## Dogfooding Program Security Guidelines

## You’ve Volunteered to Dogfood a Confidential Product/Project!

As part of the Dogfooding program, you will have the opportunity to preview some of our latest innovations and provide essential feedback to help with continued development of cutting-edge technology. This is an amazing opportunity and a big responsibility. You may be issued a Confidential Product or Prototype Device to take home that is to be used only at home or other locations as specified by the Dogfooding Coordinator.

**REMEMBER** – *You are responsible for the safekeeping of*[redacted] *product(s) and are obligated under the terms of your Non-Disclosure Agreement (NDA) to maintain the confidentiality of Intellectual Property and Confidential Information. Please review the Protecting Intellectual Property (IP) & Confidential Information (CI) guidelines.*

**To facilitate your responsibilities, please follow the requirements below:**

|  |
| --- |
| **Best Practices** |
| 1. **Follow employee hand carry guidelines**  * Head straight home – no pit stops! * Conceal confidential assets, IP devices, and any other confidential information in transit using a dark opaque bag or similar container. * If you are transporting documents, do not leave them anywhere where they can be viewed by the public (e.g., on the seat of your car).  Keep them in your backpack! * If taking transportation (shuttles, trains, etc.), keep the IP (e.g., devices/software/prototypes) and other CI in your direct possession at all times until you arrive at your destination. * If you are utilizing a personal vehicle, make sure IP devices and other confidential information is out of sight and secured in lockable compartments, if available. Remove IP and confidential materials from the vehicle as soon as you arrive home. * If you are using a rideshare service, keep confidential materials close to you to ensure it does not get left behind. * For additional hand carry guidelines, please review Employee Work from Home Hand Carry Guidelines.  1. **Secure Shipping**  * The transport of unreleased [redacted] assets and [redacted] is handled by the [redacted] team. The team will work closely with the Dogfooding Team for the allocation, distribution, and return of devices. For inquiries, please reach out to the [redacted] team.  1. **Protect IP, CI, and confidential devices at home**  * Retain all packaging and printed materials with the same level of care as IP devices. * Ensure IP devices are always password-protected and if possible, use Two-factor authentication (2FA). * Know where the IP devices and other CI are at all times. * Ensure the device or other CI are not used or stored in the public view of house guests or other visitors. * Ensure all IP devices and other CI are secured and covered when not in use (e.g., lockable cabinet, container or safe). * Ensure printed documents containing IP & CI are destroyed properly when no longer needed. (e.g., use a shredder or dispose of them in the confidential document bins in the office).  1. **Outdoor usage Best Practices**  * If outdoor testing is applicable:   + Visual deterrents are necessary to obscure the device from the line of sight of unauthorized persons.   + If testing on a terrace, balcony, be aware of surroundings and neighboring buildings. * Camouflage the design of the device.   + [redacted].   + Use assistant wakeword and other product functionality when there are no bystanders around.   + Be vigilant of the volume, voice, and tone while interacting with the device. * Ensure that the device is kept on the user's person at all times during the testing and concealed when not in use, or in transit to/from the location. * Ensure not to capture any non-consenting bystanders in images and/or video. All subjects in the image/video should have explicit consent through the NDAs.   + If the user is approached by a bystander, disclose that the user is capturing data for product development and nothing more.   + Use general descriptions (e.g., [redacted]) to not reveal the [redacted] brand. * Expect questions and have prepared answers for law enforcement or property owners that may question the activity:   + Answers should be general; disclose only as much information as requested.   + Use general descriptions (e.g., [redacted]) to not give brand specific information.  1. **Maintain inventory control of Dogfooding products and verify it daily**  * Conduct inventory control of all IP devices daily to ensure the device is in your presence * Employees must update location changes, employee transfers, or change in device status in the inventory database. * If you notice missing, lost, or stolen items, follow the below escalation process.      1. **Return the Dogfooding product promptly**    * As part of the Dogfooding process, there may be a need to recall devices to exchange for an updated version or to collect at the end of a project. These [redacted] assets must be returned upon request. The following process will assist with returning:    * A Dogfooding Coordinator will contact you to discuss logistics for return of the device.    * If there is no response after two attempts to contact you, the device will be escalated to Global Security for further action. 2. **Escalate Dogfooding losses and/or leaks (actual or suspected)**  * Report any unplanned disclosures, missing, lost or stolen items. * Notify your Dogfooding Coordinator immediately. * Escalate to [redacted] immediately at [redacted]. The operator will guide you through the reporting process. |

|  |
| --- |
| **Restrictions** |
| * **Do not** travel with IP devices outside of your home without approval. * **Do not** work with IP devices at unapproved spaces. Unapproved spaces include, but are not limited to, the following: * Common areas where other non-disclosed parties may be present * Public areas like coffee shops, houses of worship, malls, public streets, airports, trains, friend’s home, etc. where bystanders are clearly visible * A private property the user does not rent or own * **Do not** give IP & CI to others for transportation unless authorized by Global Product Security. * **Do not** share and/or disclose the IP & CI with anyone else in your household, or any guests. This includes close friends, family members, or spouses unless they work for [redacted]. * **Do not** take photos, videos, or other recordings of IP & CI unless approved by management. * **Do not** post photos, videos, or any recordings of IP & CI to social media unless approved by management. * **Do not** leave the IP & CI unsecured while non-authorized persons are in the residence and/or you are not at your residence. * **Do not** sell, loan, or gift IP & CI to anyone including family members and co-workers who are not authorized. |

|  |  |  |
| --- | --- | --- |
| **Escalations** | **Contact Info** | **Resources** |
| For Prototypes | [redacted, here and below] | [redacted, here and below] |
| Specifically for [device] Dogfooding |  |  |
| Global Product Security |  |  |
| Global Security Operations Center |  |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Update | Reviewer |
| V 2.2 | 01/04/22 | URL updates and other edits | John Walasik |