Arctic Wolf's Technical & Organizational Measures

(Last Updated: February 3, 2025)

Table of Contents

Managed Detection and Response (MDR), Managed Risk (MR), and/or Managed Security Awareness (MA)

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Arctic Wolf ("Data Importer") has implemented and will maintain the following security measures for the protection of Personal Data (as defined in the Data Processing Addendum), which in conjunction with the security commitments in the Addendum and the General Terms are Arctic Wolf's responsibilities with respect to the security of Personal Data delivered by a Customer ("Data Exporter") for the above named Products for Arctic Wolf's delivery of such Products.

1. **Logical Access Controls**: Data Importer shall employ effective logical access control measures over all systems used to access, create, transmit, or process Personal Data, including but not limited to:
   a) User authentication must use unique identifiers ("**User ID's**") consistent with individual accountability and a complex password.
   b) Prohibition of clear-text credentials must be enforced.
   c) User access rights/privileges to information resources containing Personal Data must be granted on a need-to-know basis consistent with role-based authorization.
   d) User access must be removed immediately upon user separation or role transfer eliminating valid business need for continued access.
   e) Default passwords and security parameters must be changed in third-party products/applications used to support Personal Data and systems for the performance of the Solutions under the Agreement.
   f) Two-factor authentication shall be used to secure all remote administrative access.

2. **Network Security Architecture:** Data Importer shall employ effective network security control measures over all systems used to create, transmit, or process Personal Data including but not limited to:
   a) Firewalls shall be operational at all times and shall be installed at the network perimeter between Data Importer's internal (private) and public (Internet) networks.
   b) Properly configured and monitored IDS/IPS (Intrusion Detection/Prevention Systems) must be used on Data Importer's network.
   c) Secure channels (e.g., SSL, SFTP, SSH, IPSEC, etc.) must be used at all times.

3. **Physical Security:** Data Importer shall maintain servers, databases, and other hardware and/or software components that store information related to Data Exporter's business activities in an access controlled and consistently monitored Data Center secured by appropriate alarm systems, which will not be commingled with another unrelated party's software or information. The facility storing Personal Data must follow best practices for infrastructure systems to include fire extinguishing, temperature control and employee safety.

4. **Risk Assessment/Audit:** At no additional cost Data Importer shall provide Data Exporter with results of a current security assessment by an accredited third party (e.g., SSAE 16-Type II reports, ISO 27001 certification, penetration test report etc.).

5. **Security Policy:** Data Importer maintains and enforces security policies consistent with all legal and privacy requirements applicable to Data Importer as a provider of the Solutions.

6. **Training and Awareness:** Data Importer shall provide necessary training to ensure security awareness in Data Importer personnel that are directly or indirectly engaged in handling Personal Data and systems for the performance of the Solutions, onsite or remotely.

7. **Protection of Personal Data**: In addition to what may be described in the Agreement, where applicable, Data Importer agrees to protect Personal Data as it would its own. For purposes of clarity, Data Importer agrees to adhere to the following controls surrounding the use and protection of Personal Data:
   a) Clear text (ftp, telnet, etc.) protocols may not be used to access or store Personal Data.
   b) Personal Data stored at rest must be encrypted with key sizes of 256-bit for symmetric and 2048-bit for asymmetric encryption.
   c) Personal Data may not be copied, sold or used for solicitation purposes by the Data Importer or its business partners. Personal data may only be used in conjunction with and within the scope of the Agreement.
   d) Personal Data must be segregated from other Data Importer customers, systems, or applications unrelated to Data Exporter.

8. **System Monitoring**: Data Importer shall regularly audit and monitor information systems processing of configured Data Exporter's business activities to ensure the protection of Personal Data. Data Importer must have defined processes for security alerting, escalation and remediation that are consistent with the Solutions procured pursuant

to the Agreement.

9. **Vulnerability Management Controls**: Data Importer shall employ effective vulnerability management control measures over all its systems used to perform the applicable Product and that are used to create, transmit, or process Personal Data, including, but not limited to:
   a) Conduct vulnerability scans of their network to ensure no critical security vulnerabilities remain unresolved post 30 days.
   b) Deploy and maintain currency of up-to-date commercially available anti-virus, anti-spam, anti-malware software on all information system components used for the purpose of managing Personal Data. Additionally, provide for regular scanning for viral infections and update virus signature files frequently.
   c) Maintain a standard patch management process and practice to ensure the protection of any devices used to access, process or store Personal Data.
   d) Within 72 hours of confirmed fraudulent or malicious activity occurring on the Data Importer Solution, to inform the Data Exporter team about the activity to the extent it results in or may result in an unauthorized use or disclosure of Personal Data. Any request by the Data Exporter team for information will be provided to Data Exporter within two hours, to the extent known by Data Importer.
   e) Any security breach that involves Personal Data must be reported to Data Exporter without unreasonable delay. Data Importer shall immediately perform a root cause analysis as well as provide detailed information about measures taken by the Data Importer to prevent future breaches. All efforts to rectify or resolve the situation must include subsequent and regular notification for the reported incident.
   f) Data Importer agrees to provide full cooperation with Data Exporter and in the event of a data breach involving Personal Data including, but not limited to: server log information showing network and application traffic.

10. **Data Destruction:** Data Importer shall ensure that residual magnetic, optical, or electrical representation of Personal Data that has been deleted may not be retrieved or reconstructed when storage media is transferred, become obsolete or is no longer usable or required by Data Exporter.
   a) Data Importer data retention and destruction must comply with applicable laws or regulations.
   b) Personal Data stored on Data Importer media (e.g., hard drive, optical discs, digital media, tapes, paper, etc.) must be rendered unreadable or unattainable using the NIST Guidelines for Media Sanitization (Special Pub 800-88), prior to the media being recycled, disposed of, or moved off-site.

IR JumpStart Retainer (IRJS), Cyber Defense Operations Services (CDO), Cyber JumpStart Portal, Incident Response Services

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Arctic Wolf ("Data Importer") has implemented and will maintain the following security measures for the protection of Personal Data (as defined in the Data Processing Addendum), which in conjunction with the security commitments in the Addendum and the General Terms are Arctic Wolf's responsibilities with respect to the security of Personal Data delivered by a Customer ("Data Exporter") for the above named Products for Arctic Wolf's delivery of such Products.

1. **Logical Access Controls**: Arctic Wolf shall employ effective logical access control measures over all systems used to access, create, transmit, or process Personal Data, including but not limited to:
   a) User authentication must use unique identifiers ("**User ID's**") consistent with individual accountability and a complex password.
   b) Prohibition of clear-text credentials must be enforced.
   c) User access rights/privileges to information resources containing Personal Data must be granted on a need-to-know basis consistent with role-based authorization.
   d) User access must be removed immediately upon user separation or role transfer eliminating valid business need for continued access.
   e) Default passwords and security parameters must be changed in third-party products/applications used to support personal data and systems for the performance of the Services under the Agreement.
   f) Two-factor authentication shall be used to secure all remote administrative access.

2. **Network Security Architecture:** Arctic Wolf shall employ effective network security control measures over all systems used to create, transmit, or process Personal Data. including but not limited to: Secure channels (e.g., SSL, SFTP, SSH, IPSEC, etc.) must be used at all times to transmit data over public networks.

3. **Physical Security:** Arctic Wolf shall maintain servers, databases, and other hardware and/or software components that store Personal Data in an access controlled and consistently monitored data center(s) secured by appropriate alarm systems, which will not be commingled with another unrelated party's software or information. The facility(ies) storing Personal Data must follow best practices for infrastructure systems to include fire extinguishing, temperature control and employee safety.

4. **Security Policy:** Arctic Wolf maintains and enforces security policies consistent with all legal and privacy requirements applicable to Arctic Wolf as a provider of the Services and the specific Personal Data required to deliver the Services.

5. **Training and Awareness:** Arctic Wolf shall provide necessary training to ensure security awareness in Arctic Wolf personnel that are directly or indirectly engaged in handling Personal Data and systems for the performance of the Services, onsite or remotely.

6. **Protection of Personal Data**: In addition to what may be described in the Agreement, where applicable, Arctic Wolf agrees to protect Personal Data as it would its own. For purposes of clarity, Arctic Wolf agrees to adhere to the following controls surrounding the use and protection of Personal Data:
   a) Clear text (ftp, telnet, etc.) protocols may not be used to access or store Personal Data.
   b) Personal Data may not be copied, sold, or used for solicitation purposes by Arctic Wolf or its business partners. Personal Data may only be used in conjunction with and within the scope of the Agreement.
   c) Personal Data must be segregated from other Arctic Wolf customers, systems, or applications unrelated to Customer.

7. **System Monitoring**: Arctic Wolf shall regularly audit and monitor information systems which process Personal Data to ensure the protection of the Personal Data. Arctic Wolf must have defined processes for security alerting, escalation and remediation that are consistent with the Services procured pursuant to the Agreement.

8. **Vulnerability Management Controls**: Arctic Wolf shall employ effective vulnerability management control measures over all its systems used to perform the Services and that are used to create, transmit, or process Personal Data, including, but not limited to:
   a) Within 72 hours of confirmed fraudulent or malicious activity occurring in Arctic Wolf's systems used to process Personal Data, Arctic Wolf will inform the Customer team about the activity to the extent it results in or may result in an unauthorized use or disclosure of Personal Data. Any request by the Customer team for information will be provided to Customer within two (2) hours, to the extent known by Arctic Wolf.
   b) Any security breach that involves Personal Data must be reported to Customer without unreasonable delay.

Arctic Wolf shall immediately perform a root cause analysis as well as provide detailed information about measures taken by the Arctic Wolf to prevent future breaches. All efforts to rectify or resolve the situation must include subsequent and regular notification for the reported incident.

c) Arctic Wolf agrees to provide full cooperation with Customer and in the event of a data breach involving Personal Data.

9. **Personal Data Destruction:** Arctic Wolf shall ensure that residual magnetic, optical, or electrical representation of Personal Data that has been deleted may not be retrieved or reconstructed when storage media is transferred, become obsolete or is no longer usable or required by Customer.

a) Arctic Wolf data retention and destruction must comply with applicable laws or regulations.

b) Personal Data stored on Arctic Wolf media (e.g., hard drive, optical discs, digital media, tapes, paper, etc.) must be rendered unreadable or unattainable, prior to the media being recycled or disposed.

CylanceENDPOINT, CylanceEDGE, CylanceMDR, Aurora Protect, Aurora Endpoint Defense, Aurora Endpoint Defense Mobile Addon, Aurora Managed Endpoint Defense on Demand, Aurora Managed Endpoint Defense

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Arctic Wolf ("Data Importer") has implemented and will maintain the following security measures for the protection of Personal Data (as defined in the Data Processing Addendum), which in conjunction with the security commitments in the Addendum and the General Terms are Arctic Wolf's responsibilities with respect to the security of Personal Data delivered by a Customer ("Data Exporter") for the above named Products for Arctic Wolf's delivery of such Products.

Information Security Policies

- Management approves, maintains, communicates, and enforces policies to provide direction and support for information security to employees and relevant external parties.

Organization of Information Security

- Maintains an information security program that designates technical and organizational measures required to protect the security, confidentiality, and integrity of Personal Data processed on behalf of Data Exporter.

Resource Security

- Performs background checks, where permitted by local laws.
- Requires employees and resources to sign confidentiality and code of conduct agreements.
- Requires employees and resources to affirm compliance with code of conduct agreement annually.
- Requires employees and resources to complete information security and privacy training upon hire and annually.
- Requires employees and resources to be aware of and fulfill their information security responsibilities and obligations.

Asset Management

- Requires information assets be identified, classified, and appropriate responsibilities for ensuring their protection, and establishing retention schedules be assigned.
- Requires an appropriate level of protection for information assets in accordance with their sensitivity level and importance to the organization.
- Prevents the unauthorized disclosure, modification, removal, or destruction of information stored on media.
- Requires data on persistent storage media be rendered unrecoverable and securely disposed of based on information classification.

Access Control

- Establishes governing principles to restrict access to information and reduce the risk of unauthorized access.
- Restricts access to information, systems, and facilities on a need-to-know and job-specific (role-based) basis.
- Assigns system administrative accounts using the least-privilege necessary to support the Products provided to the Data Exporter.
- Requires system administrators accounts follow strong authentication practices.
- Revokes access at the end of an individual's employment or engagement.

Cryptography

- Restricts use of cryptographic modules to algorithms that have received substantial public review and have been proven to work effectively.
- Requires cryptographic keys be protected against modification, loss, destruction, deletion, and unauthorized disclosure.
- Follows industry standards and procedures on proper encryption for data in transit, data at rest, and key management.
- Data Encryption:
    - Encrypts data in transport using strongest ciphers supported by endpoint / client and the service provided to Data Exporter.
    - Implements encryption algorithms according to industry best practices.
    - Reliably manages encryption keys.
    - Encrypts data at rest (including data backups from operational systems).

Physical and Environmental Security

- Establishes procedures to classify physical areas and their security requirements.
- Requires physical access controls to protect facilities from unauthorized access and safeguard against environmental hazards. Access to specific areas is restricted based on job function.
- Utilizes video surveillance in key areas within Data Importer's facilities and perimeter.
- Requires employees and resources to always wear provided photo identification badges while in the Data Importer's facilities.

- Requires visitors to follow Data Importer's visitor management processes which mandate visitor badges be worn and to be always escorted by authorized personnel.

Operations Security
- Establishes security requirements and operating procedures for protecting information resources, which includes change management, anti-malware, vulnerability management, log management, backup and recovery, and audit controls.
- Requires logging and monitoring of user and service activity.
- Engages third parties to conduct independent security testing of systems to validate efficacy of internal security processes and tools.

Communications Security
- Establishes security requirements and operating procedures for Data Importer's networks which includes network segregation, network intrusion detection, and network threat protection systems.

System Acquisition, Development and Maintenance
- Establishes security requirements and operating procedures for the acquisition, development, deployment, and support of technology solutions.

Supplier Relationships
- Establishes security requirements and operating procedures to conduct due diligence to evaluate information security and privacy practices of vendors deemed critical for Product delivery.
- Manage vendors to ensure the agreed-upon level of information security and service delivery is maintained.

Information Security Incident Response
- Maintains security incident response processes to detect, remediate, and inform relevant internal and external stakeholders of security incidents resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Information Security Aspects of Business Continuity Management
- Develops and maintains business continuity plans for critical business operations and is exercised annually.
- Resiliency is designed into critical service components to ensure minimal impairment during any failure events or maintenance activities. Disaster recovery testing is done at least annually using a combination of walkthroughs, simulations, and production testing.

Compliance
- Ensures Data Importer's compliance to internal policies and procedures, contractual obligations and applicable privacy, information security, and data protection laws and regulations.
- Regularly conducts internal and third-party audits of products and services against industry standard security frameworks.

Organizational Measures
- Information Security Practices Based on International Standards
  - Maintains information security and privacy polices based on ISO standards and international best practices.
  - Maintains industry standard certifications and regularly audits its practices.
- Transparency
  - Provides descriptions of Personal Data collected by the Products in Data Importer's Privacy Notice.
- Data Minimization
  - Conducts security and privacy reviews of products and services during software development.
  - Data collected and processed is accessible only to authorized personnel.