ACCEPTABLE USE POLICY

Last Updated Date: July 1, 2026

This Acceptable Use Policy is made part of and included in the General Terms by reference. All capitalized terms have the meaning set forth in the General Terms.

In addition to any requirements and obligations in the General Terms, Customer acknowledges and agrees to:

- Not probe, scan, or test the vulnerability of any Arctic Wolf Technology, including any sensor, system, or network without prior written notice to Arctic Wolf;
- Not breach or otherwise circumvent any security or authentication measures;
- Not Access, tamper with, or use non-public areas or parts of the Products, or shared areas of the Products of which access has not been granted by Arctic Wolf;
- Not interfere with or disrupt any user, host, or network (e.g. sending a virus, intentionally overloading, flooding, spamming, or mail-bombing any part of the Products);
- Not access or search the Products by any means other than our publicly supported interfaces (e.g., "scraping");
- Not restrict, inhibit, interfere with, or otherwise intentionally disrupt or cause a performance degradation to the Products, or otherwise cause a performance degradation to any Arctic Wolf (or Arctic Wolf supplier) facilities;
- Not alter, modify, or tamper with the Products or permit any other person to do the same who is not first authorized to do so by Arctic Wolf;
- Not provide guidance, information, or assistance which may cause damage or a security breach to Arctic Wolf's network or systems;
- Use commercially reasonable efforts to implement and enforce multi-factor authentication (MFA) for all accounts where Arctic Wolf makes such controls available;
- Maintain accurate records of the systems, endpoints, and environments for which the Products are deployed; and
- Reasonably cooperate with Arctic Wolf's onboarding, configuration, and operational requirements to enable effective Product delivery;
- Not to transmit, upload, store, or process Data that contains malware, ransomware, destructive code, or other harmful content not authorized by Arctic Wolf as part of a managed security test;
- Not to submit to the Products any Special Categories of Data (as defined under GDPR), Protected Health Information (as defined under HIPAA), or payment card data (within scope of PCI DSS) unless Customer has obtained the applicable written authorization from Arctic Wolf and executed any required supplemental terms; and
- Not use Arctic Wolf Technology, including but not limited to any artificial intelligence prompts or outputs, to develop, train, or improve data sets, foundation models, LLMs, or other models that may compete with Arctic Wolf Technology.

ARCTIC WOLF RESERVES THE RIGHT TO NOTIFY ITS CUSTOMERS OF ANY INFORMATION THAT AFFECTS THE SECURITY OF ARCTIC WOLF PRODUCTS.