

STAFF REPORT*CITY OF OCEANSIDE*

DATE: June 21, 2023

TO: Honorable Mayor and City Councilmembers

FROM: Human Resources Department, Information Technologies Division

SUBJECT: **AGREEMENT AND PURCHASE ORDER FOR THE DEPLOYMENT OF THE ARCTIC WOLF CYBERSECURITY SOLUTION**

SYNOPSIS

Staff recommends that the City Council approve a solutions agreement with Arctic Wolf and a three-year purchase order, in an amount not to exceed \$444,639, to CDW Government (CDWG) for the purchase of the Arctic Wolf Cybersecurity Solution; authorize the City Manager to execute the agreement; and authorize the Financial Services Director, or designee, to execute the purchase order.

BACKGROUND

The City's Information Technologies Division is responsible for monitoring and protecting the City from threats to its servers and data. Cyber attacks have been a growing concern for a number of years, and it takes proper tools and educated teams to prevent malicious and criminal attacks that can have harmful and financial repercussions. The City currently deploys a solution that has limited monitoring support for external threats, but lacks a more comprehensive platform that would provide 24/7 monitoring, internal and host-based scanning, rapid incident response, log collection and professional vulnerability management guidance.

ANALYSIS

Founded in 2012, Arctic Wolf is a market leader in security operations, offering cloud-based platforms that provide active monitoring by a team of individuals rather than a passive system that relies solely on automated detection. Arctic Wolf offers a Managed Detection and Response Solution that will complement the City's existing efforts for detecting threats by adding much needed tools and access to experienced personnel. The proposed solution will bring 24/7 threat monitoring with active response to the City's data centers. Dedicated security engineers will be assigned to the City as contacts, and will proactively provide guidance on vulnerabilities, schedule regular posture reviews and create and review reporting.

The Arctic Wolf Managed Detection and Response Solution is provided through the City's distribution partner CDWG. CDWG is an authorized reseller and provides products and

technology services under a cooperative National IPA/OMNIA Technology Solutions contract (#2018011-01). The agreement price was quoted from the terms in that agreement.

FISCAL IMPACT

The total cost of the three-year purchase order is \$444,639 and will be charged to the Cybersecurity account 155168841.5320. The Department has a current vacancy in AD76CM01 (Security Officer) that will not be filled in FY 2023-24. Staff will use salary savings from that vacant position in the amount of \$156,552 to pay the year one cost; therefore, sufficient funds are available. Staff will return at a later date to either request separate funding for future years or to eliminate the position and use that savings to pay for future years.

Arctic Wolf Cybersecurity Solution		
	155168841.5320 Cybersecurity	Purchase Order
Funds available from vacant Security Officer position	\$ 156,552	
Year one cost (FY 2023-24)		\$ 147,860
Remaining account balance	\$ 8,692	
Year two cost		\$ 144,770
Year three cost		\$ 152,009
Total Purchase Order Amount		\$ 444,639

The funding source is Information Services Internal Service Fund 841.

COMMISSION OR COMMITTEE REPORT

Does not apply.

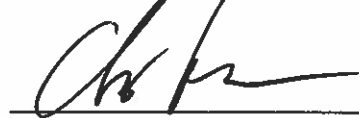
CITY ATTORNEY'S ANALYSIS

Purchases will be made according to the procedures set forth in Chapter 28A of the City Code.

RECOMMENDATION

Staff recommends that the City Council approve a solutions agreement with Arctic Wolf and a three-year purchase order, in an amount not to exceed \$444,639, to CDW Government (CDWG) for the purchase of the Arctic Wolf Cybersecurity Solution; authorize the City Manager to execute the agreement; and authorize the Financial Services Director, or designee, to execute the purchase order.

PREPARED BY:



Chris Freeman
IT Procurement Analyst

SUBMITTED BY:



Jonathan Borrego
City Manager

REVIEWED BY:

Robert O'Brien, Deputy City Manager

Dave Riha, Information Technologies Division Manager

Jill Moya, Financial Services Director



ATTACHMENTS:

A: Quote

B: Agreement



Thank you for choosing CDW. We have received your quote.

Hardware Software Services IT Solutions Brands Research Hub

Review and Complete Purchase

DAVID RIHA,

Thank you for considering CDW•G for your technology needs. The details of your quote are below. **If you are an eProcurement or single sign on customer, please log into your system to access the CDW site.** You can search for your quote to retrieve and transfer back into your system for processing.

For all other customers, click below to convert your quote to an order.

Convert Quote to Order

ACCOUNT MANAGER NOTES:

Please note: tax is NOT applicable for Year 2 and 3. Please disregard the added tax. Subtotal of \$444,637.22 is total 3 year cost.

QUOTE #	QUOTE DATE	QUOTE REFERENCE	CUSTOMER #	GRAND TOTAL
NJRV997	5/9/2023	AW MDR+MR 3YR	1969817	\$469,121.42

QUOTE DETAILS

ITEM	QTY	CDW#	UNIT PRICE	EXT. PRICE
<u>ARCTIC WOLF MDR USER LIC CLD</u> Mfg. Part#: AW-MDR-USER Electronic distribution - NO MEDIA Contract: National IPA Technology Solutions (2018011-01)	900	5839578	\$74.96	\$67,464.00
<u>Arctic Wolf Managed Detection and Response - license - 1 server</u> Mfg. Part#: AW-MDR-SE Electronic distribution - NO MEDIA Contract: National IPA Technology Solutions (2018011-01)	200	5744220	\$69.74	\$13,948.00
<u>ARCTIC WOLF MDR LOG RETENTION LIC 1Y</u> Mfg. Part#: AW-MDR-1YR Electronic distribution - NO MEDIA Contract: National IPA Technology Solutions (2018011-01)	1100	6124471	\$4.79	\$5,269.00
<u>Arctic Wolf Managed Detection and Response - subscription license - 1 senso</u> Mfg. Part#: AW-MDR-2XX-S Contract: National IPA Technology Solutions (2018011-01)	2	5745583	\$900.23	\$1,800.46
<u>Arctic Wolf Managed Detection and Response for Office 365 - subscription li</u> Mfg. Part#: AW-MDR-O365 Electronic distribution - NO MEDIA Contract: National IPA Technology Solutions (2018011-01)	200	5744235	\$7.49	\$1,498.00
<u>ARCTIC WOLF MR USER LIC CLD</u>	900	5839580	\$37.14	\$33,426.00

QUOTE DETAILS (CONT.)

Mfg. Part#: AW-MR-USER

Electronic distribution - NO MEDIA

Contract: National IPA Technology Solutions (2018011-01)

ARCTIC WOLF MR SVR LIC CLD

200

5744241

\$34.89

\$6,978.00

Mfg. Part#: AW-MR-SE

Electronic distribution - NO MEDIA

Contract: National IPA Technology Solutions (2018011-01)

ARCTIC WOLF IR JUMPSTART RETAINER

1

7251118

\$0.00

\$0.00

Mfg. Part#: AW-IR-JSR

Electronic distribution - NO MEDIA

Contract: National IPA Technology Solutions (2018011-01)

Arctic Wolf Platform - Base license - 1 license

1

7040196

\$870.60

\$870.60

Mfg. Part#: AW-PLATFORM-BASE

Electronic distribution - NO MEDIA

Contract: National IPA Technology Solutions (2018011-01)

Arctic Wolf Platform - license - 1 access

1100

6773750

\$6.02

\$6,622.00

Mfg. Part#: AW-PLATFORM

Electronic distribution - NO MEDIA

Contract: National IPA Technology Solutions (2018011-01)

ARCTIC WOLF MDR ONBOARDING CLDS

1

5749862

\$6,789.03

\$6,789.03

Mfg. Part#: AW-MDR-OB

Electronic distribution - NO MEDIA

Contract: National IPA Technology Solutions (2018011-01)

ARCTIC WOLF MGD RISK ONBOARD CLDS

1

5749357

\$3,193.92

\$3,193.92

Mfg. Part#: AW-MR-OB

Electronic distribution - NO MEDIA

Contract: National IPA Technology Solutions (2018011-01)

NEW ITEM

1

NEW-ITEM

\$144,769.86

\$144,769.86

Mfg. Part#: NEW-ITEM

Year 2 cost (based on today's configuration): \$144,769.86

Contract: Standard Pricing

NEW ITEM

1

NEW-ITEM

\$152,008.35

\$152,008.35

Mfg. Part#: NEW-ITEM

Year 3 cost (based on today's configuration): \$152,008.35

Contract: Standard Pricing

These services are considered Third Party Services, and this purchase is subject to CDW's [Third Party Cloud Services Terms and Conditions](#), unless you have a written agreement with CDW covering your purchase of products and services, in which case this purchase is subject to such other written agreement.

The third-party Service Provider will provide these services directly to you pursuant to the Service Provider's standard terms and conditions or such other terms as agreed upon directly between you and the Service Provider. The Service Provider, not CDW, will be responsible to you for delivery and performance of these services. Except as otherwise set forth in the Service Provider's agreement, these services are non-cancellable, and all fees are non-refundable.

SUBTOTAL**\$444,637.22**

SHIPPING _____ \$0.00

SALES TAX _____ \$24,484.20

GRAND TOTAL _____ \$469,121.42

PURCHASER BILLING INFO

Billing Address:
CITY OF OCEANSIDE
ACCTS PAYABLE
300 N COAST HWY
OCEANSIDE, CA 92054-2859
Phone: (760) 435-3065
Payment Terms: NET 30-VERBAL

DELIVER TO

Shipping Address:
CITY OF OCEANSIDE
DAVE RIHA
300 N COAST HWY
OCEANSIDE, CA 92054-2859
Phone: (760) 435-3065
Shipping Method: FEDEX Ground

Please remit payments to:

CDW Government
75 Remittance Drive
Suite 1515
Chicago, IL 60675-1515



Sales Contact Info

Jay Moore (State and Local Government) | (877) 685-2961 |
jay.moore@cdwg.com

LEASE OPTIONS

FMV TOTAL	FMV LEASE OPTION	BO TOTAL	BO LEASE OPTION
\$444,637.22	\$11,800.67/Month	\$444,637.22	\$13,663.70/Month

Monthly payment based on 36 month lease. Other terms and options are available. Contact your Account Manager for details. Payment quoted is subject to change.

Why finance?

- **Lower Upfront Costs.** Get the products you need without impacting cash flow. Preserve your working capital and existing credit line.
- **Flexible Payment Terms.** 100% financing with no money down, payment deferrals and payment schedules that match your company's business cycles.
- **Predictable, Low Monthly Payments.** Pay over time. Lease payments are fixed and can be tailored to your budget levels or revenue streams.
- **Technology Refresh.** Keep current technology with minimal financial impact or risk. Add-on or upgrade during the lease term and choose to return or purchase the equipment at end of lease.
- **Bundle Costs.** You can combine hardware, software, and services into a single transaction and pay for your software licenses over time! We know your challenges and understand the need for flexibility.

General Terms and Conditions:

This quote is not legally binding and is for discussion purposes only. The rates are estimate only and are based on a collection of industry data from numerous sources. All rates and financial quotes are subject to final review, approval, and documentation by our leasing partners. Payments above exclude all applicable taxes. Financing is subject to credit approval and review of final equipment and services configuration. Fair Market Value leases are structured with the assumption that the equipment has a residual value at the end of the lease term.

Need Help?



My Account



Support



Call 800.800.4239

[About Us](#) | [Privacy Policy](#) | [Terms and Conditions](#)

This order is subject to CDW's Terms and Conditions of Sales and Service Projects at

<http://www.cdwg.com/content/terms-conditions/product-sales.aspx>

For more information, contact a CDW account manager

© 2023 CDW•G LLC, 200 N. Milwaukee Avenue, Vernon Hills, IL 60061 | 800.808.4239



May 3rd, 2023

Executive Proposal: SOC-as-a-Service



Prepared By: Arctic Wolf & CDW-G

Aaren Larsen – Sr. Account Executive

David Ta – Sr. Systems Engineer



THE LEADER IN SECURITY OPERATIONS

Outline

- 01 Project Discussion**
- 02 Why Arctic Wolf**
- 03 Pricing, Benefits, & ROI**
- 04 Solution Overview**
- 05 Onboarding / Implementation Timeline**

Project Discussion

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Confidential



Project Discussion – What We Heard

Current State:

- No 24x7 monitoring / environment-wide log management today (network, endpoint, cloud, & identity)
- Monitoring network via CIS Albert service
- Only external vulnerability scanning today, no internal or host-based scanning, etc.
- Lean team that wear a lot of hats and do not have the time or systems to detect & respond to threats efficiently or effectively
- No comprehensive vulnerability management product/service today to identify and measure risk in environment

Business Initiative:

- Looking for 24x7 Security Operations Center (SOC) Partnership
 - Guidance of current threats / market trends
 - Recommendations on posture improvements
 - Monitor entire environment 24x7 (network, endpoint, cloud, & identity)
 - Minimize noise and provide actionable business outcomes
 - Contain threats in the event of an incident
 - Manage risk through effective vulnerability management strategy

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Confidential



Why Arctic Wolf

©2023 Arctic Wolf Networks Inc. All rights reserved. | Classification: Confidential



ARCTIC WOLF OVERVIEW

Arctic Wolf® is the market leader in security operations. We use our cloud-native security operations platform to deliver security as a concierge service. Taking the operational approach to cybersecurity means that we can protect our customers in a uniquely effective way. Our protection is personal because members of the Concierge Security® Team are paired with customers to develop a close working relationship and tailor our solutions to their unique needs. Our protection is predictable because the scope of the solution includes both tactical actions as well as strategic, long-term security objectives. The ultimate outcome that we deliver for the customer is personal, predictable, protection.

The cybersecurity industry has an effectiveness problem.

3,500+ Vendors
\$120B+ Total Spend
3500+ Reported Breaches

About Arctic Wolf

2012 Founded
3,000+ Employees
3.8k+ Customers



THE LEADER IN SECURITY OPERATIONS

Industry Cybersecurity Challenges

Mean Time to Identify (MTTI)
Malicious and Criminal Attacks

Mean Time to Contain (MTTC) the Attack



Audit/Compliance Drivers

• PCI DSS • FFIEC-NCUA • HIPAA • NIST 800-171 • 23 NYCRR 500

Better Protection Against All Attack Types

Dwell Time	Time of Attack	Advanced Threats	Account Takeover	Unpatched Vulnerabilities
0:30	40%	43%	70%	58%
Industry average time to identify an intrusion is 214 days. Arctic Wolf does it in 30 minutes or less.	Threats that were detected after 8PM and before 8AM by Arctic Wolf	Of customers have advanced threat activity being missed by security tools but caught by Arctic Wolf	Of customers have some PII exposure and 5.5% have plaintext passwords exposed online	Reduction in time to patch critical vulnerabilities after activating Arctic Wolf

Arctic Wolf Detects & Responds to the Top 5 Attack Vectors:

- Malware/Ransomware
- Phishing
- PUP Adware
- Account Hijacking
- Unpatched Outdated Software

Classification: Confidential



Why Arctic Wolf

THE LEADER IN SECURITY OPERATIONS

- The Proposed Arctic Wolf solution will assist City of Oceanside with aligning to the NIST Cybersecurity Framework and proactively protecting City of Oceanside 24x7 from advanced threats & the evolving threat landscape
 - 2-3 US based Concierge Security Engineers/Analysts who help support City of Oceanside's IT Team
 - 24x7x365 Managed Detection and Response
 - 24x7 Triage Team triaging all alerts
 - Active DNS Monitoring
 - Managed Intrusion Detection System (IDS)
 - Reduction in the Mean-Time To Identify (MTTI) and Remediate Cybersecurity Incidents (30-minutes or less)
 - Potential for Reduced Cyber Insurance Premiums
 - Broad Visibility and Unlimited data ingestion across the entire City of Oceanside attack surface
 - Centralized Log Collection with 1-year log retention period
 - Unlimited Remote Incident response assistance, Expert-guided Remediation, and Incident Response Jumpstart Planning
 - Active Response (host-based isolation) via Arctic Wolf Agent & Network containment via Arctic Wolf Sensor
 - Security Posture Guidance:
 - Architecture & Configuration Reviews
 - CIS Controls
 - Root Cause Analysis
 - Security Posture In-depth Reviews, aka SPIDRs
 - Comprehensive vulnerability management services to minimize risk posture of organization



THE LEADER IN SECURITY OPERATIONS

Arctic Wolf Key Differentiators

- 2-3 US based Security Engineer/Analysts who help support City of Oceanside's IT Team
 - We own security outcomes with you!
- **Unlimited Data Ingestion** → No limits around cost/gb or cost/event/sec allowing you to capture visibility of your entire attack surface
- **Vendor agnostic** → We leverage your existing tools technology stack
- **Broad Visibility across the entire City of Oceanside attack surface:**
 - Network - Ingress/Egress Network Flow data
 - Unlimited network flow data
 - Commercial Threat Feeds
 - Network - Asset Profiling (AD/NMAP/SNMP, OS Details)
 - Network - Log Aggregation
 - Endpoint - Arctic Wolf Agent
 - Cloud - SaaS - M365
- 30-minute Emergency Service Level Agreement (SLA)
- Unlimited Remote Incident Response
- 0\$ IR Retainer
- \$500K Security Operations Warranty
- **Security Guidance:** Architecture Reviews, CIS Controls Guidance, RCA, SPIDRs
- **Project Management-led Onboarding process**
 - Guided onboarding - service delivery clock begins following 30-day onboarding period
 - White-glove approach – Arctic Wolf preconfigures our tools prior to deployment



Why Now: Business Value Drivers for City of Oceanside

Value Drivers	Description
Faster Intrusion Detection	Leverage your existing technology stack to discover and profile assets and collect data and security event observations from multiple sources so you don't have to rip and replace your existing systems
Team Enhancement	Enhance your existing IT team leveraging named security operations experts. Trusted security operations advisors with years of expertise instantly provide you with a security operations team.
Rapid response	Get a rapid response through managed investigations, remote incident response and log retention and search.
Harden your environment	Receive guided risk remediation and validation on security threats, on-demand reporting to improve security posture throughout regular engagements



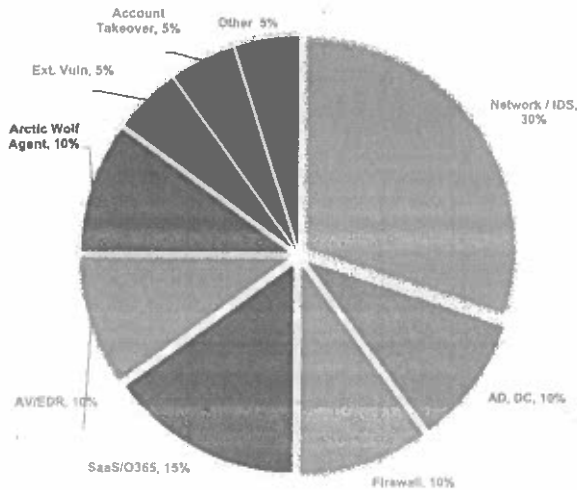
Security Partnership - The Arctic Wolf Security Journey

The Arctic Wolf Security Journey is how we end cyber risk for our customers. We treat security as a journey rather than a destination. Our **Concierge Security Team** takes a long-term approach and guides our customers to adopting the **NIST CSF** or similar frameworks such as **ISO 27001** in a custom way that prioritizes high-impact work based on the customer's unique business context. This approach ensures that customers are rapidly and systematically reducing both the likelihood and impact of cyber security incidents.

By measuring progress on the **Security Journey**, customers have a clear understanding of their security posture, level of security maturity and overall cyber resilience.



Arctic Wolf Networks Attack Surface Visibility



Arctic Wolf Networks allows for full visibility into your environment

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Investigation Source Breakdown

Network/IDS – 30%

- Phishing
- Data Exfiltration
- Exploitation of Vulnerabilities
- IP and domain IOCs
- C2/Beaconing
- Adware
- Coin miners

Active Directory -10%

- Failed Logins
- Privilege Escalation
- DCSync Attack
- Password Spraying

SaaS/Cloud - 15%

- Impossible Travel
- Password Spray
- Business Email Compromise
- Anomalous Logins
- Concurrent Logins

AV/EDR - 10%

- Malware
- Quarantine/Clean

External Vulnerabilities – 5%

- Open Ports
- Vulnerabilities
- OWASP 10

Arctic Wolf Agent – 10%

- Process Anomalies
- Suspicious PowerShell
- Adversary Tools
- Lateral Movement

Account Takeover – 5%

- Credential Stuffing

Other – 5%

- Malicious Site Visited – Email Security
- MFA Deactivation - Auth

Firewall – 10%

- Brute Force



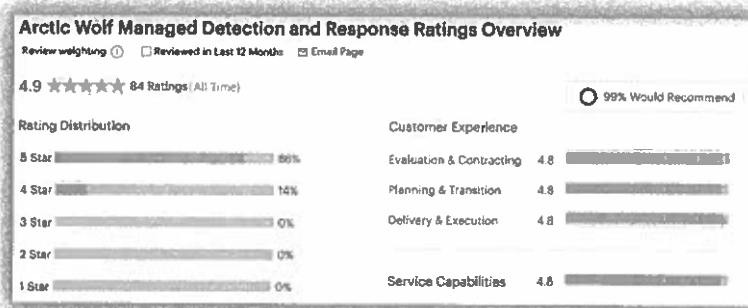
Customer Satisfaction focused on Security Outcomes

Concierge Security is unique to Arctic Wolf and is the primary reason customers rave about our service.

<https://www.gartner.com/reviews/market/managed-detection-and-response-services/vendor/arctic-wolf-networks/product/arctic-wolf-managed-detection-and-response>



"Partnering with Arctic Wolf has truly been a fantastic move for our organization. Getting everything set up and deployed was very simple. They are very responsive, when needed. And they have also been A+ in helping keep our organization secure."



"The experience with Arctic Wolf has been beyond excellent. This is probably one of the best services we could ever have purchased. It is definitely the best decision we have made in the past 5 years. The professionalism and communication is top-notch. We have complete insight into our environment, and access to our Concierge team."

"The level of success I have had with using Arctic Wolf continues to grow through a continual commitment with their concierge service. One of a very few solutions that I would readily recommend, with no hesitation, to individuals considering using them."

"Arctic Wolf is extremely responsive. There is no other company that I have dealt with in my 20 years in IT that have continuously impressed me as much as Arctic Wolf has."



ANALYSTS



LEADER
MDR MarketScape

Gartner.

PEER INSIGHTS



kuppingercoie
ANALYSTS

MARKET COMPASS:
Security Operations Center as a Service
(SOCaaS) "Outstanding in functionality"
5/5 in All Criteria

AWARDS



500™
Technology Fast 500
2021 NORTH AMERICA
Deloitte.



CERTIFICATIONS



Privacy Shield
Compliant



ALLIANCES



Member of
Microsoft Intelligent
Security Association
Microsoft

Financials, Benefits, & ROI

Managed Detection & Response

- Fully managed and hosted SIEM
- 24x7 monitoring (network, endpoint, identity, & cloud)
- 24x7 Eyes on Glass Triage Team
- Named Concierge Security Team to augment your team (2 to 3 resources)
- Regular Security posture reviews
- Monthly External vulnerability scan
- Monthly, quarterly, & ad hoc reporting
- Audit support w/ named CST
- Custom rule creation
- Unlimited log ingestion
- Use of Arctic Wolf Agent & containment action
- 1-year log retention
- Managed IDS
- \$0 IR Retainer

Managed Risk

Quantify Your Cyber Risk Posture

- Comprehensive risk profiling
- Proactive notifications and alerts
- Actionable reporting

External Vulnerability Assessment

- Asset discovery based on root domains and IP addresses
- Automatic IP, domain, sub-domain detection

Internal Vulnerability Assessment

- Dynamic asset discovery and credential scanning
- Asset inventory, categorization, notes, and tags



Pricing Overview: MDR & MR

THE LEADER IN SECURITY OPERATIONS

Contract: 1-Year Agreement Paid Upfront – \$500K Security Operations Warranty & IR JumpStart Ret Eligible

Item	SKU	Quantity	List Price Total	Extended Price
Arctic Wolf Managed Detection & Response	MDR	1	\$246,339.96	\$97,472.06
Arctic Wolf Managed Risk	MR	1	\$110,000.04	\$40,403.85
Total Annual Subscription Fees				\$137,875.91
One-Time Fees – Onboarding				\$9,982.95
Total Fees				\$147,858.86
Savings				\$223,795.69

Pricing Overview: MDR

Contract: 1-Year Agreement Paid Upfront – IR JumpStart Ret Eligible

Item	SKU	Quantity	List Price Total	Extended Price
Arctic Wolf Managed Detection & Response	MDR	1	\$246,339.96	\$97,472.06
Total Annual Subscription Fees				\$97,472.06
One-Time Fees – Onboarding				\$6,789.03
Total Fees				\$104,261.09
Savings				\$152,667.17

*Upon renewal of the Subscription of equal or greater Quantities and Subscription Terms, the subscription fee will increase by 8%



- ▶ 1-hour response time
- ▶ IR Plan Builder to organize must-have information to quicken response SLA
- ▶ Discounted hourly rate in the event of an incident
- ▶ Plan review by Arctic Wolf to identify gaps
- ▶ Complimentary scoping call in the event of an incident

18 **A**

- Identify key contacts
- Organize data and network assets
- Secure online plan storage
- Review plan with IR Director
- Identify gaps in IR plan and processes

IR Plan Builder





SECURITY OPERATIONS WARRANTY

The **Arctic Wolf Security Operations Warranty** is a benefit offered to eligible Arctic Wolf customers that provides up to **\$500,000** of financial assistance should the customer experience a covered security event.

Security Operations Warranty Benefits

- Customers are eligible for up to **\$1,000,000**, when investing in Arctic Wolf's full product portfolio (MDR, Managed Risk, and Managed Awareness) for 3-year commitment (billing annual or upfront)
- A **\$500,000** benefit is available to an eligible customer leveraging MDR and one other core product (Managed Risk or Managed Awareness) – 1-year commitment minimum
- Security Operations Warranty is available for 12 months from subscription start date, and requires acceptance of additional standard terms

Total Benefit Amount	\$1,000,000	\$500,000
Ransomware and BEC	\$200,000	\$100,000
Compliance	\$200,000	\$100,000
Cyber Legal Liability	\$500,000	\$250,000
Business Income Loss	\$100,000	\$50,000

Arctic Wolf Cost Savings Summary

Option 1: Build an Internal SOC (12 resources) = \$1.6M+ PER YEAR

- Expensive option to achieve what Arctic Wolf is providing at a fraction of the price – security talent is in high-demand and supply is short (Security Expertise most expensive component of DIY SOC) – 6+ month time to value to protect environment

Option 2: Subscribe to Arctic Wolf for 3-Years = Less Than \$150K Per Year

- Affordable option, scalable, time to value in 30-days, built out processes, completely managed and hosted SIEM, unlimited log ingestion, proprietary technology, dedicated security expertise, 450+ labor years of R&D into our technology and processes, leader in Security Operations

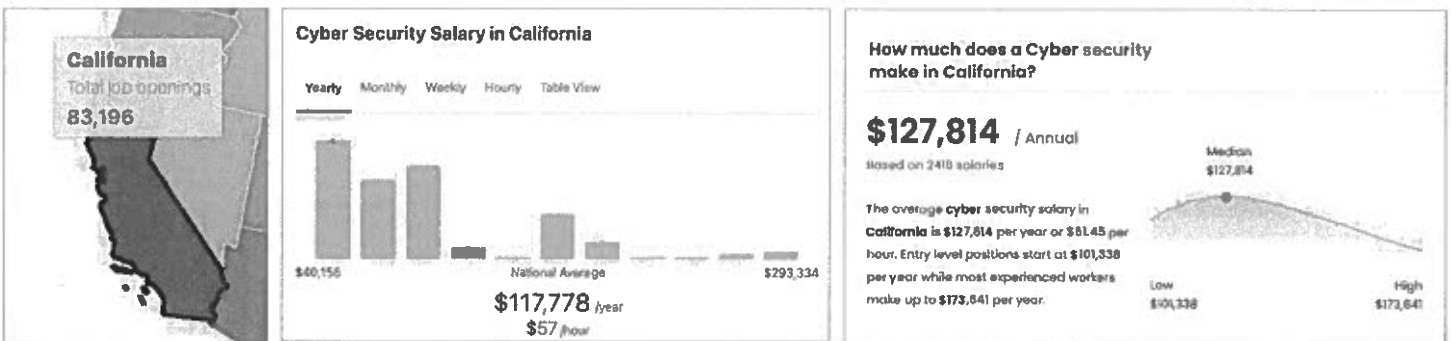
Classification: Public



22

Cybersecurity Talent Gap in Southern California

Retaining talent with experience in building/sustaining a SOC (security operations center) is very expensive



How much does a Cyber Security Engineer make in California? The average Cyber Security Engineer salary in California is \$162,705 as of December 27, 2022, but the range typically falls between \$147,398 and \$180,104. Salary ranges can vary widely depending on the city and many other important factors, including education, certifications, additional skills, the number of years you have spent in your profession.



Sources

- Cybersecurity Engineer Salary in California - ZipRecruiter
- Cybersecurity Engineer Salary in California - Salary.com
- Cybersecurity Average Salary in California in 2023 - Talent.com
- Cybersecurity Supply/Demand Heatmap

Forrester Total Economic Impact of Arctic Wolf's Security Operations Solution

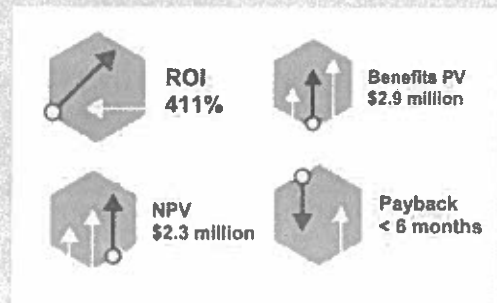
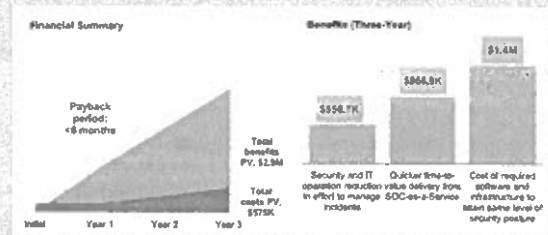
Key Benefits

- Arctic Wolf vs. DIY SOC results in a **411% ROI** and **<6 month payback**
- For resource constrained but growing organizations who require improved capabilities in detection and response, Arctic Wolf saves:
 - 50% of effort from the internal security operations group for triage and investigation activities
 - 90% for IT operations that are involved in incident management
- Reduction of security alerting noise by 60%
- Time-to-value with Arctic Wolf is one-month vs. 10 months for a traditional SIEM or logging tool

[Read the full study](#)

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Confidential

THE LEADER IN SECURITY OPERATIONS



25



2021 Cybersecurity Trends

• High Profile Ransomware Attacks

- **Kaseya VSA** - \$70M ransom demand, 1,000+ companies impacted
- **CNA Financial** - \$40M paid
- **JBS Foods** - \$11M paid
- **Colonial Pipeline** - \$4.4M paid
- **Brenntag** - \$4.4M paid

• Cyber insurance policies are drastically changing...

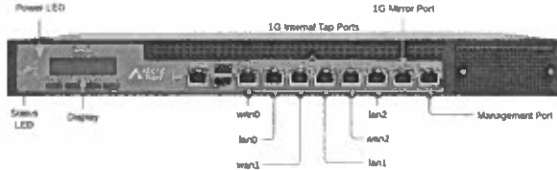
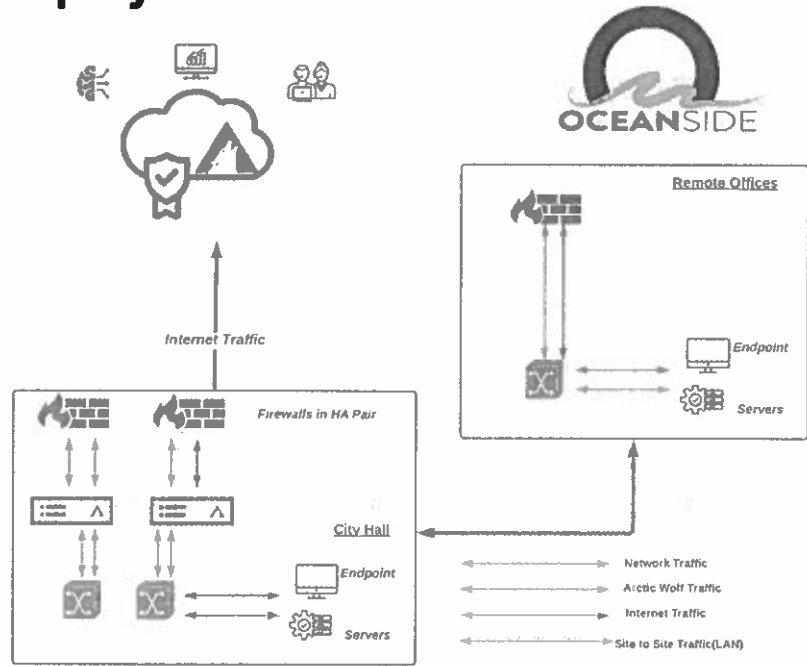
- Evaluation criteria of Customer Risk Profile becoming more strict
- Reduced Coverage (some dropping ransomware coverage)
- Increased Rates
- Ransomware Carveouts

Classification: Confidential

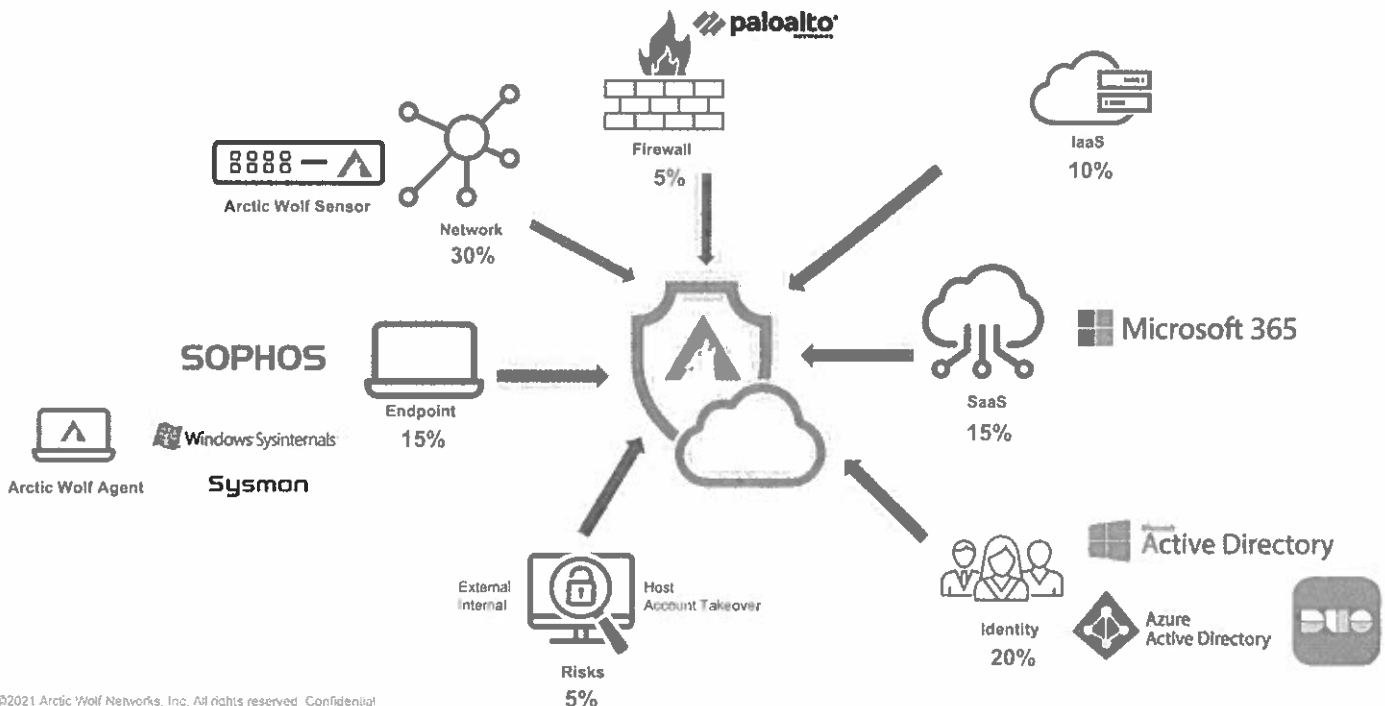


26

- Managed Intrusion Detection System(IDS)
- Monitors NetFlow Data
- Network Security Monitoring
- Log Aggregator(syslog and NXLog)
- Fully Managed by Arctic Wolf
- Containment Support – Network Block(when deployed internal tap)
- Remote installation support provided by Arctic Wolf Onboarding team.
- Sensors delivered pre-configured
- Additional Information:
<https://docs.arcticwolf.com/>



Arctic Wolf observations that lead to ticketed incidents



Log Sources and Sensor Summary

THE LEADER IN SECURITY OPERATIONS

Key Log Sources:

- **Firewall:** Palo Alto
- **Endpoint:** AW Agent
- **Identity:** Active Directory
- **DNS:** MSFT

Scope

Users: **900**
Servers: **200**
Office365: **200**
Monitored Egress Locations: **2**
Log Retention Period: **12 Months**
Number of Sensors: **2 AWN200s**



Sensor Details

Egress Location	Sensor Type	Port Mirror or Inline Network Monitoring	Connector(s) into Arctic Wolf Sensor	Connector between Firewall and Switch	Internet Speed (Max)
City Hall	2 – AWN200	Inline/Internal Tap	2 – Inside	1Gbps Copper	500 Mbps

Important Note: Any changes to these values will require a change in price of the overall solution. Please review for accuracy.

- The Arctic Wolf Agent will be deployed on MS Windows and Apple desktops (on-premise and/or remote), however, we do not support deploying the agent on non-persistent virtual desktops for the RDS environment.

Deployment Summary:

- We will be deploying 3 network/log sensors total. The included AWN200 sensors can support up to 1Gbps of sustained Internet throughput. We will monitor the Internet traffic via a 1Gb RJ-45 ethernet port mirror. The sensor will also have a 1Gb Ethernet management port to be used to ingest on-prem log sources and provide a connection to our cloud service. Installation instructions for all components available at docs.arcticwolf.com

30



Sensor Datasheet

DNS

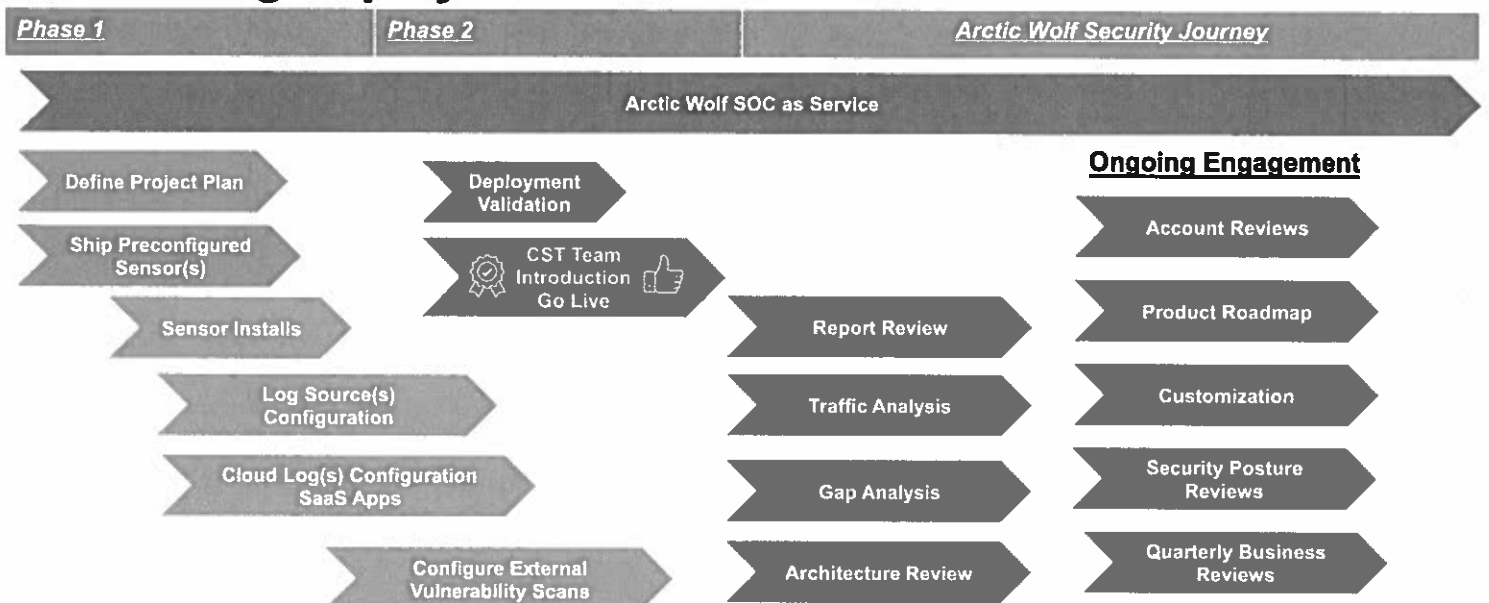
				
SPECIFICATION	100 SERIES	200 SERIES	300 SERIES	1000 SERIES
LOGICAL				
Form Factor	SFF Desktop	1U Rack Mount	1U Rack Mount	1U Rack Mount
Processor	Intel Atom C3308	Intel Core i7-7700	Intel Xeon E-2248G	Intel Xeon Gold 5118
System Memory	8GB	16GB	32GB	48GB
Storage	256 GB SSD	256 GB SSD	480 GB SSD	256 GB SSD
I/O Built In Minimums	3x1GbE RJ45 (With Bypass)	5x1GbE RJ45 (With Bypass) 2x10GbE SFP+ (RJ45, Twinax, Fiber)	5x1GbE RJ45 4x10GbE MM Fiber (With Bypass) 2x10GbE SFP+ (RJ45, Twinax, Fiber)	8x1GbE RJ45 (With Bypass) 4x10GbE SFP+ (RJ45, Twinax, Fiber)
I/O Expansion	N/A	2x10GbE MM Fiber Bypass with LC Connector		2x10GbE MM Fiber Bypass with LC Connector
Management	1x1GbE RJ45	1x1GbE RJ45	1x1GbE RJ45	1x1GbE RJ45
TPM	V2.0 Built In	V2.0 Built In	V2.0 Built In	V2.0 Built In
PHYSICAL				
WxHxD	8.54" x 1.73" x 5.73"	17.25" x 1.7" x 16.3"	17.1" x 1.7" x 21.5"	25.59" x 1.71" x 17.24"
Weight	2.8lbs, 1.2kg	22.0lbs, 10.0kg	28.9lbs, 13.6kg	38.3lbs, 16.5kg
Mounting	Rack Ears Included	Rack Ears Included	Rails Included	Rails Included
Power Supply	36W	220W	2 x 350W	2 x 650W
Power Input	AC 100V - 240V@ 50-60 Hz	AC 98V - 284V@ 47-63 Hz	AC 100V - 240V@ 50-60 Hz	AC 100V - 240V@ 47-63 Hz
Manufacturer	Lanner Technology Co., Ltd.	Lanner Technology Co., Ltd.	Dell, Inc	Lanner Technology Co., LTD
ENVIRONMENTAL				
Ambient Temp	32 to 122 F 0 to 50 C 5% to 95% Humidity	32 to 104 F 0 to 40 C 5% to 90% Humidity	50 to 95 F 10 to 35 C 10% to 80% Humidity	32 to 104 F 0 to 40 C 5% to 90% Humidity
Storage Temp	(-4) to 158 F (-20) to 70 C	(-4) to 158 F (-20) to 70 C	(-40) to 149 F (-40) to 65 C	(-4) to 158 F (-20) to 70 C



June Implementation & PO Timeline

Onboarding Deployment

THE LEADER IN SECURITY OPERATIONS



Rapid Onboarding: 2 Week Deployment Phase

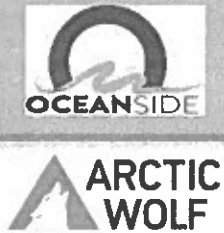
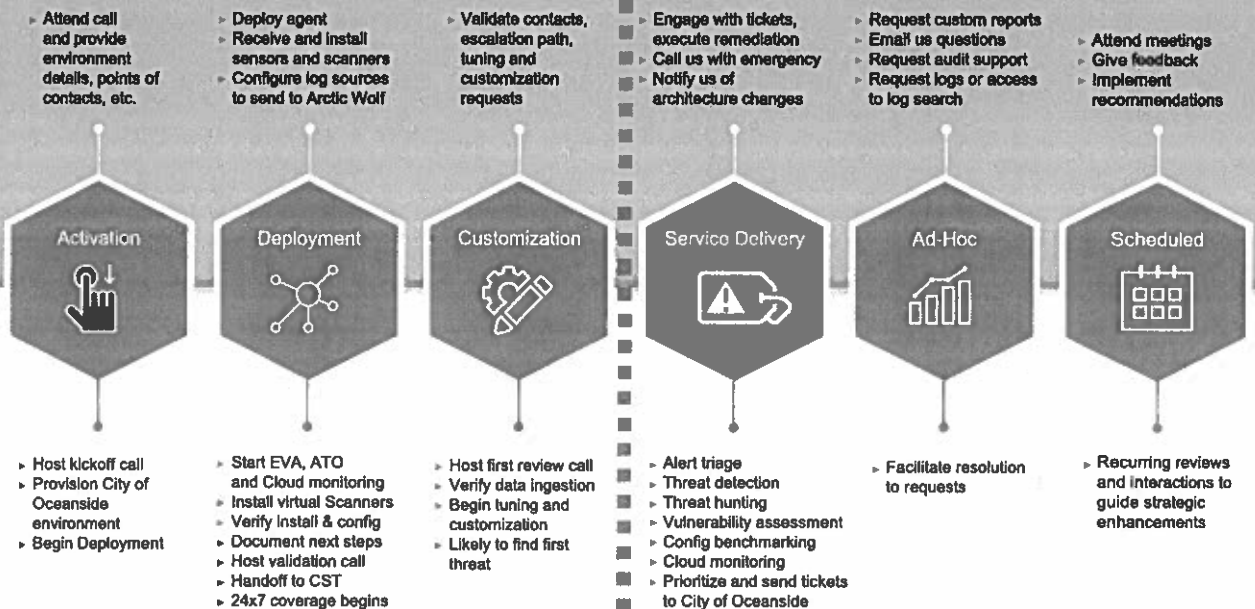
- AW Provides Dedicated Onboarding Team: Project Manager and Onboarding Engineer

Deployment & Engagement Model

THE LEADER IN SECURITY OPERATIONS

Deployment: 2 - 4 weeks

Ongoing Engagement



©2023 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

34

June 30th, 2023 - Project Timeline & Layout

Date Details:

- Quote Signature / PO Date: 06/30/2023
- Order Processing Date: 06/30/2023
- Subscription Start Date: 07/31/2023

Friday, June 30th

City of Oceanside issues PO or signs quote for Arctic Wolf to CDW by Friday, June 30th

Friday, June 30th

Arctic Wolf processes PO & invoices for service

July 31st, 2023

3-year subscription start date

June 2023

July 2023

Onboarding (8-12 hours) will take place over this 30-day period. City of Oceanside IT/IS team will be assigned an Arctic Wolf Project Manager and Professional Services Engineer (Concierge Onboarding Team) who will assist with onboarding from beginning to end, remotely

©2021 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Confidential

35

Solution Overview

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Confidential

36



Arctic Wolf Overview

Arctic Wolf is the market leader in security operations. Using the cloud-native Arctic Wolf Platform, we provide security operations as a concierge service. Highly trained Concierge Security experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture.

The cybersecurity industry has an **effectiveness** problem.

3,000 Vendors

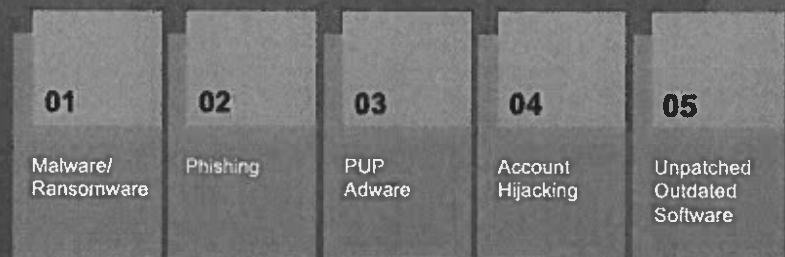
\$120B Total Spend

3,950 Reported Breaches

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public



Arctic Wolf Helps Detect and Respond to the Top 5 Attack Vectors:



END CYBER RISK

37



Arctic Wolf Service Offerings



PROPOSED SOLUTION Managed Detection & Response



Addon:
Cloud Detection and Response
(M365)

The purpose of this solution is to help you defend against advanced threats that bypass prevention tools. We fundamentally believe that you can't have protection if you don't have detection first.

Detect

Leverage your existing tech stack to identify advanced network, endpoint, and cloud threats

Respond

24/7 coverage and guided response stops threats before they can do harm

Recover

Find root cause, validate remediation, and collaborate to continuously improve your overall security posture

70% of new customer environments have latent threats



PROPOSED SOLUTION Managed Risk

Managed Risk is designed to help you prevent incidents in the first place. We know this capability is badly needed because the Center for Internet Security says that 80% of breaches could have been prevented if the organization had met the top 5 CIS controls.

Discover

Identify and categorize risky IaaS Services, SaaS apps, assets, and accounts

Benchmark

Understand your current digital risk posture and identify gaps relative to best practices

Harden

Know when you're exposed and prioritize security posture improvements

80% of threats can be prevented by meeting the top 5 CIS controls



NOT-PROPOSED Managed Security Awareness

End the cyber risk of social engineering attacks and human error by preparing every employee to be an active participant in your security posture and strengthen your cyber resilience.

Engage

Educate and prepare employees to stop social engineering attacks, like phishing.

Measure

Identify employees that fall behind and determine which threat topics require reinforcement.

Transform

Achieve a culture of security and strengthen cyber resilience.

85% of data breaches result from employee actions

©2021 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Confidential



AWN Concierge Security Team (CST)

Arctic Wolf® Concierge Security® Team (CST) includes **2-3 Named Security Engineers** (experts) who work alongside the Arctic Wolf Triage Team to monitor security events 24x7 enriched and analyzed by the Arctic Wolf® Open-XDR Platform, to provide your team with coverage, security operations expertise, and strategically tailored security recommendations to continuously improve your overall posture at City of Oceanside.

EXPERTISE

Deliver execution and operational excellence with skills required to detect advanced threats and manage risks in a way that's customized to your environment.

► Security Operations Experts

- Hundreds of years of combined experience with cybersecurity accreditations like CISSP, HCISPP, CCSP, CISM, CRISC, 15+ industry certifications

► Proactive Threat Hunting

- Daily hunting for suspicious activity across your environment

► Informed Incident Insights

- Filter out the noise to reveal what happened, and what to do about it



COVERAGE

Work around the clock to triage critical events and deliver actionable insights when you need them the most.

► 24x7 Continuous Monitoring

- Your environment is monitored around the clock for threats and risks

► Rapid Response

- Detect and investigate critical events within five minutes

► Real-Time Remediation

- Rapidly contain incidents and get detailed guidance on remediation

STRATEGY

Strategic security guidance drives continuous improvement that's tailored to the specific needs of your organization.

► Security Posture Reviews

- Evaluate the root cause of threats and get prioritized recommendations to improve posture

► Named Advisors

- Trusted security operations experts paired with you to deliver tailored triage and strategic guidance

► Security Journey Guidance

- Quarterly reviews to help you design, implement, and achieve your security vision

Concierge Security Engagement & Service Facilitation

The Arctic Wolf Concierge Security Team (Security Engineer & Security Analyst) will work with you to build and execute a Security Journey that meets your organization's goals and objectives while identifying opportunities to strengthen your security posture over time.

The Arctic Wolf Triage Team (500+ Security Engineers & Security Analysts) works 24/7x365 to investigate alerts generated by the Arctic Wolf Platform. This team provides tactical support and guidance to customers and the Concierge Security Team during security events.



- ✓ SOC 2 Type 2
- ✓ CISSP
- ✓ CCSP
- ✓ HCISPP
- ✓ ISO 27001:2013
- ✓ GIAC
- ✓ GFCE
- ✓ GCIH
- ✓ GICSP
- ✓ GXPIN
- ✓ CEH
- ✓ CPT
- ✓ CIH
- ✓ OSCP

98%

Customer
Retention Rate YoY

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Confidential

40

Service Engagement Overview THE LEADER IN SECURITY OPERATIONS

Arctic Wolf Concierge Security Team & Triage Team are responsible for:

24x7 Monitoring

Triage/Investigating Alerts

Threat Hunting

Actionable Remediation Plan

Strategic Insights/Advice

Emergency incidents will be escalated to City of Oceanside in under 30 minutes from discovery with an internal service expectation of under 5 minutes



AWN Concierge Security Team



Critical Incident = Direct call from CST to City of Oceanside IT/IS Team

Office365

Email sent to City of Oceanside IT/IS Team



All Incidents ticketed in portal

City of Oceanside is only responsible for IT Functions:

IT Remediation e.g.,

Device re-image (malware)

Password reset (phishing)

FW Rule Change

Patching

Have an emergency? Call our SOC and state you have an emergency and be routed to your CST in under 5 minutes 24x7x365



©2022 Arctic Wolf Networks, Inc. All rights reserved. Classification: Confidential



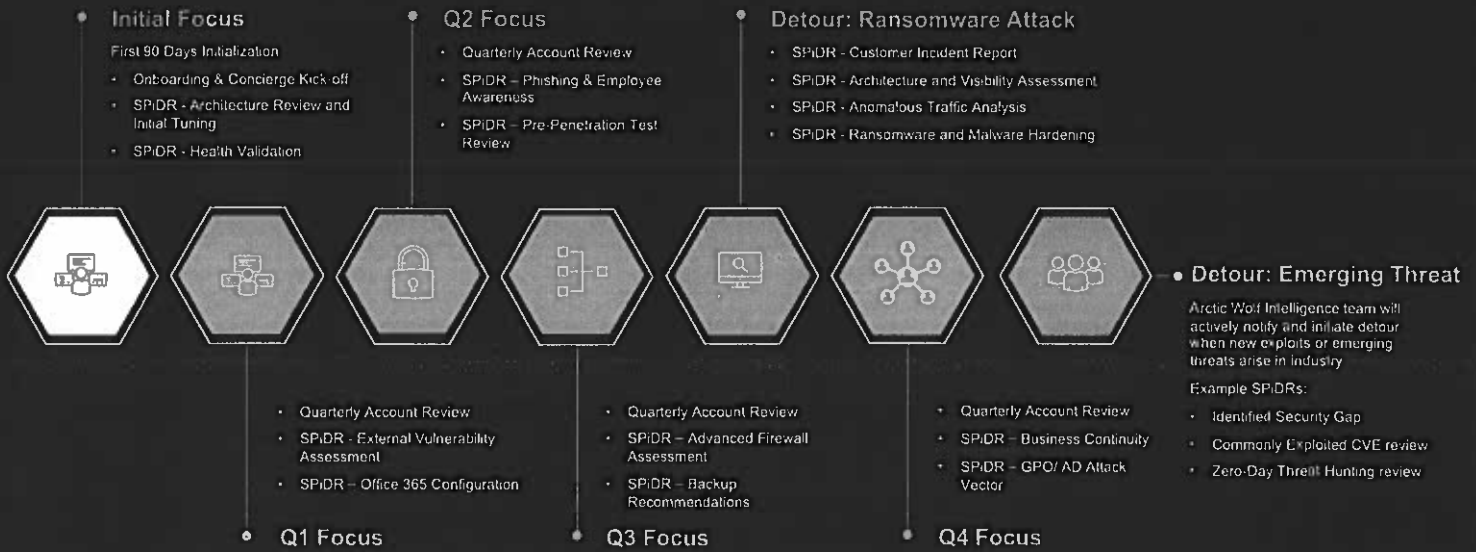
Security Journey Timeline

First Year Example

Start-up Focus

Steady-State Focus

Detour/ Ad-hoc Focus



©2022 Arctic Wolf Networks, Inc. All rights reserved. Classification: Restricted



Different Approaches to 'Security Operations'

	Security Operations framework coverage	Tech Stack & Compatibility	Visibility across attack surfaces	Pricing	Service Delivery Engagement	Service Operations Warranty
SIEM						
MSSP						
EDR						
MDR						
XDR						
AW						
	Coverage across Sec Ops framework	Use existing tech and or AW tech	Endpoint, network, Cloud, Apps, Identity and People	Unlimited & unmetered data pricing	Invented Concierge Security Team	First with \$1M Service Operations Warranty

©2023 Arctic Wolf Networks, Inc. All rights reserved. Confidential

Arctic Wolf Delivers Security Outcomes

DWELL TIME

0:30

Industry average time to identify an intrusion is 206 days. Arctic Wolf does it in 30 minutes or less.

TIME OF ATTACKS

39%

Threats that were detected after 8PM and before 8AM by Arctic Wolf

ADVANCED THREATS

43%

Of customers have advanced threat activity being missed by security tools but caught by Arctic Wolf

ACCOUNT TAKEOVER

69%

Of customers have some PII exposure, with 19% with critical exposure (plain text passwords)

UNPATCHED VULNERABILITIES

58%

Reduction in time to patch critical vulnerabilities after activating Arctic Wolf

PHISHING

18%

Of customers have phishing activity that is missed by email security but caught by Arctic Wolf



Aaren Larsen – Arctic Wolf Account Executive
Email: aaren.larsen@arcticwolf.com
Phone: (952) 797-3905



David Ta – Arctic Wolf Systems Engineer
Email: david.ta@arcticwolf.com
Phone: (612) 644-1028



Jay Moore – CDW-G Account Representative
Email: Jay.Moore@cdwg.com
Phone: (312) 547-2777



Rich Adams – CDW-G Account Executive
Email: Richada@cdw.com
Phone: (805) 559-0563



Appendix

Growth & Funding

THE LEADER IN SECURITY OPERATIONS



- \$900 Million in funding
- Most recent was \$401M October 6th, 2022
- 100% YoY growth the past 8 consecutive years
- Organic & inorganic growth (Acquisitions)
 - Ex. vxIntel, Tetra Defense, etc.

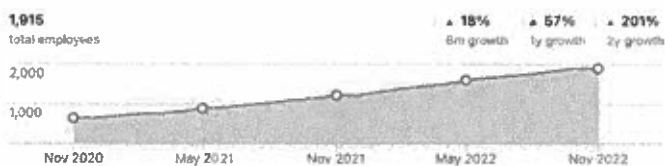
Arctic Wolf

At Arctic Wolf, our mission is to End Cyber Risk through effective security operations.
Computer and Network Security · Eden Prairie, Minnesota · 45,471 followers

PREMIUM

Total employee count

Based on LinkedIn data.



Median employee tenure - 1.2 years

PREMIUM

Employee distribution and headcount growth by function

Based on LinkedIn data.

Functions

Functional distribution



Headcount growth

	6m	1y
Information Technology	▲ 19%	▲ 55%
Sales	▲ 41%	▲ 90%
Engineering	▲ 32%	▲ 60%
Support	▲ 24%	▲ 89%



THE LEADER IN SECURITY OPERATIONS

Arctic Wolf Solutions Agreement – Frequently Asked Questions

Thank you for reviewing the Arctic Wolf Solutions Agreement. We appreciate your interest in becoming a customer of Arctic Wolf. We hope the below information will help you better understand how Arctic Wolf's security solutions (the "Solution" or "Solutions") contracting model works.

Please note that this information is not considered part of the contract at any time. This is provided for information purposes only.

Who is Arctic Wolf?

- Arctic Wolf is a cybersecurity company that provides security operations Solutions, including managed detection and response, managed risk, and managed security awareness to mitigate our customers' exposure to cyber threats.
- We offer standard, highly configurable, Solutions to our customers which allows us to leverage the power of scale across our customer base to deliver cost effective and operationally efficient Solutions.
- Arctic Wolf's customers may subscribe to and license for the purchased Subscription Term the right to receive and use, in whole or in part, the various Solutions offered by Arctic Wolf. All customers subscribing to a particular Solution are on the same release using the same operational infrastructure and the same security and support operations for such Solution.

Who is the Authorized Partner?

Arctic Wolf leverages its channel partner relationships (its "Authorized Partners") to resell our Solutions to our customers. The Authorized Partner may be selected by you or introduced to you by Arctic Wolf.

The Authorized Partners act as the financial arm in our transactions with you. You contract directly with the Authorized Partner related to purchase and payment of your subscription to our Solutions. The Authorized Partners are not involved in the delivery of our Solutions and, therefore, are not contemplated in the obligations and liabilities within the Solutions Agreement related to the delivery of our Solutions to you. You and the Authorized Partner will have separate contractual terms in place to address the financial aspects of the subscription transaction.

What data do you provide to Arctic Wolf?

Arctic Wolf monitors systems telemetry data received from our customers via the sensors, scanners and agents our customers install within their environment. The systems telemetry data allows us to identify potential security threats that may impact your environment. Systems telemetry data may include names, email addresses, phone numbers, usernames, passwords IP Address, geolocation data, deviceID, and other system log metadata. Arctic Wolf should not receive other more sensitive information, including the content of your business files, your customer's business information, social security numbers, financial information, etc. We trust that our customers have appropriate system and operational controls in place to prevent disclosure of such information to us.

Why does Arctic Wolf reserve the right to change certain terms within the Solutions Agreement?

Like other subscription-based solutions providers, customer-generic terms that apply across our customer base are set forth as url links within the overarching Solutions Agreement. This allows Arctic Wolf to maintain consistency in the Solutions across its customers. To address any customer concerns related to this model, Arctic Wolf: (i) provides that the url terms are last in line from an order of precedence; (ii) agrees that we will not materially decrease the features and functionalities during any customer then-current Subscription Term; (iii) provides notice of the change; and (iv) allows customers to object to any specific modification for the remaining period of their then-current Subscription Term.

Does Arctic Wolf offer service levels?

Arctic Wolf provides for response time service levels. These service levels can be found in the Managed Detection and Response Solutions Terms located at <https://arcticwolf.com/terms/>. These terms are password protected. Please contact your sales representative for the password.

Does Arctic Wolf offer termination for convenience?

As a subscription Solution, Arctic Wolf does not allow for termination for convenience. Arctic Wolf relies on committed subscription terms, in part, to manage our dedicated CST resource model.

We have special data security requirements. Can we include our security and privacy requirements in the Solutions Agreement?

We are unable to include customer specific data security requirements in our Solutions Agreement. We offer a consistent Solution across our customer base. Arctic Wolf maintains the same IT security controls and processes for all customers. These controls and processes are reflected in our SOC2 Type II Report and its ISO 27001 certification.

Where is the Statement of Work for the services described in the Solutions Agreement?

Arctic Wolf's provides a subscription Solution that, depending on the Solution, is comprised of hardware, software and services. All designated components of the Solution are required to use and receive the Solutions. While services are an important part of the Solution, we do not define the services component of the Solutions as separate "professional services". Unlike a traditional professional service offering, the services do not include deliverables and are not subject to acceptance.

Can we make changes to the Beta Terms?

Because participation in the beta programs is completely voluntary and there is no cost for participation, we do not agree to modifications to the beta terms.

We are a Covered Entity under HIPAA. Can we use our Business Associate Agreement?

Arctic Wolf should not receive PHI during the delivery of the Solutions to you, nor does Arctic Wolf process PHI on your behalf. Accordingly, Arctic Wolf is not a business associate under HIPAA. Arctic Wolf appreciates that certain customers may take a conservative approach and require a business associate agreement (BAA) to cover the exchange of any inadvertently disclosed PHI provided during our relationship. Given this, Arctic Wolf is amenable to execution of its template BAA in which each party's liabilities and requirements are strictly construed to HIPAA requirements and incorporates such terms by url reference in the Solutions Agreement.

(For information purposes only, this FAQ does not form part of any contract)

SOLUTIONS AGREEMENT
(via Authorized Partner)

This Solutions Agreement (the "**Agreement**") is a legal agreement entered into by and between the Customer identified in the signature block below ("**Customer**") and Arctic Wolf Networks, Inc. ("**Arctic Wolf**") and governs any order forms, quotes, or other ordering document executed by the Customer ("**Order Form**") that reference this Agreement. An Order Form will be issued to Customer by an Arctic Wolf authorized partner ("**Authorized Partner**"). This Agreement is effective on the date last executed in the signature block below (the "**Effective Date**"). This Agreement permits Customer to purchase subscriptions to the Solutions, as defined below, identified in the Order Form from its Authorized Partner and sets forth the terms and conditions under which those Solutions will be delivered. The Agreement consists of the terms and conditions set forth below, any attachments or exhibits identified herein and any Order Forms that reference this Agreement. If there is a conflict between the terms below, the Order Form, or the terms set forth in a URL referenced herein (such URL terms, the "**Terms**"), the documents will control in the following order: the Order Form, this Agreement, and the Terms.

In consideration of the mutual covenants and agreements contained herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Scope.

1.1 Solutions. Customer will purchase and Arctic Wolf, together with its Affiliates, will provide the specific products and services (each a "**Solution**" or collectively, "**Solutions**") as specified in the applicable Order Form. For purposes of this Agreement, "**Affiliate**" means any company or other entity, which directly or indirectly controls, is controlled by or is under joint control with Arctic Wolf.

A Solution will be comprised of the following components:

	Managed Detection & Response Solution	Managed Risk Solution	Managed Security Awareness / Managed Security Awareness+ Solution
Software	The object form of any software, including any operating system software included in the Equipment, and add-ons offering enhanced features and functionality made generally available to Arctic Wolf customers from time-to-time	The object form of any software, including any related to virtual Equipment, if applicable, any operating system software included in the Equipment, and add-ons offering enhanced features and functionality made generally available to Arctic Wolf customers from time-to-time	N/A
Equipment	Virtual appliances or physical sensors	Virtual appliances or physical scanners	N/A
Content	N/A	N/A	Online access and download rights, if licensed by Customer, to Customer learning content and Content Compliance Pack within the Administrator Dashboard and/or Content Library
Content Management Hosting Environment	N/A	N/A	Access to and use of a cloud-based learning management tool (the "Administrator Dashboard") and metrics related to the use of the Content by Customer's users
Services	Support, onboarding services, and services provided by Security Services, all as described in the Solutions Terms (defined below)	Support, onboarding services, and services provided by Security Services, all as described in the Solutions Terms (defined below)	Support, onboarding services, and Content modification services, all as described in the Solutions Terms (defined below)
Professional Services	As agreed by the parties in accordance with Section 3	As agreed by the parties in accordance with Section 3	As agreed by the parties in accordance with Section 3
Platform	One (1) vSensor 100 series Unlimited data ingestion Access to the Customer Portal Use of the Arctic Wolf Agent 90-day Log Retention (unless another retention period is purchased by Customer and set forth on an Order Form)	Unlimited data ingestion Access to the Customer Portal Use of the Arctic Wolf Agent	N/A

1.2 License Grant. The Solutions are provided on a subscription basis for a set term designated on the Order Form (each, a "**Subscription Term**") for the one-time costs and subscription fees set forth therein (the "**Fees**"). Provided Customer is in compliance with the terms of this Agreement, including payment of Fees, Arctic Wolf grants to Customer a limited, non-transferable, non-sublicensable, non-exclusive right and/or license during the Subscription Term, to the extent a component of the Solutions being licensed by Customer as set forth in Section 1.1 above, to:

- (i) Install, use and access the Software,
- (ii) Use the Equipment for purposes of the use of the Solutions,
- (iii) Obtain and use the Services in conjunction with Customer's use of the Solutions,
- (iv) Load Customer's users and associated information for delivery of Content and use of the Administrator Dashboard,
- (v) Access the Customer Portal and/or Administrator Dashboard, as applicable, subject to the Privacy Notice located at <https://arcticwolf.com/privacy-policy-for-customer-portal-users/>, as may be updated from time-to-time in accordance with Section 13 below (the "**Privacy Notice**"),
- (vi) Access and use the Platform features and functionality,
- (vii) Use Arctic Wolf Trademarks included in the Content in accordance with the Solutions Terms, and
- (viii) Distribute, display, transmit, and, if licensed by Customer, download certain Content in electronic format.

Customer may access and use the Solutions, and any Documentation associated therewith, solely for its own internal business purposes and in accordance with the terms and conditions of this Agreement, such associated Documentation, any scope of use restrictions and license counts, including by server, user, or such other licensing metric designated in the applicable Order Form, and the Solutions Terms found at <https://arcticwolf.com/terms/solutionsterms/>, as may be updated from time to time by Arctic Wolf in accordance with Section 13 herein (the "**Solutions Terms**"). "**Documentation**" means user manuals, training materials, product descriptions and specifications, and other printed information relating to the Solution, as in effect and generally available from Arctic Wolf, but expressly excluding marketing and sales collateral and materials.

1.3 Future Functionality. Subject to the warranties set forth in Section 10, Customer agrees that it has not relied on the promise of availability of any future functionality of the Solutions or any other future product or service in executing this Agreement or any Order Form. Customer acknowledges that information provided by Arctic Wolf regarding future functionality should not be relied upon to make a purchase decision. Should Arctic Wolf offer additional optional functionality in the future that complement the Solutions, Customer may elect to subscribe to and obtain a license to the optional functionality for an additional fee.

1.4 Except as otherwise provided herein, Customer understands and agrees that the Authorized Partner may not modify this Agreement or make any commitments related to the delivery or performance of the Solutions on Arctic Wolf's behalf.

1.5 Beta Solutions.

1.5.1 From time-to-time Arctic Wolf may invite Customer to try, at no charge, Arctic Wolf products, features, or functionality that are not generally available to Arctic Wolf's customers ("Beta Solutions"). Customer may accept or decline any such trial in its sole discretion. Any Beta Solutions will be clearly designated as beta, pilot, limited release, developer preview, non-production or by a description of similar import.

1.5.2 Restrictions and Disclaimers. Beta Solutions are provided for evaluation purposes and not for production use, are not supported, may contain bugs or errors, and may be subject to additional terms. To the full extent permitted by applicable U.S. and foreign consumer protection laws, Beta Solutions are not considered Solutions hereunder and are provided solely and exclusively "AS IS" with no express or implied warranty of any kind. TO THE FULL EXTENT PERMITTED BY APPLICABLE U.S. AND FOREIGN CONSUMER PROTECTION LAWS, (THE "CONSUMER PROTECTION LAWS"), CUSTOMER ASSUMES AND UNCONDITIONALLY RELEASES ARCTIC WOLF FROM ALL RISKS ASSOCIATED WITH THE USE OF ANY BETA SOLUTIONS. Arctic Wolf may discontinue the Beta Solutions at any time in its sole discretion and Arctic Wolf will make reasonable efforts to provide Customer with advanced notice of any such discontinuance. Arctic Wolf does not promise or represent that Beta Solutions will be made generally available.

1.5.3 NO DATA RETENTION. ANY DATA ENTERED INTO THE BETA SOLUTIONS MAY BE PERMANENTLY LOST UNLESS CUSTOMER: (i) PURCHASES A SUBSCRIPTION TO THE COMMERCIALY AVAILABLE VERSION OF THE BETA SOLUTIONS AS MAY BE MADE AVAILABLE BY ARCTIC WOLF; OR (ii) TO THE EXTENT POSSIBLE, EXPORTS SUCH DATA PRIOR TO TERMINATION OF THE BETA SOLUTIONS.

1.5.4 LIMITED LIABILITY. TO THE FULL EXTENT PERMITTED BY LAW, INCLUDING THE CONSUMER PROTECTION LAWS, ARCTIC WOLF'S ENTIRE LIABILITY IN CONNECTION WITH ANY USE OF THE BETA SOLUTIONS WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WILL NOT, AS TO ANY INDIVIDUAL CLAIM OR IN THE AGGREGATE, EXCEED \$50. IF CUSTOMER DOES NOT AGREE TO THE ALLOCATION OF RISK IN THIS SECTION, ITS SOLE RECOURSE IS TO IMMEDIATELY DISCONTINUE THE USE OF THE BETA SOLUTIONS.

1.5.5. Despite anything to the contrary in this Agreement, Customer acknowledges that (a) Beta Solutions may not be supported and may be changed at any time, including in a manner that reduces functionality, (b) Beta Solutions may not be available or reliable, and (c) Beta Solutions may not be subject to the same security or audits as the Solutions.

1.6 IR JumpStart. In the event Customer's Order Form includes the license of IR JumpStart, Customer agrees that the IR JumpStart Agreement located at <https://arcticwolf.com/terms/> shall apply. If Customer is a managed service provider Authorized Partner ("MSP"), MSP, as Customer, understands that the IR JumpStart Agreement is an agreement between Arctic Wolf and MSP's end user and MSP is reselling IRJS to its end user.

2. Equipment. If the Order Form specifies that Customer will receive Equipment, then Customer is responsible for installing the Equipment at the location(s) specified by Arctic Wolf and for the implementation of appropriate data protection practices related to the protection of any information included on such Equipment while the Equipment is located within Customer's environment. The Equipment is a part of the Solutions and included with the subscription to the Solutions for use by Customer during the Subscription Term. If Customer attempts to install or use the Equipment at a location other than the location determined by Customer and communicated to Arctic Wolf during onboarding or at any time

thereafter, the Solutions may fail to function or may function improperly. In the event Customer installs, uses, or relocates the Equipment, Customer will promptly notify Arctic Wolf so that Equipment deployment information can be updated within Customer's account. Other than normal wear and tear, Customer is directly responsible for the replacement cost of the Equipment associated with any loss, repair, or replacement, including any other costs, damages, fees and charges to repair the Equipment. If applicable, Arctic Wolf will ship Equipment to Customer and will pay the freight costs associated with shipping the Equipment to Customer's designated locations. Customer is responsible for all additional costs and expenses associated with shipping the Equipment to its designated locations and for the return of the Equipment to Arctic Wolf. Such additional costs and expenses may be reflected on an Order Form, from time-to-time following shipment of the Equipment and will be invoiced by Arctic Wolf or the Authorized Partner. Customer understands and agrees if the Equipment is shipped outside of the United States or Canada (or such other locations identified by Arctic Wolf), Customer is responsible for acting as the importer of record.

3. Professional Services. In the event Arctic Wolf and Customer agree on the delivery of Professional Services, any such Professional Services shall be specified on an Order Form and described in a statement of work which shall reference this Agreement.

4. Reservation of Rights and Ownership. Arctic Wolf owns or has the right to license the Solutions and any associated Documentation ("**Arctic Wolf Technology**"). Customer acknowledges and agrees that: (a) the Arctic Wolf Technology is protected by United States and international copyright, trademark, patent, trade secret and other intellectual property or proprietary rights laws; (b) Arctic Wolf retains all right, title and interest (including, without limitation, all patent, copyright, trade secret and other intellectual property rights) in and to the Arctic Wolf Technology, excluding any rights, title, and interest in any Third Party Products (as defined in Section 10.3 below) which shall be retained by its third party licensor(s), any other deliverables, know-how, databases, developed programs, and registered or unregistered intangible property rights; (c) there are no implied licenses and any rights not expressly granted to Customer hereunder are reserved by Arctic Wolf; (d) the Solution, excluding Professional Services, is licensed on a subscription basis, not sold, and Customer acquires no ownership or other interest (other than the license rights expressly stated herein) in or to the Arctic Wolf Technology; and (e) the Solution is offered as an on-line, hosted solution, and Customer has no right to obtain a copy of the Software.

5. Restrictions, Responsibilities, and Prohibited Use.

5.1 Restrictions. Customer agrees not to, directly or indirectly: (i) modify, translate, copy or create derivative works of the Arctic Wolf Technology except as otherwise expressly permitted under applicable U.S. and foreign copyright laws ("Copyright Laws") which may not be excluded by agreement between the parties; (ii) reverse engineer, decompile, disassemble, or otherwise seek to obtain the intellectual property contained within Solutions, except as otherwise expressly permitted under the Copyright Laws which may not be excluded by agreement between the parties; (iii) interfere with or disrupt the integrity or performance of the Solutions or the data and information contained therein or block or disrupt any use or enjoyment of the Solutions by any third party; (iv) attempt to gain unauthorized access to the Arctic Wolf Technology or related systems or networks; (v) remove or obscure any proprietary or other notice contained in the Arctic Wolf Technology, including on any reports or data printed from the Arctic Wolf Technology; (vi) unless Customer is an authorized MSP partner of Arctic Wolf, use the Solutions in connection with a service bureau, service provider or like activity whereby Customer operates or uses the Solutions for the benefit of a third party; (vii) use the Solutions to monitor or scan any environments for which Customer has not received consent; or (viii) with respect to Customer's subscription to the Managed Security Awareness Solution, include material or information that is obscene, defamatory, libelous, slanderous, that violates any person's right of publicity, privacy or personality, or otherwise results in any tort, injury, damage or harm to any person. Customer agrees to abide by the terms of the Acceptable Use Policy at <https://arcticwolf.com/terms/acceptable-user-policy/>, as may be updated from time-to-time in accordance with Section 13 below. If Arctic Wolf, in its reasonable discretion, determines that Customer's use of or access to the Solutions imposes an actual or imminent threat to the security or stability of Arctic Wolf's infrastructure or that Customer is abusing its use of the Solutions in contravention with the terms of this Agreement, Arctic Wolf may, in addition to any other right herein, temporarily suspend Customer's access to the Solutions, without liability except as otherwise provided by Consumer Protection Laws, until such activity is rectified. If commercially practicable, Arctic Wolf shall provide Customer with notice prior to any such suspension and shall work with Customer in good faith to reinstate the Solutions promptly.

5.2 Arctic Wolf Responsibilities. Arctic Wolf shall provide the Solutions Customer subscribes to as set forth on an Order Form in accordance with the terms of this Agreement, as further described in the Solutions Terms. The Solutions provided under this Agreement shall include any updates, upgrades, bug fixes, version upgrades or any similar changes that are made generally available to Arctic Wolf's customers free of charge from time to time during the Subscription Term.

5.3. Customer Responsibilities. Customer must identify the administrative users for its account which may include Customer's authorized (email authorization sufficient) third party service providers and agents ("**Administrators**"). Each Administrator will receive an administrator ID and password and will need to register with Arctic Wolf. Customer is responsible for notifying Arctic Wolf about changes to Administrators, including but not limited to termination, change of authority, and the addition of Administrators. Customer acknowledges and agrees that Administrators will be able to view all Solutions Data and other traffic and activities that occur on Customer's network and that Customer is responsible for all activities that occur under Administrator accounts. Administrator IDs are granted to individual, named persons and cannot be shared or used by more than one Administrator but may be reassigned from time-to-time to new Administrators. Notwithstanding anything contrary herein, Customer understands and agrees that transmission of Solutions Data to Arctic Wolf may be impacted by in-country technical issues and requirements. Arctic Wolf will provide reasonable assistance to Customer in such instances but is not liable if the Solutions Data cannot be transmitted outside of such country. Customer is responsible for implementing appropriate internal procedures and oversight to the extent it utilizes the configuration of workflows and processes, including but not limited to containment actions, and similar functionalities in conjunction with the Services. Arctic Wolf may recommend Customer, depending on the scope of the deployment, implement software and services to enable features of the Solutions or to permit increased visibility into Customer's environment. Customer is responsible for making such determinations in its discretion and Arctic Wolf has no liability for Customer's decisions related thereto. Customer acknowledges that any changes Customer makes to its code, infrastructure or configuration of the Solutions after initial deployment may cause the Solutions to cease working or function improperly or could prevent Arctic Wolf from delivering the Solutions and Arctic Wolf will have no responsibility for the impact of any such Customer changes. Customer understands that depending on the Solution deployed, a Solution may consume additional CPU and memory in Customer's environment while running in production.

5.4 Anti-corruption. In no event shall Arctic Wolf be obligated to take any action (including the shipping of any product or the provision of any service) or omit to take any action that Arctic Wolf believes in good faith would cause it to be in violation of any U.S. or foreign laws or

regulations, including, without limitation, the U.S. Foreign Corrupt Practices Act (the "**FCPA**"). Neither party will (i) attempt to, directly or indirectly, improperly influence the sale or purchase of products by payments or other actions contrary to law or regulation, or (ii) take any action or permit or authorize any action that would violate or cause a party to violate the FCPA, the UK Bribery Act, or other applicable anti-corruption laws or regulations. Neither party will, for the purpose of influencing any act or decision to obtain or retain business or direct business to any person, pay, offer or promise to pay, or authorize the payment of, directly or indirectly, any money or anything of value to or for the use or benefit of any of the following: (a) any government official (including any person holding an executive, legislative, judicial or administrative office, whether elected or appointed, or any representative of any public international organization, or any person acting in any official capacity for or on behalf of any government, state-owned business or public organization); (b) any political party, official thereof, or candidate for political office; or (c) any other person if a party or any respective partner, officer, director, employee, agent, representative or shareholder of such party knows or has reason to suspect or know that any part of such money or thing of value will be offered, given or promised, directly or indirectly, to any of the above-identified persons or organizations. Each party acknowledges and agrees that none of its officers, directors, employees, agents or representatives is a government official or employee or an official or employee of any department or instrumentality of any government, nor is any of them an officer of a political party or candidate for political office, who will share directly or indirectly any part of the sums that may be paid pursuant to performance of this Agreement; and each party agrees to immediately notify the other party should the foregoing change during the term of this Agreement. Each party represents and warrants that neither this Agreement nor the performance of or exercise of rights under this Agreement is restricted by, in conflict with, requires registration or approval or tax withholding under, or will require any termination or expiration, compensation, or any compulsory licensing under, any applicable law or regulation of any country or other governmental entity, and each party will not make any claim to the contrary (each party is relying on this representation and warranty, among other provisions of this Agreement, in entering this Agreement and would not enter this Agreement in its absence).

5.5 Trade Controls. Customer understands that the Solutions may be subject to the export control, economic sanctions, customs, import, and anti-boycott laws, regulations, and orders promulgated or enforced by Canada, the United States, Customer's jurisdictions of incorporation and operations, and any other country or governmental body having jurisdiction over the parties to this Agreement ("**Trade Controls**"). Customer shall ensure that the Solutions are not re-exported, provided or transferred to any person or entity listed on any restricted or prohibited persons list issued by Canada, the United States, Germany, or any governmental authority of any applicable jurisdiction, including but not limited to the Bureau of Industry and Security's Denied Persons, Entity, or Unverified List or the Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List, Foreign Sanctions Evaders List, or Sectoral Sanctions Identifications List (collectively, the "**Restricted Persons Lists**"). Customer represents and warrants that it and its shareholders, members, partners, or other owners are not listed on, or owned 50% or more, collectively or individually, by anyone on a Restricted Persons List. Customer shall not use the Solutions (a) for a military application, wherever located; or (b) with knowledge or reason to know that the Solutions will be used for nuclear, chemical, or biological weapons proliferation or (c) for any other end use or by any end user otherwise prohibited by applicable Trade Controls. Upon request by Arctic Wolf, Customer will complete and provide an end use certificate in the form requested by Arctic Wolf. Arctic Wolf may suspend and/or cancel the export, delivery, and/or servicing of the Solutions, if: (i) Arctic Wolf has not received requested end-user certifications; (ii) Arctic Wolf has not received any government approvals required to comply with Trade Controls, or (iii) Arctic Wolf believes that such activity may violate any Trade Controls. If the Solutions are resold or transferred in violation of any Trade Controls or the provision of this Agreement, Arctic Wolf shall not be obligated to provide any warranty service or technical support for such Items.

5.6 Public Entity Customers. If Customer is a public entity, Customer acknowledges and agrees this Agreement is the sole set of terms governing the delivery of the Solutions to Customer and for the avoidance of doubt, terms related to acceptance related to any services or work product shall not apply. The terms of any request for proposal(s), request for information, invitation to qualify, purchasing agreement or cooperative contract, or similar agreement Customer is using to purchase the Solutions (as defined below) from an Authorized Partner do not apply to Arctic Wolf. Further, Customer understands, and hereby consents, that Solutions Data may be accessed and processed by Arctic Wolf and its non-US Affiliates and their non-US citizen employees and Arctic Wolf's authorized third-party service providers in the United States, Europe, or other locations around the world.

Customer represents that in purchasing the Solutions, (i) Customer is not relying on Arctic Wolf for performance of a federal prime contract or subcontract and (ii) Customer is not receiving federal funds to purchase the Solutions. If Customer does intend to rely on Arctic Wolf Solutions to fulfill its obligations under a federal prime contract or subcontract or utilize federal funds to purchase the Solutions, Customer agrees to provide Arctic Wolf advance written notice of that intention, and Arctic Wolf shall have the option to terminate this Agreement.

Technology is a "commercial item", "commercial computer software" and "commercial computer software documentation," pursuant to DFARS Section 227.7202 and FAR Sections 12.211-12.212, as applicable. All Arctic Wolf Technology is and was developed solely at private expense and the use of Arctic Wolf Technology by the United States Government are governed solely by this Agreement and are prohibited except to the extent expressly permitted by this Agreement.

Customer represents it has the requisite authority to enter into and perform under this Agreement.

6. Fees, Payment, Taxes, and Audit.

6.1 Fees, Payment, & Taxes. Customer will purchase the Solutions through the Authorized Partner. The Order Form containing terms related to fees, payment, taxes, audit, and any other related terms shall be between Customer and the Authorized Partner. Customer will pay any owed amounts to the Authorized Partner, as agreed between Customer and Authorized Partner. Customer agrees that Arctic Wolf may suspend or terminate Customer's use of the Solutions upon ten (10) days' written notice to Customer if Arctic Wolf does not receive payment of Fees from the Authorized Partner. The amounts paid by Authorized Partner to Arctic Wolf for Customer's use of the Solutions under this Agreement will be deemed the amount actually paid or payable under this Agreement for purposes of calculating Arctic Wolf's liability under Section 11. Customer's renewal pricing will be communicated to Customer by the Authorized Partner in accordance with the terms Customer has with the Authorized Partner or by Arctic Wolf prior to the renewal Subscription Term.

6.2 Audit. During the term of this Agreement and for one year thereafter, Customer shall provide Arctic Wolf, or its designated representative, promptly upon request with appropriate records requested by Arctic Wolf to verify Customer's compliance with the Agreement,

including specifically its license counts as set forth on an Order Form. Arctic Wolf, at its option, may require that an executive officer of Customer certify in writing to Customer's compliance with this Agreement and disclose the scope of use of the Solutions by Customer. If, because of such audit, Arctic Wolf determines that Customer has exceeded the number of licenses subscribed to by Customer on an Order Form, Arctic Wolf will notify Customer of the number of additional licenses, along with the associated Subscription Fees prorated through the end of the then-current Subscription Term, and Customer will remit payment for such Subscription Fees in accordance with this Section 6.

7. Confidentiality. Either party (as a "**Discloser**") may disclose confidential and proprietary information, orally or in writing ("**Confidential Information**") to the other party (as a "**Recipient**"). Confidential Information (a) shall be marked with a restrictive legend of the Discloser or, (b) if orally or visually disclosed to Recipient by Discloser, or disclosed in writing without an appropriate letter, proprietary stamp or legend, shall be confidential if it would be apparent to a reasonable person that such information is confidential or proprietary. Confidential Information of Arctic Wolf includes the following: any pricing, trade secrets, know-how, inventions (whether or not patentable), techniques, ideas, or processes related to the Arctic Wolf Technology; the design and architecture of the Arctic Wolf Technology; the computer code, internal documentation, and design and functional specifications of the Arctic Wolf Technology; Arctic Wolf's security and privacy due diligence material such as SOC2 reports, security and privacy questionnaire responses & memos; and any intellectual property and know-how included in the problem reports, analysis, and performance information related to the Arctic Wolf Technology. Confidential Information of Customer may include the following:

(i) If the MA or MA+ Solution is deployed: User setup details, including email, work title, and name; Solution metrics related to such Users, including your Users' learning status, training scores, and Phishing results associated with such Users' use of the Solution (collectively "**Learner Data**"); Customer created and owned content, if any; and

(ii) If MDR and/or MR Solutions are deployed: Solutions Data (as defined in Section 8.1 below).

Each party agrees to hold the other party's Confidential Information in strict confidence, not to disclose such Confidential Information to third parties not authorized by the Discloser to receive such Confidential Information, and not to use such Confidential Information for any purpose except as expressly permitted hereunder and as described in the Privacy Notice. Each party agrees to take commercially reasonable steps to protect the other party's Confidential Information and to ensure that such Confidential Information is not disclosed, distributed or used in violation of the provisions of this Agreement. The Recipient may disclose Confidential Information only: (a) with the Discloser's prior written consent; or (b) to those employees, officers, directors, agents, consultants, third party service providers, and advisors with a clear and well-defined "need to know" purpose who are informed of and bound by confidentiality obligations no less restrictive than those set forth in this Section 7. Notwithstanding the foregoing, the Recipient may disclose Confidential Information to the extent required by law; however, the Recipient will give, to the extent legally permissible and reasonably practical, the Discloser prompt notice to allow the Discloser a reasonable opportunity to obtain a protective order and such Confidential Information disclosed to the extent required by law shall otherwise remain confidential and subject to the protections and obligations of this Agreement. For the avoidance of doubt, Arctic Wolf may share Customer's name with Customer's services providers to assist Customer in the resolution of technical issues pertaining to the Solutions. To the extent legally required, Arctic Wolf may report any violations of law pertaining to Customer's use of the Solutions. The Discloser agrees that the foregoing confidentiality obligations shall not apply with respect to any information that the Recipient can document is: (i) rightfully in its possession or known to it prior to receipt from the Discloser without an obligation of confidentiality; (ii) or has become public knowledge through no fault of the Recipient; (iii) rightfully obtained by the Recipient from a third party without breach of any confidentiality obligation; or (iv) independently developed by employees of the Recipient who had no access to Discloser's Confidential Information. Upon expiration or termination of this Agreement for any reason, and except as otherwise provided in Section 14 below, each party shall promptly destroy all copies of the other party's Confidential Information and copies, notes or other derivative material relating to the Confidential Information. Notwithstanding the foregoing, and subject to the Privacy Notice, Arctic Wolf may retain Point of Contact Information which may include first name, last name, corporate email address, phone number, job title, address, and organization hierarchy following termination of this Agreement for its internal business purposes.

8. Solutions Data.

8.1 Solutions Data. "**Solutions Data**" means, depending on the Solution deployed, the operational system log data and any other information provided by Customer in furtherance of its use of the Solutions and which Customer may elect to submit to Arctic Wolf through the Solutions, including, but not limited to operational values, event logs, and network data such as flow, HTTPS, TLS, DNS metadata, cursory inventory data, operating systems and versions, users and groups from Active Directory, system level inventory, event data, and network vulnerability data, but excluding Threat Intelligence Data (as defined below). As between the parties, Customer shall retain all right, title and interest (including any and all intellectual property rights) in and to the Solutions Data (excluding any Arctic Wolf Technology used with the Solutions Data). Customer hereby grants Arctic Wolf, during the term of the Agreement, a non-exclusive, worldwide, royalty-free right to collect, use, copy, store, transmit, modify and create derivative works of the Solutions Data solely to the extent necessary to provide the Solutions to Customer. The location of the storage of raw Solutions Data within Arctic Wolf's third party service providers' data centers will be as set forth in the Solutions Terms. "**Threat Intelligence Data**" means any malware, spyware, virus, worm, trojan, or other potentially malicious or harmful code or files, URLs, DNS data, public IP addresses, network telemetry, commands, processes or techniques, tradecraft used by threat actors, metadata, or other information or data, in each case that is potentially related to unauthorized third parties associated therewith and that: (i) Customer provides to Arctic Wolf in connection with this Agreement, or (ii) is collected or discovered during the course of Arctic Wolf providing Solutions, excluding any such information or data that identifies Customer or to the extent that it includes Personal Data (as defined below) of the data subjects of Customer (but including personal information of threat actors).

8.2 Personal Information. Confidential Information may include information that identifies, relates to, describes, is reasonably capable of being associated with or linked to a particular individual, whether directly or indirectly ("**Personal Information**"). Customer is responsible for the lawfulness of any such Personal Information and the receipt, use, and processing of it under the Agreement. Customer represents and warrants that, where it provides Personal Information to Arctic Wolf or requests Arctic Wolf collect or process such information, it (1) has complied with any applicable laws relating to the collection or provision of such information, (2) possesses any consents, authorizations, rights and authority, and has given all required notices to individual data subjects as are required to transfer or permit Arctic Wolf to collect, receive, or access any Personal Information for the Solutions, and (3) to the extent required by applicable law, informed the individuals of the possibility of Arctic Wolf processing their Personal Information on Customer's behalf and in accordance with its instructions.

8.3 European Union and United Kingdom General Data Protection Regulation. If and to the extent Customer submits to Arctic Wolf personal data (as that term is defined under the General Data Protection Regulation ("**GDPR**") of individuals located in the European Economic

Area or United Kingdom, the Arctic Wolf Data Processing Agreement available at <https://arcticwolf.com/terms/dpa/>, as may be updated by Arctic Wolf from time-to-time in accordance with its terms (the "DPA"), may be executed by Customer and upon execution and return to Arctic Wolf in accordance with its terms will be incorporated into this Agreement. It is Customer's sole responsibility to notify Arctic Wolf of requests from data subjects related to the modification, deletion, restriction and/or objection of personal data. Customer represents and warrants that any processing of personal data in accordance with its instructions is lawful.

8.4 California Consumer Privacy Act. The parties acknowledge and agree that Arctic Wolf is a service provider for the purposes of the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA") and may receive personal information (as defined by the CCPA) from Customer pursuant to this Agreement for a business purpose. The parties agree to comply at all times with the applicable provisions of the CCPA in respect to the collection, transmission, and processing of all personal information (as defined by the CCPA) exchanged or shared pursuant to the Agreement. Arctic Wolf shall not (i) sell any such personal information; (ii) retain, use or disclose any personal information provided by Customer pursuant to this Agreement except as necessary for the specific purpose of performing the Solutions for Customer pursuant to this Agreement or as permitted by the CCPA; (iii) retain, use, or disclose such personal information for a commercial purpose other than providing the Solutions unless otherwise explicitly permitted under the Agreement; or (iv) retain, use, or disclose such personal information outside of the direct business relationship between Customer and Arctic Wolf unless otherwise permitted under the Agreement. The terms "personal information," "service provider," "sale," and "sell" are as defined in Section 1798.140 of the CCPA. Arctic Wolf certifies that it understands the restrictions of this Section 8.4. It is Customer's sole responsibility to notify Arctic Wolf of any requests from consumers (as defined in the CCPA) seeking to exercise rights afforded in the CCPA with regard to personal information received or processed in connection with the Solutions. Arctic Wolf agrees to provide reasonable cooperation to Customer in connection with such requests.

8.5 Canadian Privacy Laws. If and to the extent Customer submits to Arctic Wolf personal information (as that term is defined under applicable Canadian privacy laws, being all applicable federal, and provincial laws and regulations relating to the processing, protection or privacy of personal information ("Privacy Laws"), of individuals located in Canada, Customer agrees that it is solely responsible for and shall obtain from all such individuals, all required consents and/or provide all required notifications, regarding the collection, use, disclosure, and processing of their personal information by Arctic Wolf/Arctic Wolf's subcontractors/third party service providers (which may be located outside of Canada), and/or the transfer by Customer of such individual's personal information to Arctic Wolf/Arctic Wolf's subcontractors/third party service providers (which may be located outside of Canada). Upon request of Customer, Arctic Wolf will inform Customers of the locations to which the personal information is transferred and processed by Arctic Wolf and/or its subcontractors/third party service providers.

Customer retains control of the personal information and remains solely responsible for its compliance with Privacy Laws and for the processing instructions it gives to Arctic Wolf. The parties agree that this Agreement, together with Customer's use of the Solution in accordance with this Agreement, constitutes Customer's instructions to Arctic Wolf in relation to the processing of such personal information. Subject to Section 8.1 of this Agreement, Arctic Wolf will only process the personal information to the extent, and in such a manner, as is necessary for the performance of the Solutions. Arctic Wolf will reasonably assist Customer with meeting the Customer's compliance obligations under applicable Privacy Laws, considering the nature of Arctic Wolf's processing and the information available to Arctic Wolf.

Arctic Wolf shall:

- Comply with its obligations as a third party service provider/mandatory under applicable Privacy Laws, including by implementing appropriate technical, physical and organizational measures to safeguard the personal information;
- Periodically conduct audits of its information security controls for facilities and systems used to deliver the Solutions and make relevant audit reports available to Customer for review. The Customer will treat such audit reports as Arctic Wolf's Confidential Information;
- Within seventy-two (72) hours of discovery notify Customer of any unauthorized or unlawful access to or processing of the personal information;
- Limit access to those employees who require the personal information access to meet Arctic Wolf's obligations under this Agreement and ensure that all employees are informed of the personal information's confidential nature;
- Notify Customer if it receives any complaint, notice, or communication that directly or indirectly relates to the personal information processing or to either party's compliance with Privacy Laws, and provide its full co-operation and assistance in responding to such complaint, notice or communication; and
- Upon Customer's request, provide the Customer a copy of or access to all or part of the Customer's personal information in its possession or control in the format reasonably agreed to by the parties.

8.6 Australian Privacy Laws. If and to the extent Customer submits to Arctic Wolf personal information (as that term is defined in the Australian Privacy Act 1988 (Cth)) on your behalf, as agent for you, Arctic Wolf will only handle your personal information for the purpose of performing the Solutions, in accordance with the Privacy Notice or as required by applicable law, and ensuring you have access to your Solutions Data in accordance with this Agreement. Customer will maintain effective control of how Solutions Data is handled by retaining the right to access, changing and retrieving Solutions Data, limiting others' use of Solutions Data and specifying security measures that are used in relation to Solutions Data as set forth in this Agreement, including the Privacy Notice.

8.7 South African Privacy Laws. If and to the extent Customer submits to Arctic Wolf personal information (as that term is defined in the Protection of Personal Information Act, 4 of 2013) of individuals located in South Africa, Customer agrees that it is solely responsible for and shall obtain from all such individuals, all required consents and/or provide all required notifications, regarding the collection, use, disclosure, and processing of their personal information by Arctic Wolf/Arctic Wolf's subcontractors/third party service providers (which may be located outside of South Africa, and/or the transfer by Customer of such individual's personal information to Arctic Wolf/Arctic Wolf's subcontractors/third party service providers (which may be located outside of South Africa). Upon request of Customer, Arctic Wolf will inform Customers of the locations to which the personal information is transferred and processed by Arctic Wolf and/or its subcontractors/third party service providers. Arctic Wolf will only handle personal information for the purpose of performing the Solutions and ensuring Customer has access to its Solutions Data in accordance with this Agreement. Customer will maintain effective control of how Solutions Data is handled by retaining the right to access, changing, and retrieving Solutions Data, limiting others' use of Solutions Data. Arctic Wolf shall take appropriate, reasonable technical and organizational security measures to prevent the loss of, damage to or unauthorized destruction of personal information, and the unlawful access to or processing of personal information.

9. Indemnity.

9.1 Arctic Wolf's Indemnity. Subject to Section 9.3, Arctic Wolf will defend and indemnify Customer from any unaffiliated third party claim or action to the extent based on the allegation that the Solutions infringe any intellectual property right (patents, utility models, design rights, copyrights and trademarks or any other intellectual property right) having effect in the United States, Canada, Australia, United Kingdom, and the European Union. Arctic Wolf will pay any settlements that Arctic Wolf agrees to in a writing signed by an authorized officer of Arctic Wolf or final judgments awarded to the third party claimant by a court of competent jurisdiction. The foregoing obligations do not apply with respect to the Solutions, or portions or components thereof, that are: (a) not provided by Arctic Wolf; (b) combined with other products, processes or materials that are not reasonably contemplated by the Documentation where the alleged infringement relates to such combination; (c) modified other than with Arctic Wolf's express consent; (d) used after Arctic Wolf's notice to Customer of such activity's alleged or actual infringement; or (e) not used by Customer in strict accordance with this Agreement or the published Documentation. The indemnification obligations set forth in this Section 9.1 are Arctic Wolf's sole and exclusive obligations, and Customer's sole and exclusive remedies, with respect to infringement or misappropriation of third-party intellectual property rights of any kind.

9.2 Customer Indemnity. Subject to Section 9.3, Customer agrees to defend and indemnify Arctic Wolf from any third-party claim or action brought against Arctic Wolf to the extent based on Customer's alleged breach of Sections 5 or 8. Customer agrees to pay any settlements that Customer agrees to in a writing signed by an authorized officer of Customer or final judgments awarded to the third party claimant by a court of competent jurisdiction.

9.3 Procedures. Each party's indemnification obligations are conditioned on the indemnified party: (a) providing the indemnifying party with prompt written notice of any claim, provided that the failure to provide such notice shall only limit the indemnifying party's obligation to indemnify to the extent that the failure prejudices the indemnifying party in its defense of the claim; (b) granting the indemnifying party the sole control of the defense or settlement of the claim; and (c) providing reasonable information and assistance to the indemnifying party in the defense or settlement of the claim at the indemnifying party's expense. Notwithstanding the foregoing, the indemnifying party (i) may not make an admission of fault on behalf of the other party without written consent, (ii) any settlement requiring the party seeking indemnification to admit liability requires prior written consent, not to be unreasonably withheld or delayed, and (iii) the other party may join in the defense with its own counsel at its own expense.

9.4 Options. If Customer's use of the Solutions has become, or in Arctic Wolf's opinion is likely to become, the subject of any claim of infringement, Arctic Wolf may at its option and expense: (a) procure for Customer the right to continue using and receiving the Solutions as set forth hereunder; (b) replace or modify the Solutions to make them non-infringing; (c) substitute an equivalent for the Solutions; or (d) if Arctic Wolf, in its sole discretion, determines that options (a)-(c) are not reasonably practicable, terminate this Agreement and refund any pre-paid unused Fees as of the effective date of termination.

10. Warranty and Warranty Disclaimer.

10.1 Solutions Warranty. ARCTIC WOLF WARRANTS THAT DURING THE SUBSCRIPTION TERM AND PROVIDED THAT CUSTOMER IS NOT IN BREACH OF THIS AGREEMENT OR AS OTHERWISE PROHIBITED BY CONSUMER PROTECTION LAWS INCLUDING ANY CUSTOMER RIGHTS UNDER SUCH CONSUMER PROTECTION LAWS THAT: (I) THE SOLUTIONS PROVIDED UNDER THIS AGREEMENT DO NOT INFRINGE OR MISAPPROPRIATE ANY INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY; (II) THE SOLUTIONS SHALL SUBSTANTIALLY PERFORM AS DESCRIBED IN THE DOCUMENTATION; AND (III) IT WILL COMPLY WITH ALL FOREIGN, PROVINCIAL, FEDERAL, STATE AND LOCAL STATUTES, LAWS, ORDERS, RULES, REGULATIONS AND REQUIREMENTS, INCLUDING THOSE OF ANY GOVERNMENTAL (INCLUDING ANY REGULATORY OR QUASI-REGULATORY) AGENCY APPLICABLE TO ARCTIC WOLF AS IT PERTAINS TO ITS OBLIGATIONS AND THE DATA REQUIRED FOR THE PERFORMANCE OF THE SOLUTIONS DESCRIBED HEREIN. IN THE EVENT OF ANY BREACH OF THIS SECTION 10.1, ARCTIC WOLF SHALL, AS ITS SOLE LIABILITY AND CUSTOMER'S SOLE REMEDY (OTHER THAN ARCTIC WOLF'S INDEMNIFICATION OBLIGATIONS IN SECTION 9.1 ABOVE, OR OTHERWISE PROHIBITED BY CONSUMER PROTECTION LAWS AND SECTION 11.2 OF THIS AGREEMENT), REPAIR OR REPLACE THE SOLUTIONS THAT ARE SUBJECT TO THE WARRANTY CLAIM AT NO COST TO CUSTOMER OR IF ARCTIC WOLF IS UNABLE TO REPAIR OR REPLACE, THEN ARCTIC WOLF WILL REFUND ANY PRE-PAID FEES FOR THE SOLUTIONS, OR PARTS THEREOF, SUBJECT TO THE WARRANTY CLAIM. EXCEPT FOR THE WARRANTIES DESCRIBED IN THIS SECTION, THE SOLUTIONS ARE PROVIDED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF DESIGN, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES OF TITLE. CUSTOMER ACKNOWLEDGES THAT THE SOLUTIONS ARE PROVIDED "AS IS" AND FURTHER ACKNOWLEDGES THAT ARCTIC WOLF DOES NOT WARRANT: (A) THE OPERATION OF THE SOLUTIONS WILL BE UNINTERRUPTED, OR ERROR FREE; AND (B) THE SOLUTIONS ARE NOT VULNERABLE TO FRAUD OR UNAUTHORIZED USE. CUSTOMER IS RESPONSIBLE AND ARCTIC WOLF SHALL HAVE NO RESPONSIBILITY FOR DETERMINING THAT THE USE OF THE SOLUTIONS COMPLIES WITH APPLICABLE LAWS IN THE JURISDICTION(S) IN WHICH CUSTOMER MAY DEPLOY AND USE THE SOLUTIONS.

10.2 No Guarantee. CUSTOMER ACKNOWLEDGES, UNDERSTANDS, AND AGREES THAT ARCTIC WOLF DOES NOT GUARANTEE OR WARRANT THAT IT WILL FIND, LOCATE, OR DISCOVER ALL OF CUSTOMER'S SYSTEM THREATS, VULNERABILITIES, MALWARE, AND MALICIOUS SOFTWARE, OR THAT ALL SUCH SYSTEM THREATS, VULNERABILITIES, MALWARE, AND MALICIOUS SOFTWARE CAN OR WILL BE CONTAINED OR UNCONTAINED IN THE DELIVERY OF THE SOLUTIONS. CUSTOMER ACKNOWLEDGES THAT CERTAIN FEATURES AND ACTIVITIES PERFORMED BY ARCTIC WOLF AND MORE FULLY DESCRIBED IN THE SOLUTIONS TERMS COULD POSSIBLY RESULT IN INTERRUPTIONS OR DEGRADATION TO CUSTOMER'S SYSTEMS AND ENVIRONMENT AND ACCEPTS THOSE RISKS AND CONSEQUENCES. CUSTOMER ASSUMES ALL RISKS IN USING THIRD PARTY SYSTEMS OR SERVICES IN CONNECTION WITH THE DELIVERY OF THE SOLUTIONS.

10.3 Open Source Warranty. The Software may include Open Source Software. To the extent included in the Software, Open Source Software is governed solely by the applicable open source licensing terms, if any, and is provided "AS IS", and Arctic Wolf hereby disclaims all copyright interest in such Open Source Software. Arctic Wolf provides no warranty specifically related to any Open Source Software or any applicable Open Source Software licensing terms. Any fees paid by Customer to Arctic Wolf are for Arctic Wolf's proprietary Software only, and not for any Open Source Software components of the Software. Any license associated with an Open Source Software component applies only to that component and not to Arctic Wolf's proprietary Software or any other third-party licensed software. The foregoing language is not intended

to limit Arctic Wolf's warranty obligation for the Solutions set forth in Section 10.1. "Open Source Software" means software with its source code made available pursuant to a license by which, at a minimum, the copyright holder provides anyone the rights to study, change, and/or distribute the software to anyone and for any purpose.

10.4 Third Party Product. Third Party Product (as defined in this Section 10.4) may carry a limited warranty from the third-party publisher, provider, or original manufacturer of such Third Party Products. To the extent required or allowed, Arctic Wolf will pass through to Customer or directly manage for the benefit of Customer's use of the Third Party Products as part of the Solutions (such decision to be made in Arctic Wolf's discretion), the manufacturer warranties related to such Third Party Products. "Third Party Product" means any non-Arctic Wolf branded products and services (including Equipment, and any operating system software included therewith) and non-Arctic Wolf-licensed software products, including Open Source Software.

10.5 Customer Warranties. Customer represents and warrants that it shall: (i) be responsible for ensuring the security and confidentiality of all Administrator IDs and passwords; (ii) use commercially reasonable efforts to prevent unauthorized access to, or use of, the Solutions; (iii) notify Arctic Wolf promptly upon discovery of any unauthorized use of the Solutions or any breach, or attempted breach, of security of the Solutions; (iv) not violate any foreign, provincial, federal, state and local statutes, laws, orders, rules, regulations and requirements applicable to Customer's performance of its obligations herein, including those of any governmental (including any regulatory or quasi-regulatory) agency, Trade Control laws, and regulations and the U.S. Foreign Corrupt Practices Act (the "**FCPA**"); (v) not use the Solutions and transfer any Solutions Data to Arctic Wolf for any fraudulent purposes; and (vi) implement safeguards within Customer's environment to protect the Solutions, including specifically, the Equipment, from the introduction, whether intentional or unintentional, of: (1) any virus or other code, program, or sub-program that damages or interferes with the operation of the Equipment or halts, disables, or interferes with the operation of the Solutions; or (2) any device, method, or token whose knowing or intended purpose is to permit any person to circumvent the normal security of the Solutions. Customer authorizes Arctic Wolf to perform Services (and all such tasks and tests reasonably contemplated by or reasonably necessary to perform the Services) on network resources with the internet protocol addresses or other designated identifiers identified by Customer. Customer represents that, if Customer does not own such network resources, it will have obtained consent and authorization from the applicable third party to permit Arctic Wolf to provide the Services on such third party's network resources.

11. Limitation of Liability.

11.1 TO THE FULL EXTENT PERMITTED BY LAW AND SUBJECT TO SECTION 11.2 BELOW, FOR ANY CAUSE RELATED TO OR ARISING OUT OF THIS AGREEMENT, WHETHER IN AN ACTION BASED ON A CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR ANY OTHER LEGAL THEORY, HOWEVER ARISING, ARCTIC WOLF WILL IN NO EVENT BE LIABLE TO CUSTOMER OR ANY THIRD PARTY FOR: (A) DAMAGES BASED ON USE OR ACCESS, INTERRUPTION, DELAY OR INABILITY TO USE THE SOLUTIONS, LOST REVENUES OR PROFITS, LOSS OF SOLUTIONS, BUSINESS OR GOODWILL, LOSS OR CORRUPTION OF DATA, LOSS RESULTING FROM SYSTEM FAILURE, MALFUNCTION OR SHUTDOWN, FAILURE TO ACCURATELY TRANSFER, READ OR TRANSMIT INFORMATION, FAILURE TO UPDATE OR PROVIDE CORRECT INFORMATION, SYSTEM INCOMPATIBILITY OR PROVISION OF INCORRECT COMPATIBILITY INFORMATION, BREACHES BY AN AUTHORIZED PARTNER, OR BREACHES IN CUSTOMER'S SYSTEM SECURITY; OR (B) ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR (C) ANY AMOUNTS THAT EXCEED THE TOTAL FEES PAID OR PAYABLE BY CUSTOMER FOR THE SOLUTIONS THAT ARE THE SUBJECT OF THE CLAIM DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRIOR TO THE EVENT WHICH GIVES RISE TO SUCH DAMAGES. THESE LIMITATIONS SHALL APPLY WHETHER OR NOT ARCTIC WOLF HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. BOTH PARTIES UNDERSTAND AND AGREE THAT THE LIMITATIONS OF LIABILITIES FOR EACH PARTY SET FORTH IN THIS AGREEMENT ARE REASONABLE AND THEY WOULD NOT HAVE ENTERED INTO THE AGREEMENT WITHOUT SUCH LIMITATIONS. THE FOREGOING LIMITATIONS OF LIABILITY IN THIS SECTION 11, WITH RESPECT TO ARCTIC WOLF AUSTRALIAN CUSTOMERS, ARE SUBJECT TO THE *COMPETITION AND CONSUMER ACT 2010 (CTH) SCH 2* AND SECTION 11.2 OF THIS AGREEMENT.

11.2 FOR CUSTOMERS DEEMED "CONSUMERS" AS DEFINED BY THE *COMPETITION AND CONSUMER ACT 2010 (CTH) SCH 2*, SECTION 11.1 IS REPLACED IN ITS ENTIRETY WITH THE FOLLOWING:

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW ARCTIC WOLF SHALL NOT BE LIABLE TO CUSTOMER (UNDER ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STATUTE, TORT OR OTHERWISE) FOR: (A) ANY LOST PROFITS, REVENUE, OR SAVINGS, LOST BUSINESS OPPORTUNITIES, LOST DATA, OR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, EVEN IF ARCTIC WOLF HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES OR SUCH DAMAGES OR LOSSES WERE REASONABLY FORESEEABLE; OR (B) AN AMOUNT THAT EXCEEDS THE TOTAL FEES PAID OR PAYABLE BY CUSTOMER FOR THE SOLUTIONS THAT ARE THE SUBJECT OF THE CLAIM DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRIOR TO THE EVENT WHICH GIVES RISE TO SUCH DAMAGES. THESE LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY SPECIFIED IN THESE TERMS. MULTIPLE CLAIMS SHALL NOT EXPAND THE LIMITATIONS SPECIFIED IN THIS SECTION 11.2. THIS SECTION 11.2 DOES NOT SEEK TO LIMIT OR EXCLUDE THE LIABILITY OF ARCTIC WOLF OR ITS AFFILIATES IN THE EVENT OF DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE OR FOR FRAUD OR FOR ANY OTHER LIABILITY FOR WHICH IT IS NOT PERMITTED BY LAW TO EXCLUDE. TO THE EXTENT APPLICABLE, THIS PROVISION MUST BE READ SUBJECT TO THE *COMPETITION AND CONSUMER ACT 2010 (CTH) SCH 2*.

12. Term and Renewal. This Agreement shall be in effect for the Subscription Term specified in the Order Form. The Order Form or other equivalent transaction document containing the terms related to the length of the Subscription Term and any renewal thereof, and any other related terms, as may be applicable, shall be between Customer and the Authorized Partner. Notwithstanding the foregoing, and unless otherwise set forth on an Order Form, the Subscription Term to the Solutions, in its entirety, will automatically renew at the end of the initial Subscription Term for the same period of time as the initial Subscription Term, but in no event more than a twelve (12) month term, and subject to the then-current terms and price at the time of renewal; provided however, if either party would like to opt out of automatic renewal of the Subscription of the Solutions or reduce Subscription scope, then such party must notify the other party no less than sixty (60) days prior to the expiration of the then-current Subscription Term.

13. Updates. Arctic Wolf reserves the right to modify this Agreement, the Terms, and the Documentation in Arctic Wolf's sole discretion provided that changes to the Solutions Terms shall not materially decrease the Solutions features and functionalities that Customer has

subscribed to during the then-current Subscription Term. Should Arctic Wolf make any modifications to the Agreement, the Terms, or Documentation, Arctic Wolf will post the amended terms on the applicable URL links and will update the **"Last Updated Date"** within such documents and notify Customer via email, the Customer newsletter or such other written communication method implemented by Arctic Wolf from time-to-time. Customer may notify Arctic Wolf within 30 days after the effective date of the change of its rejection of such change. If Customer notifies Arctic Wolf of its rejection during such thirty (30) day period, then Customer will remain governed by the terms in effect immediately prior to the change until the end of Customer's then-current Subscription Term. However, any subsequent renewal of the Subscription Term will be renewed under the then-current terms, unless otherwise agreed in writing by the parties.

14. Termination. Either party may terminate this Agreement for cause if the other party commits a material breach of this Agreement, provided that such terminating party has given the other party ten (10) days advance notice to try and remediate the breach. Upon termination, Customer agrees to cease all use of the Arctic Wolf Technology, installed or otherwise, and permanently erase or destroy all copies of any Arctic Wolf Technology, including all Content and virtual Equipment, that are in its possession or under its control and promptly remove and return all physical Equipment to Arctic Wolf. Except as otherwise required by law, Arctic Wolf will remove, delete, or otherwise destroy all copies of Confidential Information in its possession upon the earlier of (i) the return of the Equipment, if applicable, to Arctic Wolf, or (ii) one hundred-twenty (120) days following termination. Notwithstanding anything contrary in this Agreement, should Customer fail to return any Equipment within ninety (90) days following discontinuation of use of the Equipment or termination or expiration of this Agreement, Customer will be liable for the replacement cost of the Equipment, which shall be due and owing upon receipt of the invoice from Arctic Wolf or the Authorized Partner, and Customer shall be liable for any breach of the Confidential Information and Arctic Wolf Technology contained within the unreturned Equipment. Sections 6 through 13, 14, and 15 will survive the non-renewal or termination of this Agreement.

15. Miscellaneous.

15.1 Except as otherwise provided herein, all notices, requests, consents, claims, demands, waivers and other communications hereunder shall be in writing and shall be deemed to have been given: (a) when delivered by hand (with written confirmation of receipt); (b) on the next business day after the date sent, if sent for overnight delivery by a generally recognized international courier (e.g., FedEx, UPS, DHL, etc.) (receipt requested); or (c) on the date sent by e-mail (with confirmation of transmission) if sent during normal business hours of the recipient, and on the next business day if sent after normal business hours of the recipient. Such communications must be sent to the respective parties at the addresses set forth on the signature page hereof (or at such other address for a party as shall be specified in a notice given in accordance with this Section 15). For contractual purposes, Customer (1) consents to receive communications in an electronic form via the email address it provides herein or via the Customer Portal; and (2) agrees that all agreements, notices, disclosures, and other communications that Arctic Wolf provides electronically satisfies any legal requirement that those communications would satisfy if they were on paper. This Section does not affect Customer's non-waivable rights.

15.2 Notwithstanding any other terms to the contrary contained herein, Customer grants Arctic Wolf the right to use Customer's name or logo in customer lists, marketing materials, and verbal discussions with prospective customers to communicate that Customer uses the Solutions. If Arctic Wolf intends to disclose information about Customer's purchase(s) (such as dollar amount of sale or project objectives) in conjunction with the use of Customer's name or logo, Arctic Wolf will obtain Customer's prior written or email approval.

15.3 The parties to this Agreement are independent contractors. Neither party has the authority to bind the other party without the express written authorization of the other party. Nothing herein may be construed to create an employer-employee, franchisor-franchisee, agency, partnership, or joint venture relationship between the parties. Arctic Wolf shall be primarily liable for the obligations of its Affiliates and any subcontractors used in the delivery of the Solutions.

15.4 This Agreement shall inure to the benefit of and be binding upon the respective permitted successors and assigns of the parties. Customer shall not be entitled to assign, subcontract, delegate or otherwise transfer any of its rights and/or duties arising out of this Agreement and/or parts thereof to third parties, voluntarily or involuntarily, including by change of control, operation of law or any other manner, without Arctic Wolf's express prior written consent. Any purported assignment, subcontract, delegation or other transfer in violation of the foregoing shall be null and void. No such assignment, subcontract, delegation or other transfer shall relieve the assigning party of any of its obligations hereunder.

15.5 The rights and obligations of the parties under this Agreement shall not be governed by the provisions of the 1980 U.N. Convention on Contracts for the International Sale of Goods or the United Nations Convention on the Limitation Period in the International Sale of Goods, as amended. This Agreement shall be governed by the laws of the State of California without regard to the conflicts of law provisions thereof. Any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be settled by arbitration in Santa Clara County, California in English and in accordance with the JAMS International Arbitration Rules then in effect. Any judgment on the award rendered by the arbitrator may be entered in any court having jurisdiction thereof. Notwithstanding the foregoing, each party shall have the right to institute an action in a court of proper jurisdiction for preliminary injunctive relief pending a final decision by the arbitrator(s), provided that a permanent injunction and damages shall only be awarded by the arbitrator(s). In any action or proceeding to enforce rights under this Agreement, the prevailing party shall be entitled to recover costs and attorneys' fees.

15.6 Each party acknowledges and agrees that any dispute or claim that may arise out of or relate to this Agreement is likely to involve complicated and difficult issues and, therefore, each such party irrevocably and unconditionally waives any right it may have to a trial by jury in respect of any legal action arising out of or relating to this Agreement or the transactions contemplated hereby. Further, each party agrees that regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to this Agreement must be filed within one year after such claim or cause of action arose.

15.7 No failure or delay by any party in exercising any right, power or privilege hereunder shall operate as a waiver thereof nor shall any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any other right, power or privilege. The rights and remedies under this Agreement are cumulative and are in addition to and not in substitution for any other rights and remedies available at law or in equity or otherwise.

15.8 If any provision of this Agreement is held invalid or unenforceable by any court of competent jurisdiction, the other provisions of this Agreement will remain in full force and effect. Any provision of this Agreement held invalid or unenforceable only in part or degree will remain in full force and effect to the extent not held invalid or unenforceable. The parties agree to replace such void or unenforceable provision of this

Agreement with a valid and enforceable provision that will achieve, to the extent possible, the economic, business and other purpose of such void or unenforceable provision. Arctic Wolf does not accept, expressly or impliedly, and rejects and deems deleted any additional or different terms or conditions that Customer presents, including, but not limited to, any terms or conditions contained Customer's purchase order, or other such document, or established by trade usage or prior course of dealing.

15.9 This Agreement (including the exhibits hereto, if any, and any BAA (as defined in Section 15.10 below)) constitutes the parties' entire agreement by and between the parties with respect to the subject matter hereof and supersedes any prior or contemporaneous agreement or understanding by and among the parties with respect to such subject matter. Except as otherwise provided herein, this Agreement may be amended, modified or supplemented only by an agreement in writing signed by each party.

15.10 In the event that Arctic Wolf receives personal healthcare information in the delivery of the Solutions, the parties agree to comply with the Business Associate Addendum ("BAA") located at <https://arcticwolf.com/terms/business-associate-addendum/> or such other equivalent agreement/addendum as required under applicable health information/privacy laws. In the event the parties have entered into a BAA or equivalent agreement in relation to protected health information, the parties intend for both this Agreement and BAA or equivalent agreement to be binding upon them and the BAA or equivalent agreement is incorporated into this Agreement by reference.

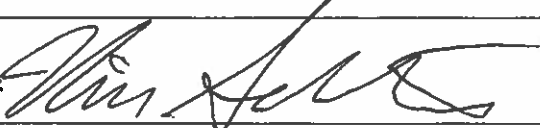
15.11 The parties have participated mutually in the negotiation and drafting of this Agreement. In the event an ambiguity or question of intent or interpretation arises, this Agreement will be construed as if drafted mutually by the parties and no presumption or burden of proof will arise favoring or disfavoring any party by virtue of the authorship of any of the provisions of this Agreement.

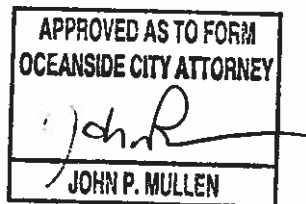
15.12 The parties have agreed that this Agreement as well as any notice, document or instrument relating to it be drawn up in English only; *les parties aux présentes ont convenu que la présente convention ainsi que tous autres avis, actes ou documents s'y rattachant soient rédigés en anglais seulement.*

15.13 Each party agrees that this Agreement and any other documents to be delivered in connection herewith may be electronically signed, and that any electronic signatures appearing on this Agreement or such other documents are the same as handwritten signatures for the purposes of validity, enforceability, and admissibility. This Agreement may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

[signature page to follow]

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives on the Effective Date.

Arctic Wolf Networks, Inc.:	Customer:
Signed: 	Signed:
Name: Nick Schneider	Name:
Title: Chief Executive Officer & President	Title:
Date: 04/08/2023	Date:
Notice Address: PO Box 46390 Eden Prairie, MN 55344 Attn: General Counsel legal@arcticwolf.com	Notice Address:



INDIVIDUAL ACKNOWLEDGMENT

State/Commonwealth of Minnesota }
County of Hennipen } ss.

On this the 8th day of June, 2023, before me,
Maggie Knutson
Name of Notary Public

personally appeared Nick Schneider
Name(s) of Signer(s)

☒ personally known to me – OR –
☐ proved to me on the basis of satisfactory evidence

to be the person(s) whose name(s) is/are subscribed
to the within instrument, and acknowledged to me
that he/she/they executed the same for the purposes
therein stated.

WITNESS my hand and official seal.



Maggie Knutson
Signature of Notary Public

Place Notary Seal/Stamp Above

Any Other Required Information
(Printed Name of Notary, Expiration Date, etc.)

OPTIONAL

*This section is required for notarizations performed in Arizona but is optional in other states.
Completing this information can deter alteration of the document or fraudulent reattachment
of this form to an unintended document.*

Description of Attached Document

Title or Type of Document: _____

Document Date: _____ Number of Pages: _____

Signer(s) Other Than Named Above: _____