SECURITY REQUIREMENTS FOR PURCHASE STANDARD

Effective date: 4/19/2022
Document number: ITS-SST-006

1.0 PURPOSE

The purpose of this document is to define the standard strategy and requirements implemented by the Department of Information Technology Services (DoITS) for purchasing software and services for the County. Deviations from this document should be discussed with the Cybersecurity Division before moving forward with a purchase.

Overview:

To protect the County's technology infrastructure, the Department of Information Technology Services (DoITS) has implemented this Security Requirements for Purchase standard. Because a successful attack and access to such sensitive information data could be detrimental to County associates and put the County at high legal or financial risk, this standard has been implemented to ensure secure practices and requirements for purchasing software solutions, software services, and contract services for the County.

This document outlines the strategy for cloud-based services, on-premises services, and vendor contracts.

2.0 SCOPE

This standard applies to purchases of software, hardware, and services that:

- Connect to the County network
- Are installed on County-owned IT assets
- Store County-owned data

The standard applies to these assets, regardless of the amount of support provided by the Department of Information Technology Services (DoITS).

3.0 STANDARD

This standard is divided into sections. A single purchase may qualify for multiple sections. For example, a cloud service dealing with sensitive data needs to meet requirements under both sections: *3.1 Cloud Services* and *3.3 Contracts*.

Note that requirements that use the term ***should*** are more flexible and should be discussed with the Cybersecurity division before deviation. Requirements that use the term ***must*** are not considered optional.

3.1 Cloud services

1. All cloud services
    a. Should utilize Active Directory for authentication and be compatible with the County's Multi-Factor Authentication (MFA) solution.
    b. Should log detailed audit events and make these logs continuously available for ingestion by a security information and event management system (SIEM) without the need to manually download or transfer data.

2. Cloud-based services that store sensitive data as defined by Georgia law, data related to law enforcement investigations or court cases, data regulated by CJIS, HIPAA, or PCI *in addition to* the requirements established by those regulations and those stated above for all cloud services:
    a. All County-owned data must be stored within the United States.
    b. Vendors that are storing data must provide a SOC 2 Type 2 report with an Unqualified opinion.
    c. Must comply with requirement 1a above relating to authentication.
    d. Must comply with requirement 1b above relating to audit-event logging.

3.2 On-premise solutions (Windows)

1. All On-premise solutions
    a. Must be capable of performing on systems with the County ITS-approved anti-virus solution with minimal exceptions. Heuristic scanning must be enabled.
    b. Must be capable of performing on systems with the ITS-approved vulnerability scanning agent installed and configured for a weekly scan.
    c. Must be architected in such a way that security updates can be applied while still meeting customer department expectations for availability.
    d. Should log detailed audit events and make these logs continuously available for ingestion by a SIEM without the need to manually download or transfer data.
    e. Internal applications should utilize Active Directory for authentication.
    f. Public/Internet-facing applications must utilize Active Directory for authentication and be compatible with the County's Multi-Factor Authentication solution. This requirement is not intended to apply to logins by County residents.
    g. Must be compatible with currently supported versions of Microsoft Windows Server, with a minimum version of n-1 from latest.

2. On-premises solutions that store sensitive data as defined by Georgia law, data related to law enforcement investigations or court cases, data regulated by CJIS, HIPAA, or PCI *in addition to* the requirements established by those regulations and those stated above:
    a. Must comply with requirement 1d above relating to audit-event logging.
    b. Must comply with requirement 1f above relating to Active Directory and MFA.
    c. Should ideally be compatible with the County's data loss prevention solution to identify and classify data.
    d. Must be compatible with the County's data encryption solution.

3.3 Contracts

1. All contracts should address the following points. Requirements must apply to Vendors and any Subcontractors.
    a. Vendor must notify Gwinnett County within 24 hours in writing if they or a Subcontractor experience a security breach that involves:
        i. County-owned data, accounts, or systems
        ii. Systems that are compromised while they are connected to the County network, including over VPN, regardless of ownership
        iii. Any other circumstance that can reasonably be expected to negatively impact the County's security posture
    b. Vendor may not provide County-owned data to any third parties unless explicitly authorized. This includes network diagrams and system information.
    c. Unless it would violate other legal requirements or is otherwise authorized, Vendor should delete County-owned data at the termination of the agreement.
    d. Vendor must promptly report observed security vulnerabilities to the County IT department.
    e. Vendor must perform background checks on any employees that access sensitive County data and must be willing to produce evidence as such if requested. Sensitive data refers to PII as defined by Georgia law, any data regulated by PCI, HIPAA, CJIS, or any other legal requirements.
    f. Any required support from the Vendor should match the expectations placed on ITS. For example, applications that are expected to be available 24/7 should have 24/7 support.

2. Contracts that include services where the Vendor accesses County-owned systems including the VPN should address the following conditions:
    a. Any changes to County-owned systems must be done in accordance with the DoITS change management policy.
    b. Vendor must agree to turn over any relevant passwords on request. This requirement is for shared resources and accounts, and not individual users.

Examples: password-protected documents; administrator accounts not tied to a specific user or service accounts

c. Vendor must agree to accept as-is all applicable County policies.

d. Any systems used to perform services for the County must run an operating system currently supported by the Vendor, have all security patches installed, and Windows systems must run anti-virus software.

e. Connections to the County VPN require the use of Multi-Factor Authentication.

f. The County provided VPN solution is the only approved method for remotely accessing the County network.

g. For personnel with access to County resources, the County should be notified in advance of employee terminations or reassignment so that access can be terminated. Notification must be made within 24 hours for unplanned changes.

h. Vendor must respond to requests by the County to validate user access lists within ten (10) business days.

i. Vendor must not transfer County data to non-County-owned systems unless authorized to do so as part of providing services. Data transferred must be protected according to industry best practices. At a minimum, this includes disk encryption on all portable systems that store County data.

j. Vendor personnel must not delete, disable, or bypass any encryption, anti-virus, or other security software installed on Gwinnett County systems without approval from the Security Operations team.

k. Vendor personnel must execute only applications that pertain to their specific contract work.

l. The County is not liable for any damages to the vendor computer equipment that may occur while installing or using software or hardware connected to any County systems.

m. Vendor personnel may not copy any data and/or software from any County resource for personal use.

n. Vendor personnel are prohibited from intercepting or monitoring network traffic by any means, including the use of network sniffers, unless authorized in writing by the Gwinnett County ITS Department.

3. Contracts that include services where the Vendor accesses sensitive data as defined by Georgia law, data related to law enforcement investigations or court cases, data regulated by CJIS, HIPAA, or PCI *in addition to* the requirements established by those regulations and those stated above:

   a. May only be accessed by individuals in the United States.

4.0 ADDITIONAL REFERENCE AND GUIDANCE

Center for Internet Security (CIS) Controls

5.0 GOVERNANCE

This standard has been defined by the Chief Information Officer of Gwinnett County and the Department of Information Technology Services. The standard is effective immediately upon approval and remains in effect until superseded by another standard or revised as business needs dictate.

This document reflects the intent of the Department of Information Technology Services to implement appropriate security controls. The Department realizes that all controls may not be in place at the time of adoption but strives to bring all in-scope IT assets into compliance as resources permit. This standard must be considered for all new initiatives, and any intentional deviations require a documented exception approved by the Department Director.

5.1 Frequency of the standards review

This standard document and related documents are reviewed and updated (generally every two years) by the DoITS Management team as necessary to ensure that the standard continues to remain appropriate in the light of any relevant changes in technology and/or organizational policies.

6.0 TERMS AND DEFINITIONS

Glossary	
Term or Acronym	**Definition**
Active Directory (AD)	Directory service developed by Microsoft for Windows domain networks.
anti-virus (AV) software	Computer software used to prevent, detect, and remove malware.
audit log	Chronological record of security-relevant activities.
authentication	Act of proving the identity of a computer system user; for example, by entering a username and password.
change management process	A collective term for all approaches to prepare, support, and help individuals, teams, and organizations in making organizational change.
cloud computing	On-demand computing services, such as software development platforms, servers, storage, and software, over the internet, often referred to as the *cloud*.
Criminal Justice Information Services (CJIS) security policy	Federal mandate from the United States Federal Bureau of Investigation (FBI) that defines the minimum standard of security controls required for every individual with access to, or who would operate in support of, criminal justice services and information.
data loss prevention (DLP)	Software that detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while

Glossary	
Term or Acronym	**Definition**
	in use (endpoint actions), in motion (network traffic), and at rest (data storage).
encryption	The process of encoding data to prevent accurate interpretation by all but those for whom the data is intended.
Health Insurance Portability and Accountability Act (HIPAA)	Act that was created primarily to modernize the flow of healthcare information, stipulate how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage.
Multi-Factor Authentication (MFA)	An electronic authentication method in which a device user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.
Payment Card Industry Data Security Standard (PCI-DSS)	A cybersecurity security standard for organizations that handle branded credit cards from the major card schemes.
personally identifiable information (PII)	Any information about an individual that can be used to distinguish or trace an individual's identity, such as name, social security number, date, and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
virtual private network (VPN)	Technology that extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
vulnerability	A weakness within a computer system that may be exploited by a threat source resulting in compromised system data or functionality.

VERSION AND APPROVAL HISTORY					
#	**Reviewed by**	**Review Date**	**Approved By**	**Approval Date**	**Changes**
1.0	Matthew Puckett, CISO / Deputy Director, Cybersecurity	11/4/2020	Dorothy Parks, CIO / Department Director of ITS	11/4/2020	Initial draft
1.1	Matthew Puckett, CISO / Deputy Director, Cybersecurity	4/19/2022	N/A	N/A	Minor edits