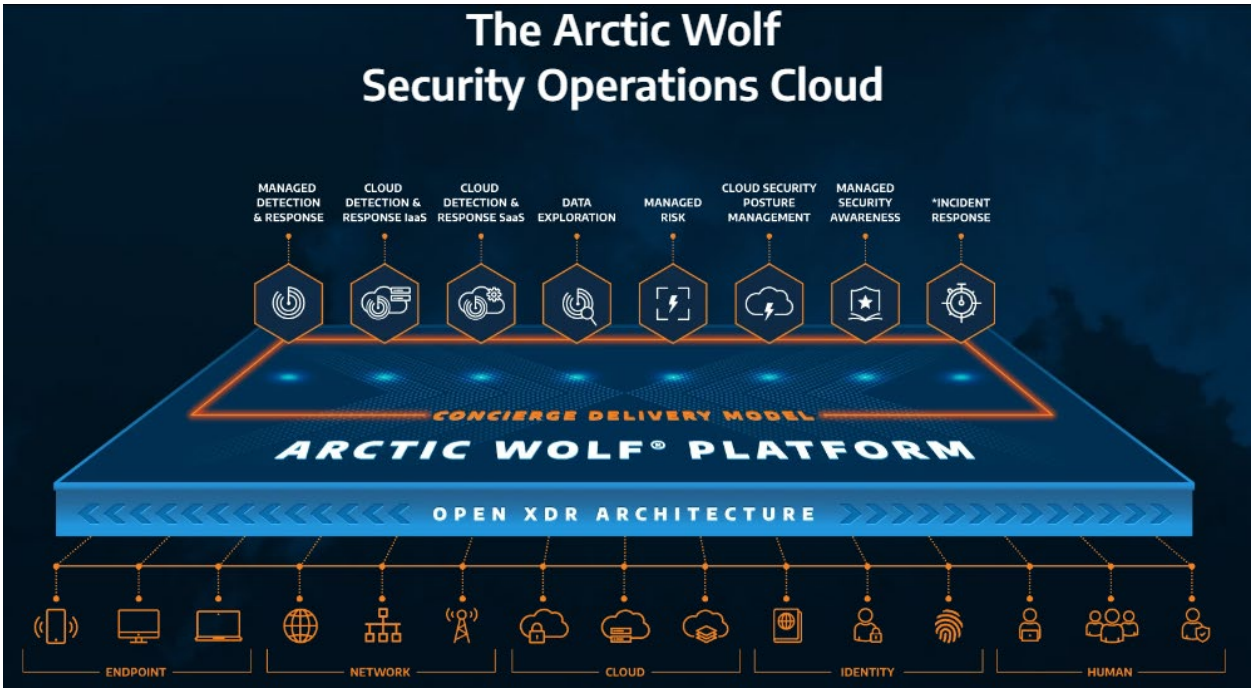
NCSA Technology Procurement 2023-2024
Effective March 16, 2023 – March 15, 2024

ARCTIC WOLF NETWORKS, INC

CYBER SECURITY SOLUTIONS: CATALOG OFFERING

6% Discount off MSRP for Main Line Items

The Platform SKU will be charged annually based on a fixed fee plus "Users" and "Servers" in the organization. The SKU will be a list price of $15,000 fixed fee plus $15 USD per user and/or server per year.



Arctic Wolf Platform

What is included in the Arctic Wolf Platform?
Evolution and advancements to the platform are required to ensure that it meets the challenge of more sophisticated threats and scales to meet the volume of threats our customers experience. Today, the Arctic Wolf Platform processes over 1.6T events and 1.3PB of data per week.

For quotes or more information, contact:
Paula Sauls, Account Manager – Paula.Sauls@ProLogicITS.com
Tony Bailey, Government Manager – Tony.Bailey@ProLogicITS.com

106 Northpoint Parkway, Bldg. 2, Ste 350 I Acworth, GA 30102 Toll Free 866-923-0513 I www.ProLogicITS.com

Enhancements include:
• Added integration support for Palo Alto Wildfire, Microsoft 365 Security and Compliance Center, Azure AD Identity Protection, Infoblox, Proofpoint TAP, Microsoft MCAS, Zscaler ZIA, and migrated multiple existing integrations to API based ingestion
• Our Platform acts as a system of record for high profile security events (such as SolarWinds) and helps customers remediate and recover from advanced threats

What entitlements are included in the Platform SKU?
• Unlimited data ingestion
• Access to AW Portal
• Access to AW Reporting
• Use of AW Agent
• Data Retention with 90 day default for MDR
• Inclusion of $0 virtual series 100 Sensor SKU

Why does Arctic Wolf include a Base Platform SKU?
The Arctic Wolf Platform recognizes the unique value of collecting security data in real time and enriching and analyzing it to drive key security operation outcomes. It ensures that customers have a foundation of relevant data to act as a system of record in driving security outcomes.

Arctic Wolf is broadening and enriching the security operations solutions and outcomes we deliver, and the platform offering enables us to continue to deliver new solutions. This SKU allows us to tailor a solution to a customer's unique business processes and needs, while ensuring they can work with the existing tools in which they are familiar with and have invested.

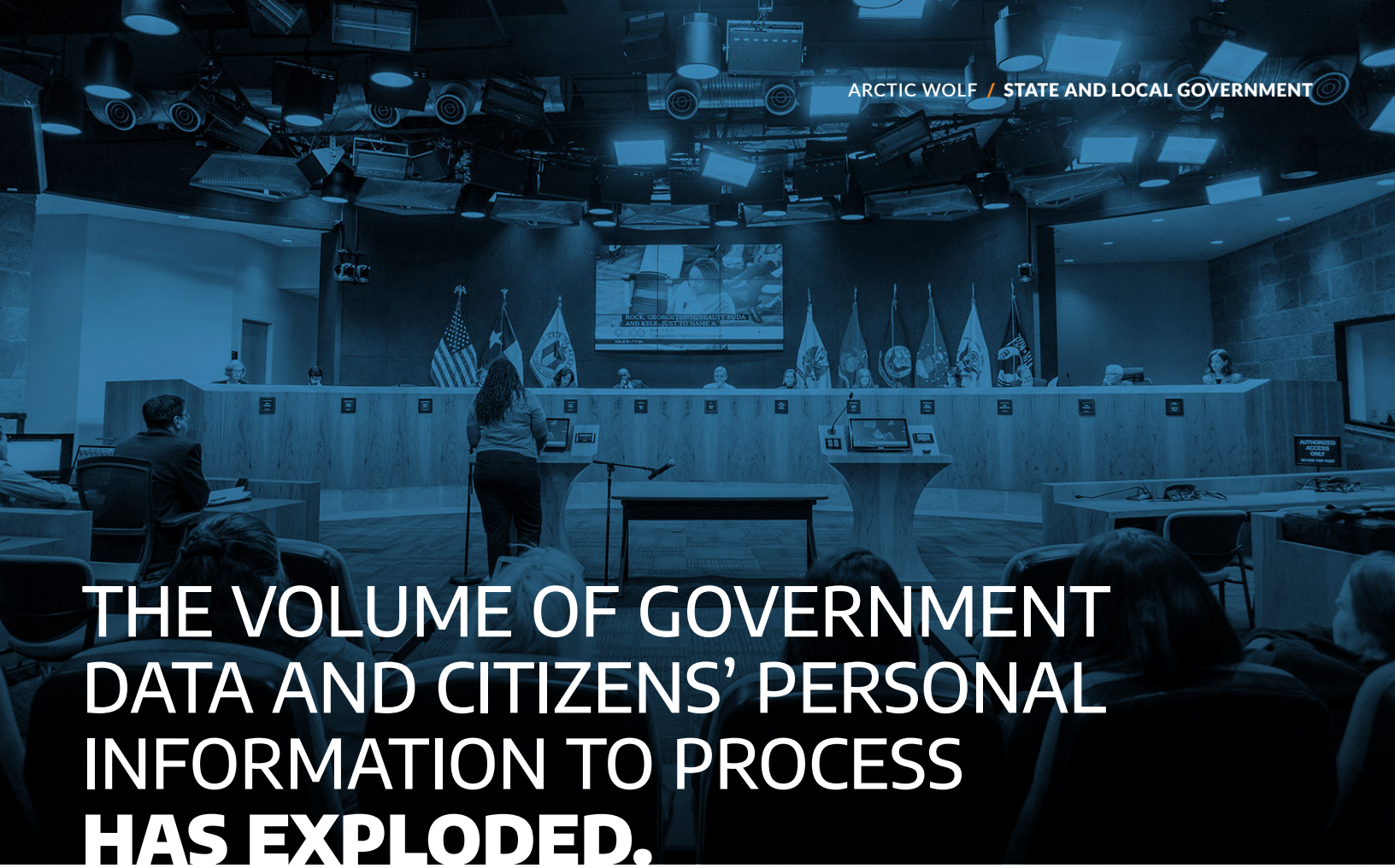
- MSRP prices are subject to change
- Multi-year subscriptions are available, but may be subject to price increase
- Please review Arctic Wolf purchase terms at this link: https://arcticwolf.com/terms/msa/

For quotes or more information, contact:
Paula Sauls, Account Manager – Paula.Sauls@ProLogicITS.com
Tony Bailey, Government Manager – Tony.Bailey@ProLogicITS.com

106 Northpoint Parkway, Bldg. 2, Ste 350 I Acworth, GA 30102 Toll Free 866-923-0513 I www.ProLogicITS.com

ARCTIC WOLF

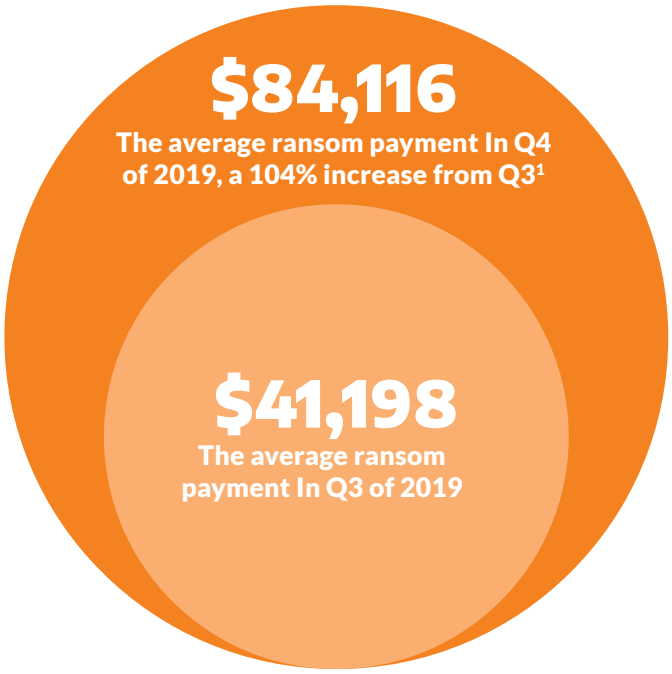
The State and Local Govenment Cybersecurity Checklist



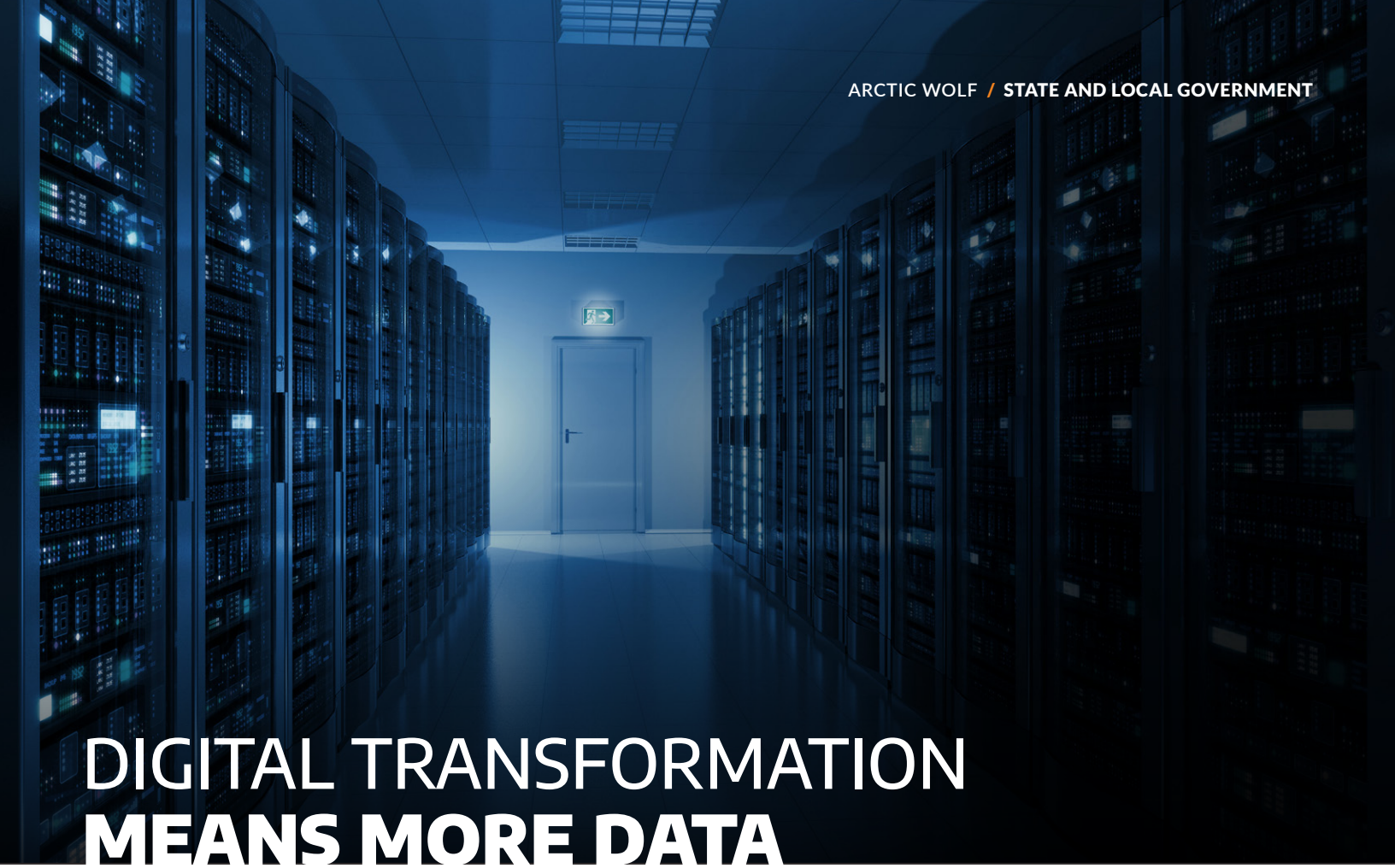
THE VOLUME OF GOVERNMENT DATA AND CITIZENS' PERSONAL INFORMATION TO PROCESS **HAS EXPLODED.**

Cybersecurity has become a top priority for state and local governments. The volume of government data and citizens' personal information to process has exploded, which makes it more challenging than ever to keep this data secure.

Adding to the challenge, cyberattacks against state and local governments have increased dramatically. In 2019 alone, there were over 100 ransomware attacks on public, state, and local governments, according to the threat intelligence firm Recorded Future.



—Coveware[1]



DIGITAL TRANSFORMATION **MEANS MORE DATA**

As citizens have embraced digital transformation in other aspects of their lives, they have begun to demand it too from public services. Government agencies have responded by digitizing access to services and information at a rapid pace, but IT teams at these public entities must often make do with tight budgets and limited personnel.

Yet, state government and local municipalities are the guardians of highly sensitive personal data that cybercriminals can steal, expose, or hold to ransom. They also control vital infrastructure, including first responder networks and school and welfare systems, that needs protection from malicious threats.

That's why a robust and comprehensive strategy is necessary to protect these systems that citizens rely on for important—and sometimes critical information.

Use this checklist to develop your cybersecurity strategy, step-by-step:

TO EFFECTIVELY PROTECT DATA AND DEVICES, YOU HAVE TO **KNOW WHAT YOU'RE PROTECTING.**

Create a Security-Conscious Workforce

Many employees use shortcuts that help them work more efficiently. However, these shortcuts—such as reusing the same password for different programs or sharing passwords with colleagues—often compromise cybersecurity. The best way to tackle this issue is to create a culture of security at work, supported by training programs and resources.

- **Implement an ongoing schedule of training and education** for all workers. Include updates on known attacks and information about best-in-class security procedures, such as two-factor authentication and password managers.
- **Monitor IT processes for complexity.** Keep ease-of-use in mind whenever you update or alter processes to avoid users turning to insecure shortcuts.
- **Implement data usage controls** that can block unsafe actions like uploading data to the web, sending emails to unauthorized addresses, or copying to external drives.
- **Establish a password policy** that requires regular password changes, using strong passwords, and never writing them down.

Inventory and Control Hardware and Software Assets

Employees in the public sector, as in other industries, like to have the latest gadgets and access business networks on a range of devices. They also download tools they think will prove useful, even if they aren't on the list of approved software for use on company devices. To effectively protect data and devices, you have to know what you're protecting.

- **Document and secure all devices that could access the network,** including personal devices.
- **Use inventory tools to keep up-to-date records** of existing software and hardware. Block unknown executable files, and automatically install software updates and security patches on all computers.
- **Quickly disconnect any detected unauthorized devices** from the network, as well as devices that run potentially dangerous software.

Create Privileged Access to Critical Assets

It is imperative to know what information needs to be protected. Resources should focus on safeguarding data that is sensitive or critical to continuity. Map and identify the data and systems you need to protect, and then ensure that only a privileged few have access.

- **Restrict access to data and applications** to only those users who need the information to perform their job. Follow the same protocol for physical access.
- **Oversee all user access to the network**, record authentication errors and unauthorized access, and sweep the network for unusual activity.
- **Restrict administrative privileges** and carefully manage the employees who can access the most sensitive data.

Build an Understanding of the Threat Landscape

State and local governments face the complex task of defending their networks due to the variety of services they offer. Understanding the threats they face is critical to establishing and maintaining a secure network.

- **Regularly consult reliable and well-informed threat intelligence** to understand potential threats.
- **Prioritize your budget** to align with current threats and provide an effective means of response.
- **Take part in information sharing** to jointly shield networks and data. Information sharing and analysis centers, or ISACs, have been developed in both the public and private sectors. These organizations provide a secure environment where you can share information on the latest threats and best practices.

Continuously Analyze, Prioritize, and Manage Vulnerabilities

Your IT team, whether in-house or outsourced, must have 24x7 real-time cybersecurity operations that can manage vulnerabilities, monitor and detect threats, and respond to malicious and risky activity in real time.

- **Identify vulnerabilities and prioritize** what needs patching. A risk-based approach to vulnerability management enables government agencies to eliminate vulnerabilities in a methodical fashion, starting with the most severe risks.
- **Have a detailed response plan in place,** not only to prevent breaches but to respond to cyber incidents as they happen.

A 2020 attack on New Orleans cost the city

OVER $7 MILLION.[2]

Maintain, Monitor, and Analyze Audit Logs

Without audit logs, attacks may go unnoticed and uninvestigated. That leaves the door open to additional attacks and untold potential damages. Most IT teams keep audit records for compliance purposes, but attackers know there are many state and local government agencies that lack the time or resources to review logs on a regular basis. This provides an ample window of time to access systems and data undetected.

- **Log, monitor, and analyze security risks.** Record and examine log activity and analyze the resulting log information.
- **Continuously monitor** networks and systems for security threats to ensure you have an audit trail when an incident occurs.
- **Perform regular risk assessments** to identify weak points in the system.
- **Be ready to report.** Use managed vulnerability assessment services to gain an understanding of your organization's IT security posture and risk profile.

Back Up Data Offsite

The fastest-growing threat facing state and local government is ransomware attacks. In these hacks, data is stolen by cybercriminals and only returned upon payment of a ransom. Criminals will also steal data or code that is critical to the running of services. A second cache of this data is essential to ensure continuity of services. It also enables data recovery in the event of a natural disaster or system failure.

- **Maintain a current, flexible, secure, and speedy process to access data at all times.** Government agencies need a recovery solution that allows them to recover data and bring applications back online as seamlessly as possible.
- **Consider cloud and physical backup solutions** and develop a backup schedule that takes the frequency of data change into account.

To recover from a $52,000 ransomware attack, Atlanta spent

OVER $2.6 MILLION.[3]

STAY ON TOP OF COMPLIANCE AND **NEW LEGISLATION**

In 2019, nearly 300 bills or resolutions were considered or introduced that dealt significantly with cybersecurity. That number continues to grow. State and local government cybersecurity is a fast-evolving sector and subject to data and privacy regulations. Compliance with data protection is a key concern, but government agencies must also keep up to date with all relevant information—which is often beyond their capacity. Here are a few recent cybersecurity laws enacted at a state level.

Colorado

Statutory Citation:
C.R.S. §§ 24-37.5-403, -404, -404.5, -405

Applies to Government:
Public agencies, institutions of higher education, General Assembly

Statutory Summary/Excerpt:
Requires the chief information security officer to:

(a) Develop and update information security policies, standards, and guidelines for public agencies;

(b) Promulgate rules pursuant to article 4 of this title containing information security policies, standards, and guidelines;

(c) Ensure the incorporation of and compliance with information security policies, standards, and guidelines in the information security plans developed by public agencies pursuant to section 24-37.5-404;

(d) Direct information security audits and assessments in public agencies in order to ensure program compliance and adjustments. Establishes the Colorado Cybersecurity Council and provides for coordination of missions related to homeland security and cybersecurity.

Requires public agencies and institutions of higher education to develop an information security plan utilizing the information security policies, standards, and guidelines developed by the chief information security officer. Provides for an information security plan for communication and information resources that support the operations and assets of the general assembly.

Encourages the CISO to assess the data systems of each public agency for the benefits and costs of adopting and applying distributed ledger technologies such as blockchains.

Maryland

Statutory Citation:
Md. State Govt. Code §§ 10-1301, -1304

Applies to Government:
An executive agency, a department, a board, a commission, an authority, a public institution of higher education, a unit or an instrumentality of the State; or a county, municipality, bi–county, regional, or multicounty agency, county board of education, public corporation or authority, or any other political subdivision of the State.

Statutory Summary/Excerpt:
Implement and maintain a written information security policy and reasonable security procedures and practices that are appropriate to the nature of the personal information collected and the nature of the unit and its operations.

Require, by written contract or agreement, that third parties implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information disclosed to the nonaffiliated third party.

Oregon

Statutory Citation:
ORS § 182.122, 2016 Ore. Laws Chap. 110

Applies to Government:
State agencies

Statutory Summary/Excerpt:
Provides for the Oregon Department of Administrative Services, in its sole discretion, to:

(a) Review and verify the security of information systems operated by or on behalf of agencies;

(b) Monitor state network traffic to identify and react to security threats; and

(c) Conduct vulnerability assessments of agency information systems for the purpose of evaluating and responding to the susceptibility of information systems to attack, disruption or any other event that threatens the availability, integrity or confidentiality of information systems or the information stored in information systems.

Oklahoma

Statutory Citation:
62 Okl. St. § 34.32

Applies to Government:
Each state agency that has an information technology system.

Statutory Summary/Excerpt:
Conduct an annual information security risk assessment to identify vulnerabilities associated with the information system. The final information security risk assessment report shall identify, prioritize, and document information security vulnerabilities for each of the state agencies assessed. Failure to comply with the requirements of this subsection may result in funding being withheld from the agency.

State agencies shall use either the standard security risk assessment created by the Information Services Division or a third-party risk assessment meeting the ISO/IEC 17799 standards and using the National Institute of Standards and Technology Special Publication 800-30 (NIST SP800-30) process and approved by the Information Services Division.

IRS Publication 1075

Mandates government adherence to certain cybersecurity and physical security controls for the protection of federal tax information.

Payment Card Industry Data Security Standard (PCI DSS)

Requires strong access control measures and other security to protect cardholder data.

Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH)

Applies where state and local governments process protected health information. This requirement has become more important with the expansion of Medicare and Medicaid.

TAKE THE NEXT STEP TO **BETTER SECURITY**

Cybersecurity is an essential part of state and local government's work to digitize services and improve productivity at lower cost. Modernization and digital transformation cannot be effective unless they are accompanied by cyber resilience and strong security protocols.

Discover how Arctic Wolf® helps bolster your agency's or organization's security strategy in the most comprehensive, secure, and affordable way possible.

Contact us today to schedule a demo.

ABOUT ARCTIC WOLF

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. For more information about Arctic Wolf, visit arcticwolf.com

1. https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate
2. https://www.scmagazine.com/home/security-news/ransomware/ransomware-attack-cost-new-orleans-7-million-and-counting/
3. https://www.csoonline.com/article/3391589/why-local-governments-are-a-hot-target-for-cyberattacks.html

ARCTIC WOLF

SOC2 Type II Certified

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

Contact Us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com