

ACCEPTABLE USE POLICY

Last Updated Date: June 17, 2019

Customer acknowledges and agrees not to or attempt to:

- Probe, scan, or test the vulnerability of any sensor, system, or network without prior written notice to Arctic Wolf;
- Breach or otherwise circumvent any security or authentication measures;
- Access, tamper with, or use non-public areas or parts of the Solutions, or shared areas of the Solutions of which access has not been granted by Arctic Wolf;
- 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 Solutions);
- Access or search the Solutions by any means other than our publicly supported interfaces (e.g., “scraping”);
- Restrict, inhibit, interfere with, or otherwise intentionally disrupt or cause a performance degradation to the Solutions, or otherwise cause a performance degradation to any Arctic Wolf (or Arctic Wolf supplier) facilities;
- Alter, modify, or tamper with the Solutions or permit any other person to do the same who is not first authorized to do so by Arctic Wolf;
- Provide guidance, information, or assistance with respect to causing damage or a security breach to Arctic Wolf’s network or systems.

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