Gwinnett Information Technology

Security Requirements for Purchases

Hardcopies are considered to be "Uncontrolled Documents"

Document #: ITS-SST-006
Effective Date: 10/15/2020
Review Date: 11/4/2020
Revision Date: 11/4/2020

Approved By: Dorothy Parks, CIO / Department Director ITS

Reviewed By: Matthew Puckett, Chief Information Security Officer

1.0 OVERVIEW

The purpose of this document is to outline requirements for software and services to ensure that the County's security needs are covered. Deviations from this document should be discussed with Security before moving forward with a purchase.

2.0 SCOPE

This standard applies to purchases of software, hardware and services which will do any of the following:

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

Regardless of the amount of support provided by the Department of Information Technology Services (DoITS)

3.0 STANDARD

This document is broken down into sections and a single purchase may qualify for multiple sections. For example, a cloud service dealing with sensitive data needs to meet requirements in both sections under Cloud Services, and the All Contracts section.

Note that requirements which use the term "should" are more flexible but should be discussed with the Security team before deviation. Requirements that use the term "must" or "shall" are not considered optional.

3.1 Cloud Services

1. All cloud services
    a. Services should utilize Active Directory for authentication and be compatible with the Microsoft Multi-Factor Authentication solution.
    b. The service 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 which 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 which are storing data must provide a SOC 2 Type 2 report with an Unqualified opinion.
c. The requirement 1a above relating to authentication is mandatory.
d. The requirement 1b above relating to audit event logging is mandatory.

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 Microsoft 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-premise solutions which 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. Requirement 1d above relating to audit event logging is mandatory.
    b. Requirement 1f above relating to Active Directory and Microsoft MFA is mandatory.
    c. Should ideally have compatibility with Symantec's Data Loss Prevention solution to identify and classify data.
    d. Must be compatible with the County's data encryption solution (Vormetric).

3.3 Contracts

1. All contracts should address the points below. Requirements shall apply to vendors and any sub-contractors.
    a. Vendors must notify Gwinnett within 24 hours in writing if they or a sub-contractor experience security breaches which involve:
        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 which 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, vendors should delete County owned data at the termination of the agreement.

d. Vendors shall promptly report observed security vulnerabilities to the County IT department.
e. Vendor must perform background checks on any employees that will be accessing sensitive County data and 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 which are expected to be available 24/7 should have 24/7 support.

2. Contracts which include services where the vendor will access 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 / accounts, and not individual users. For example, 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 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 re-assignment so that access can be terminated. Notification must be within 24 hours for unplanned changes.
    h. The vendor must respond to requests by the County to validate user access lists within 10 business days.
    i. Vendor will not transfer County data to non-County owned systems unless authorized to do so are 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 which store County data.
    j. Vendor personnel shall not delete, disable, or bypass any encryption, anti-virus or other security software installed on Gwinnett County systems without approval from the Security team.
    k. Vendor personnel shall 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 IT Department.
3. Contracts which include services where the vendor will access 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.

GOVERNANCE

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