Air Force Research Laboratory
Wright Research Site Security Requirements (SEP 2023)

(a) *Definitions.* As used in this article –

Air Force Research Laboratory (AFRL)-managed facilities means -

(1) AFRL buildings, areas, test facilities, and laboratories located at the AFRL Wright Research Site, Wright-Patterson Air Force Base (WPAFB), Ohio;
(2) Buildings owned or facility space leased by the AFRL Wright Research Site, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody, or control of the AFRL Wright Research Site;
(3) Commercial space managed by the AFRL Wright Research Site that is shared with non-government tenants. For example, if the AFRL Wright Research Site leased the 10th floor of a commercial building, the directive applies to the 10th floor only;
(4) Awardee-operated facilities owned by the AFRL Wright Research Site, including laboratories engaged in national defense research and production activities.

Augmented reality (AR) device means a device that is capable of, or assists in, augmented reality by enhancing or creating digital overlays. AR is used to enhance natural environments or situations and offers perceptually enriched and interactive experiences achieved through digital visual elements, sounds, and other sensory stimuli via holographic technology. Examples include, but are not limited to, hardware components such as display sensors, computers, projectors, input devices, mobile devices, eyewear, wireless communication devices, and cameras.

Data storage device means computer hardware used to remember/store data. Examples include, but are not limited to, remote or autonomous drones, CDs, DVDs, Blue-Rays, USB flash drives, jump/stick/pen drives, external hard drives, solid state drives, cloud storage, mainframes, laptops, desktops, and flop disks.

Formal investigation means the process of investigation ordered by a competent U.S. Government authority that involves the questioning of involved parties and gathering of data with the intent to determine if classified or controlled unclassified information (CUI) was lost, compromised, suspected to be compromised, or not compromised at all.

Personal means items that are owned by an individual, person, or private entity and not provided for use under this grant or agreement by the U.S. Government.

Physical computer network means interconnected computing devices of any kind that can exchange data and share resources or communicate with other types of devices to execute operations or store information of any kind.

Security Incident Investigation (SII) means a formal investigation that occurs when there is a known or suspected loss of national security information (NSI) or CUI. U.S. Government security personnel conduct SIIs to (1) determine the circumstances surrounding an actual or potential compromise of NSI or CUI; (2) ascertain individual responsibility; (3) notify outside stakeholders, when necessary; and (4) make recommendations to prevent similar occurrences in the future.

Virtual device means a device with no associated hardware. A virtual device mimics a physical hardware device when, in fact, it exists only in software form. Therefore, the device makes the system believe that a particular hardware exists when in reality it does not. Examples include, but are not limited to, a computer, tablet, or smartphone that is simulated in a computer.

(b) *Prohibition.* The following is prohibited within AFRL-managed facilities, except when explicitly authorized by a U.S. Government grant or agreement:

(1) Prohibited activities -

a. Photography
b. Videography
c. Live Streaming
d. Recordings of any kind (e.g., audio)

(2) Prohibited personal networks and devices -

a. AR devices
b. Virtual devices
c. Wi-Fi networks
d. Physical computer networks
e. Data storage devices

(c) *Waivers.* A request for a waiver to the prohibitions outlined in paragraph (b) shall be submitted in writing to the Government Program Manager for internal Government coordination and approval. If a waiver request is granted, written approval shall be provided by the cognizant AFRL Operations Security (OPSEC) coordinator and Security Chief. The specific format for a waiver request will be provided upon request to the Government Program Manager.

(d) *Incident Reporting Requirement.* If the awardee discovers a prohibited activity identified in paragraph (b)(1) has occurred within an AFRL-managed facility and/or a prohibited personal network or device identified in paragraph (b)(2) has been brought into an AFRL-managed facility without a valid waiver, as specified in paragraph (c), the incident shall be immediately reported in writing to the Government Program Manager with a courtesy copy to the Grant/Agreement Officer.

(e) *Violations.* If a violation of this article occurs or is suspected to have occurred, the cognizant AFRL security organization will lead and conduct a formal investigation. If a violation or suspected violation may involve classified material, the cognizant AFRL security organization will lead and conduct a Security Incident Investigation (SII). Depending on the outcome of the investigation and the information involved, penalties for violations can range from a written warning to removal from the AFRL-managed facility and/or installation. Violations and potential penalties will be governed by the applicable articles(s), law(s), or regulation(s).

(f) *Subawards/Subcontracts.* The awardee shall include this article in all subawards/subcontracts or similar contractual instruments/agreements relating to work performed under this grant or agreement.

(End of article)