroundings, potential for overhearing and potential for oversight.

11.5.16.C.03. **Control System Classifications(s): All Classifications; Compliance: Must [CID:2767]**

Where the use of personal wearable devices is permitted on medical grounds and used within a corporate or agency environment, agencies MUST ensure any relevant legislation and regulation pertaining to the protection of personal information is followed.