Security Services Catalog

Abstract

The Kansas Information Security Office was established to provide information security services to state organizations. The purpose of these security services is to ensure the confidentiality, integrity and availability of citizen services and the information with which the state is entrusted. Contained in this catalog are the services available to all state organizations from the KISO.

Rod Blunt, Chief Information Security Officer
KISO@ks.gov

This page intentionally left blank

The Kansas Information Security Office (KISO) was established by the Kansas Cybersecurity Act (KCA) in 2018. The organization's mission is to maintain a secure information network that facilitates the business of the State of Kansas, protects privacy, and reduces risk, all while promoting innovation, economic growth, and transparency.

The KISO is able to successfully fulfill this mission by providing a suite of readily available cybersecurity services to the State of Kansas' executive branch agencies, boards and commissions.

The KISO provides services in two categories: Enterprise Security Services (ESS) and Managed Security Services (MSS).

Enterprise Security Services (ESS) are included for all KANWIN network customers through the network connect rate. In FY20, ESS will be included with the Cybersecurity Rate. ESS provide multiple technology-based cybersecurity solutions designed to mitigate risk for state businesses in an effective, efficient and layered approach. All ESS solutions are implemented by an experienced staff of Information Security Professionals. Some ESS require enrollment through the KISO.

Managed Security Services (MSS) are comprised of two distinct activities: Information Security Officer (ISO) services and Technical Security Services (TSS). Although these services can be procured separately, together they provide a holistic approach to developing and maintaining an effective and efficient information security program.

- **Technical Security Services (TSS)** are those customized technical services required to secure organization-specific network, applications and systems. Also available are custom reporting and metrics. These services are priced according to the needs and size of the organization and are billed through a negotiated Service Level Agreement (SLA).
- **Information Security Officer Services (ISO)** focus on the buildout, implementation and management of a business's information security program, including training, policies, procedures and compliance. These services are priced according to the needs and size of the organization and are billed through a negotiated Service Level Agreement (SLA).

To enroll in available ESS, or to inquire about any other security services, please contact the KISO at (785) 296-0814 or kiso@ks.gov.

This page intentionally left blank

Enterprise Security Services (ESS)

All ESS are included in Network Connect Rates

** Indicates enrollment with KISO required*

1. ***Cybersecurity Awareness Training.*** The KISO provides a robust cybersecurity training solution that meets all statutory requirements for annual cybersecurity training. In addition, this solution can be customized to include additional training modules required by your organization. In addition, this solution provides email campaign tools to evaluate staff awareness of common phishing tactics and reports that identify specific areas of focus for additional training.
2. ***External Cybersecurity Scoring.*** The cybersecurity scoring solution generates objective, quantitative measurements on an organization's security performance to produce daily security ratings ranging from 250 to 900.This solution analyzes existing security incidents and practices and applies sophisticated algorithms to produce these ratings, which are based on externally observable, non-intrusive data and methods.
3. **Cyber Hygiene Scoring.** This service is provided by the Department of Homeland Security. This external vulnerability scanning service helps secure your internet-facing systems from weak configuration and known vulnerabilities and encourages the adoption of modern security best practices. DHS performs regular network and vulnerability scans and delivers a weekly report. This service is mostly automated and requires little direct interaction. Organizations interested in their specific reports should contact the KISO.
4. **Internet Firewall Administration**. The Internet firewalls implemented by the KISO are specifically configured to be the first layer of defense against unauthorized access to state computing assets. They act as a barrier to filter data between state systems and the Internet. They also work as a filter to block the incoming and outgoing traffic on the network that may be suspicious and unsafe. The KISO is responsible for the operation, maintenance and monitoring of these security controls.
5. **Internet Intrusion Prevention.** Like the Internet firewalls, the Internet Intrusion Prevention Systems (IPS) are another layer of protection deployed at the Internet border. In addition to raising an alarm, IPS can also configure rules, policies and required actions. Upon capturing these alarms, IPS can:
    a. Monitor and evaluate threats, catch intruders and act in real time to thwart such instances that firewall or antivirus software may miss.
    b. Prevent Denial of Service (DoS) attacks.
    c. Maintain the privacy of users as IPS records the network activity only when it finds an activity that matches the list of known malicious activities.
    d. Stop attacks on the SSL protocol or prevent attempts to find open ports on specific hosts.
    e. Detect and foil OS fingerprinting attempts that hackers use to find out the OS of the target system to launch specific exploits.
6. **Website Filtering.** Website Filtering is an innovative feature that screens webpages to determine whether some, or all of it, should be blocked. The website filtering solution scans websites that are likely to include

undesirable advertising, explicit content, spyware, viruses, and other malicious forms of content. With website filtering protecting your Internet activities, you can experience safer online surfing.

7. **Application Filtering**. Very similar to website filtering, the Application Filter can detect and block applications like Facebook, Netflix, Snapchat, and many others. The application filter uses deep packet inspection (DPI) and SSL certificate analysis to categorize and block dozens of applications and websites.
8. **24x7 Internet Security Monitoring.** Through a partnership with the Multistate Information Sharing and Analysis Center (MS-ISAC), the MS-ISAC Security Operations Center monitors the state's Internet border network traffic for malicious activity. This service alerts the KISO to suspicious or malicious events for further investigation.
9. ***Website Certificates.*** Website certificates provide authentication for a website and enables an encrypted connection. These certificates communicate to the client that the web service host demonstrated ownership of the domain to the certificate authority at the time of certificate issuance. This authentication process is much like sealing a letter in an envelope before sending it through the mail. By ensuring that all data passed between the two parties remains private and secure, encryption can help prevent hackers from stealing private information such as credit card numbers, bank information, names, and addresses.
10. ***Intelligent Central Logging.*** From a security point of view, the purpose of intelligent logging is to record specific actions that can then be analyzed by to identify suspicious activity. However, given the large amount of log data generated by information systems and the logs of their supporting infrastructure, a solution that provides the ability to quickly search through large amounts of data for threats and malicious behavior is critical and this solution provides that capability.
11. ***Application Firewalls.*** A Web Application Firewall (WAF) is a filter that sits in front of business-specific applications inspecting incoming traffic for potential threats and malicious activity. It is one of the most common means of protecting against attacks at the application layer. The common threats that this solution works to prevent are Denial of Service (DoS), code injection, website defacement and many more.
12. ***Load Balancing*.** Load balancing is used to distribute workloads uniformly across servers or other compute resources to optimize network efficiency, reliability and capacity. Load balancing is performed by an appliance -- either physical or virtual -- that identifies in real time which server in a pool can best meet a given client request, while ensuring heavy network traffic doesn't unduly overwhelm a single server. In addition to maximizing network capacity and performance, load balancing provides failover. If one server fails, a load balancer immediately redirects its workloads to a backup server, thus mitigating the impact on end users.
13. ***Host and Application Vulnerability Scanning.*** Vulnerability scanning is an inspection of the potential points of exploit on a computer network or application, to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks and applications and predicts the effectiveness of countermeasures. Organizations should scan computers, networks and applications for any vulnerabilities on a regular basis.
14. ***Secure Virtual Access for Vendors and Contractors.** This privileged remote access solution provides a secure remote connection for vendors or contractors to organizational information assets. The solution

provides many features, including multifactor authentication, session recording, cut and paste prevention, and many more.

15. **Continuous Monitoring.** Through all the ESS services and controls, the KISO is constantly monitoring, analyzing and responding to threats. Through collaboration with other states, other industries and our federal partners, the KISO is constantly adjusting to prevent or mitigate cybersecurity risk.
16. **Advanced Email Filtering (Summer 2019).** More than 90% of targeted attacks start with email, and these security threats are always evolving. Advanced Email Protection provides multiple layers of additional security to stop malware and non-malware threats, such as email fraud. It can detect and block threats and prevent confidential information from getting into the wrong hands. This service will automatically be provided for all organizations enrolled in the OITS O365 email solution.
17. ***Behavioral Analytics (Summer 2019).*** User Behavior Analytics (UBA) is a set of algorithms that analyze log activity to spot abnormal behavior, such as repeated login attempts from a single IP address or large file downloads. Buried in gigabytes of data, these patterns are easy for humans to miss. UBA can help security teams combat insider threats, brute-force attacks, account takeovers and data loss. Organizations interested in this service must also participate in the central logging solution mentioned in item 10.
18. ***Security Information and Event Management (SIEM) (Summer 2019).*** SIEMs provide real-time analysis of security alerts generated by applications and network hardware. SIEM has become a core security component of modern organizations. The main reason is that every user or tracker leaves behind a virtual trail in a network's log data. SIEM systems are designed to use this log data to generate insight into past attacks and events. A SIEM system not only identifies that an attack has happened but allows you to see how and why it happened. The use of SIEM also helps companies to comply with a variety of industry cyber management regulations. Combined with the Intelligent Logging solution, SIEM systems provide the best way to meet this regulatory requirement and provide the transparency over logs in order to generate clear insights and improvements.

Managed Security Services (MSS)

All MSS are provisioned through negotiated Service Level Agreements

** Indicates enrollment with KISO required*

ISO Services

1. **Security Policy Development and Maintenance.** This service provides the agency with policies that are industry standard, and compliant with applicable State and Federal requirements.
2. **Risk Management.** An Information Security Risk Assessment provides an objective, evaluation of the organization's current environment. This analysis provides an estimate of the likelihood that unacceptable impacts to customer information systems, employees, customers, reputation, assets and interests of stakeholders will occur. This service will provide the Customer with reports on risk to information technology assets and information systems.
3. **Compliance Management.** This service ensures the customer is informed of information technology assets and information systems that are compliant and non-compliant with State and Federal policies and regulations. This service also identifies what is required to bring noncompliance issues into compliance.
4. **Disaster Recovery and Business Continuity Planning.** Disaster Recovery (DR) is the process an organization uses to recover access to their software, data, and/or hardware that are needed to resume the performance of normal, critical business functions after an event of either a natural disaster or a disaster caused by humans. Business Continuity Planning (BCP) is the way an organization can prepare for and aid in disaster recovery. It is an arrangement agreed upon in advance by management and key personnel for the steps that will be taken to help the organization recover should a disaster occur. The KISO assists in developing and maintaining DR and BCP plans for information technology in support of critical business functions identified by the customer.
5. **Incident Response.** Incident management and response identifies and responds to unexpected disruptive events with the objective of controlling impacts within acceptable levels. These events can be technical, such as attacks mounted on the network via viruses, Denial of Service (DoS) or system intrusion, or they can be the result of mistakes, accidents, or system or process failure. Disruptions can also be caused by a variety of physical events such as theft of proprietary information, social engineering, lost or stolen backup tapes or laptops, environmental conditions such as floods, fires, or earthquakes. Any type of incident that can significantly affect the organization's ability to operate, or that may cause damage, must be considered by the Information Security Officer as part of the incident management and response process. This service facilitates in the development and execution of incident response.
6. **Continuous Monitoring.** Continuous monitoring is the process and technology used to detect compliance and risk issues associated with an organization's operational environment. The operational environment consists of people, processes, and systems working together to support efficient and effective operations. Controls are put in place to address risks within these components. Through continuous monitoring of the operations and controls, weak or poorly designed or implemented controls can be corrected or replaced to enhance the organization's operational risk profile. Continuous monitoring typically includes solutions that address three operational disciplines known as Continuous Audit, Continuous Controls Monitoring

and Continuous Transaction Inspection. For this service, these disciplines are monitored by collecting, correlating and alerting when certain conditions exist. Summary reports of security incidents or events of notable interest are brought to the attention of the Customer.

7. **Information Security Consulting.** Information security consulting is to assist the agency in making informed decisions regarding the confidentiality, integrity, and availability of its data. Information Security Officers can provide consulting services on a variety of topics to include but not limited to procurement process (RFPs), third party and contract management, system and software development lifecycles, security control implementation and guidance, configuration management recommendations, data classification, and data sharing agreements.

TSS Services

8. ***Vulnerability Scanning*.** Provides routine vulnerability scans and provides reports and remedies to Customer technology staff and management. This service also provides high-level repeating vulnerabilities and trend reports to senior management.
9. ***Virtual Private Networking (VPN).*** A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the Internet. VPN technology was developed as a way to allow remote users and branch offices to securely access organizational applications and other resources. To ensure safety, data travels through secure tunnels, and VPN users must use authentication methods -- including passwords, tokens or other unique identification procedures -- to gain access to the VPN server. VPNs are used by remote workers who need access to organizational resources, consumers who may want to download files and business travelers who may want to log into sites that are geographically restricted. VPN services are critical conduits through which data can be transported safely and securely.
10. ***Managed Firewall Services*.** In support of organization objectives and business functions, the KISO will provide a fully managed and proactive firewall management solution where the KISO is solely responsible for the administration, management, and monitoring of the firewall platform's configuration, security policy, and rule-set. The KISO has dedicated staff that will work with authorized departmental contacts to review, validate, implement, monitor, and audit firewall requests and/or changes as needed.
11. ***Managed Intrusion Detection and Prevention*.** This service is a comprehensive, 24x7x365 managed service incorporating industry best practices and a team of security experts. IDS/IPS devices record security relevant events from networks. With IDS/IPS devices deployed, the customer can expect prompt notification of possible security breaches, intrusions (attacks from outside the organization), and misuse (attacks from within the organization). The service also reduces the impact of attacks and malicious activity by carrying out detailed analysis and taking swift remedial action against the problem.
12. ***Log Management and Continuous Monitoring*.** Log Management and Continuous monitoring typically includes solutions that address three operational disciplines known as Continuous Audit, Continuous Controls Monitoring and Continuous Transaction Inspection. For this service, these disciplines shall be monitored by collecting, correlating and alerting when certain conditions exist, and depending upon the severity, the KISO and the Customer will respond as defined in accompanying documents to the customer's TSS Agreement. Summary reports of security incidents and/or events of notable interest shall be brought to the attention of the Customer.