



SECURITY REQUIREMENTS FOR PURCHASE STANDARD

EXHIBIT A VENDOR SECURITY & PRIVACY REQUIREMENTS EXHIBIT

Please reference the below table and review the applicable sections for this solicitation.

Solution Type	Applicable Requirements
All Technologies	3, 4, 5, 6, 7, 8, 9, 12, 14, 15, 18, 21, 22, 23
Cloud/SaaS Services	3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 17, 18, 19, 21, 22, 23
Hosted IaaS Services	3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 18, 19, 20, 21, 22, 23
Professional Services	3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 18, 19, 20, 21, 22, 23
On-Premises Software	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 23
Hardware	3, 4, 5, 6, 8, 7, 9, 12, 14, 15, 16, 18, 21, 22, 23

TABLE OF CONTENTS

1. Purpose and Applicability	3
2. Definitions	4
3. Scope and Applicable Services	5
4. SAM Exclusion and Service Provider Eligibility	6
5. ADA Requirements and WCAG 2.1 Level AA Compliance	6
6. Information Security and Privacy Programs	7
7. County Information Ownership, Confidentiality, and Use	8
8. Service Provider's Use of County Information	8
9. Subcontractors and Third Parties	8
10. Software Compatibility with County Systems	9
11. Storage, Transmission, and Residency of County Information	9
12. Return or Destruction of County Information	10
13. Physical and Environmental Security	10
14. Operational Management, Business Continuity, and Disaster Recovery	10
15. Authentication and Access Controls	10
16. System Hardening, Configurations Management, and Vulnerability Management	11
17. Logging, Monitoring, and Auditability	11
18. Security Point of Contact (SPOC) and Escalation Contact	12
19. Security and Privacy Incidents	12
20. Cloud and Hosted Services Requirements	12
21. Business Support Hours and Service-Level Agreements (SLAs)	13
22. Regulatory-specific Requirements	14
23. Audit and Compliance	15

1.0 PURPOSE AND APPLICABILITY

Gwinnett County ("County") is committed to protecting the integrity of its systems, data, and information, as well as safeguarding the privacy of the individuals it serves. This Exhibit establishes and defines the mandatory information security and privacy requirements that apply to all **SERVICE PROVIDERS** delivering technology solutions to the County. These requirements are essential to ensuring the confidentiality, integrity, and availability of County systems and data.

The standards outlined in this Exhibit incorporate applicable federal, state, and local laws and align with recognized industry frameworks, including NIST SP 800-53, NIST SP 800-171, CIS Controls, GovRAMP, CJIS, HIPAA, and PCI-DSS, as applicable.

These requirements supplement and form part of the Contract between the County and the **SERVICE PROVIDER** delivering technology solutions to the County. They must be fully implemented before the Effective Date of the Contract and maintained throughout the duration of the contract.

If any conflict arises between the terms of this Exhibit and the terms of the Contract, the terms of this Exhibit will govern unless the Contract expressly states otherwise by specific reference to this Exhibit.

2.0 TERMS AND DEFINITIONS

Glossary	
Term or Acronym	Definition
Artificial Intelligence (AI)	any system, tool, model, or functionality that uses machine learning, natural language processing, neural networks, automated decision-making, or similar techniques to generate outputs, predictions, recommendations, or decisions without direct human control for each output.
Availability	Information is accessible and usable upon demand by an authorized entity.
Confidentiality	Information is not disclosed to unauthorized entities.
County Information / County Data	All data and information belonging to or processed on behalf of the County, including PII, PHI, PCI data, CJIS data, operational data, and system metadata.
Data	A subset of information consisting of qualitative or quantitative values.
GovRAMP	(formerly StateRAMP) Government Risk and Authorization Management Program governing cloud security requirements.
Incident / Security Incident	A suspected, attempted, successful, or imminent threat involving unauthorized access, use, disclosure, modification, or destruction of information; interference with IT operations; or violation of County policy.
Information	Any communication or representation of knowledge in any medium.
Information Security Policy	High-level statements defining an organization's security direction.

Glossary	
Term or Acronym	Definition
Information Security Program	Documented policies, standards, and procedures describing safeguards and controls.
Information Technology	Any equipment or system used to process or transmit data.
Integrity	Information has not been improperly altered or destroyed.
Mobile Device Management (MDM)	Software enabling administrative control over mobile devices.
Privacy Policy	High-level statements defining an organization's privacy direction.
Privacy Program	A formal document describing an organization's privacy structure, goals, and controls.
risk	The extent to which the County is threatened by a potential event.
Sensitive Data	County data that falls into categories which are subject to legislative regulations and/or regulatory compliance requirements, including but not limited to Personally Identifiable Information (PII), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and Criminal Justice Information Services (CJIS).
Subservice provider/Subcontractor	Any third party engaged by the SERVICE PROVIDER to support delivery of services.
threat	Any circumstance with potential to adversely impact County operations or assets.
vulnerability	A weakness within a computer system that may be exploited by a threat source resulting in compromised system data or functionality.
Workforce	Employees, volunteers, contractors, and others under the direct control of Gwinnett County.

3.0 SCOPE AND APPLICABLE SERVICES

This Exhibit applies to all **SERVICE PROVIDERS**, contractors, and consultants who seek to enter into agreements, contracts, or procurement arrangements with the Gwinnett County Government, whether through competitive bidding, direct purchase, cooperative agreements, or any other procurement method. It also applies to any subcontractors, affiliates, or third-party partners engaged by the **SERVICE PROVIDER** as part of their performance under a County contract.

This Exhibit extends to the following:

- Cloud-hosted software or platforms (SaaS, IaaS, PaaS)
- Data hosting, software implementation, or integration
- Managed IT, professional consulting, or technology services
- Solutions that are installed on, connect to, involve access to, or handle County data
- Other related technology solutions provided to the County, regardless of contract value or duration

The security, data privacy, and confidentiality requirements set forth in this Agreement are predicated on a risk-based approach.

The requirements set forth in this Exhibit shall remain in effect for the full duration of the contract, including any amendments, renewals, or extensions. **SERVICE PROVIDERS** are responsible for maintaining continuous compliance and must promptly notify the County of any changes in their status regarding federal exclusion, debarment, or prohibition from participation in U.S. government contracting or procurement activities. These requirements apply to all solutions and/or services proposed, regardless of the level of involvement or support provided by ITS.

4.0 SAM EXCLUSION AND SERVICE PROVIDER ELIGIBILITY

In accordance with 2 CFR §§ 180 (Non-procurement Debarment and Suspension), the County shall not award a contract to, or otherwise conduct business with, any **SERVICE PROVIDER**, including any parent, subsidiary, affiliate, subcontractor, or agent, that is currently listed as excluded, debarred, suspended, or otherwise ineligible to participate in federal, state, or local government contracts, as identified in the System for Award Management (SAM) at www.sam.gov.

It is the **SERVICE PROVIDER's** responsibility to verify the eligibility status of itself and all relevant associated entities prior to submission of a proposal and for the duration of any resulting contract. Any change in such status must be reported to the County Attorney, CIO and CISO in writing within five (5) business days of discovery. Noncompliance with this provision may result in disqualification, contract termination, or other appropriate action as determined by the County.

5.0 ADA Requirements and WCAG 2.1 Level AA Compliance

Title II of the Americans with Disabilities Act ("ADA") requires government entities to ensure that its websites, mobile applications, and digital content is accessible by persons with disabilities. Modern accessibility standards ensure that digital content is perceivable, operable, understandable, and robust for people with a wide range of disabilities, including those affecting vision, hearing, mobility, speech, cognition, and neurological processing. A new rule by the United States Department of Justice revised Title II of the Americans with Disabilities Act ("ADA") to incorporate the World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines (WCAG) 2.1, Levels A and AA as the prevailing technical standards for digital accessibility. The County has adopted (WCAG) 2.1 as the technical benchmark for digital accessibility compliance and will align web content as required to meet these technical requirements.

WCAG 2.1 Level AA requirements include:

- Providing text alternatives for non-text content
- Ensuring captions and audio descriptions for multimedia⁷
- Maintaining sufficient color contrast and support for text resizing
- Guaranteeing full keyboard accessibility and logical navigation order
- Preventing content that may trigger seizures or harmful physical reactions

- Supporting mobile accessibility, including requirements for orientation, pointer gestures, target size, and input purpose
- Ensuring compatibility with assistive technologies through proper name, role, and value coding of interface components

These technical standards are applicable to web content and digital services that the County makes available to the public through any digital interface, including but not limited to websites, mobile apps, online forms, documents, and interactive tools. All County **SERVICE PROVIDERS** that deliver technology solutions that are made available, or provide digital service, to the public on behalf of the County are required to comply with these Title II requirements as well. Such **SERVICE PROVIDERS** are required to provide a completed VPAT ([VPAT 2.5Rev WCAG \(April 2025\)](#)) to report how the then current version of the technology solution complies with the (WCAG) 2.1 accessibility standards.

6.0 INFORMATION SECURITY AND PRIVACY PROGRAMS

6.1 Information Security Program

The **SERVICE PROVIDER** must maintain a company-wide Information Security Program that includes:

- Documented security policies, standards, and procedures
- Regular review and updates
- Administrative, technical, and physical safeguards
- Workforce communication and training
- Annual training covering secure authentication, social engineering, proper handling of County Information, incident reporting, and privacy requirements
- Compliance based on best practices of NIST SP 800-53 (Moderate baseline or higher), NIST SP 800-171 (where applicable), or CIS Controls

The **SERVICE PROVIDER** must implement measures to:

- Protect County Information from unauthorized access, disclosure, alteration, or destruction
- Protect against anticipated threats
- Prevent accidental loss or damage
- Ensure personnel accessing CJIS, PHI, or PCI data meet applicable screening requirements
- Comply with all applicable federal, state, and local laws

6.2 Privacy Program

The **SERVICE PROVIDER** must maintain a company-wide Privacy Program that includes:

- A framework ensuring compliance with applicable privacy laws, including HIPAA, CJIS, and Georgia privacy statutes
- Requiring employees and agents to sign confidentiality agreements, if they have access to County data

- Internal and external privacy policies
- Workforce privacy training
- A Privacy Incident response plan
- Ongoing assessments and audit

7.0 COUNTY INFORMATION OWNERSHIP, CONFIDENTIALITY, AND USE

All County Information is the exclusive property of the County and is treated as confidential, regardless of labeling. The **SERVICE PROVIDER** may use County Information only to fulfill its contractual obligations and for no other purpose.

The **SERVICE PROVIDER** may not disclose, sell, assign, lease, or otherwise transfer County Information to any third party without the County's prior written authorization, except where disclosure is required by law. If legally compelled disclosure is required, the **SERVICE PROVIDER** must notify the County in advance unless prohibited by law.

Aggregation of County Information is permitted only when:

- Aggregated Data contains no information identifiable as originating from the County, and
- De-identified Data cannot be associated with any individual.

The **SERVICE PROVIDER** must not disclose County non-public information (NPI) and must support the County in responding to individual privacy rights requests. County Information may be retained only as long as necessary to meet contractual or legal obligations.

The County retains the right to access County Information stored on any **SERVICE PROVIDER**-owned or leased device.

8.0 SERVICE PROVIDER'S USE OF COUNTY INFORMATION

The **SERVICE PROVIDER** must collect, maintain, transmit, store, and destroy County Information only as permitted under the Contract and in compliance with all applicable laws, including:

- Georgia breach notification laws
- Georgia Open Records Act
- Federal Trade Commission regulations
- HIPAA, PCI-DSS, CJIS, and other applicable federal privacy/security laws

County Information may not be used for analytics, AI model training, product development, or any secondary purpose without explicit prior written authorization.

9.0 SUBCONTRACTORS AND THIRD PARTIES

The **SERVICE PROVIDER** shall not subcontract any part of the work covered by this Agreement or permit subcontracted work to be further subcontracted without the DEPARTMENT's prior written approval of the subservice provider, except as may have been specifically stated in the **SERVICE PROVIDER's** response to proposal per Exhibit A. The DEPARTMENT will not approve any subservice provider for work covered by this Agreement that has not been recommended for approval by the Department Director.

Subcontractors must:

- Agree in writing to comply with this Exhibit
- Meet all regulatory requirements applicable to the data they handle

The **SERVICE PROVIDER** remains fully responsible for subcontractor actions.

10.0 SOFTWARE COMPATIBILITY WITH COUNTY SYSTEMS

The **SERVICE PROVIDER** must ensure that all on-premises applications, agents, or components installed on County systems must:

- Be fully compatible with **currently supported versions of Microsoft Windows** as defined by Microsoft's lifecycle policy (Mainstream or Extended Support).
- Remain compatible with new Windows security updates, cumulative updates, and feature updates released by Microsoft.
- Not require the County to run unsupported, end-of-life, or unpatched operating systems.
- Include timely updates or patches to maintain compatibility with supported Windows versions.

In addition, the **SERVICE PROVIDER** must ensure that all on-premises software, agents, services, or components installed on County-owned systems:

- Are fully compatible with **Microsoft Defender for Endpoint**, including real-time protection, behavioral monitoring, and endpoint detection and response (EDR) capabilities.
- Do not disable, interfere with, bypass, or degrade Microsoft Defender functionality.
- Do not require the County to disable or weaken any existing endpoint security controls.
- Are capable of operating under the County's standard security baselines, including Defender policies, Group Policy Objects (GPOs), and CIS-aligned hardening configurations.

The **SERVICE PROVIDER** must promptly update their software to maintain compatibility with County-mandated endpoint protection tools.

11.0 STORAGE, TRANSMISSION, AND RESIDENCY OF COUNTY INFORMATION

The **SERVICE PROVIDER** must:

- Identify all County Information that will be stored in any cloud environment as part of the proposal response
- Encrypt County Information at rest and in transit using FIPS-validated methods
- Use TLS 1.2 or higher for external transmissions
- Maintain current security patches and antivirus protections
- Use MDM for all mobile devices storing County Information
- Ensure County Information remains within approved geographic regions and is not transferred outside the United States without written approval

CJIS residency requirements supersede all other residency rules where applicable.

12.0 RETURN OR DESTRUCTION OF COUNTY INFORMATION

Upon request or contract termination, the **SERVICE PROVIDER** must return or destroy County Information. Returned County Information must be provided in an open, industry-standard, non-proprietary format that allows the County to access, read, and use the data without requiring the **SERVICE PROVIDER's** software, tools, or licenses.

Destruction of County Information must comply with NIST SP 800-88 or stricter applicable regulatory requirements. The **SERVICE PROVIDER** must provide written certification confirming the return or destruction of all County Information.

13.0 PHYSICAL AND ENVIRONMENTAL SECURITY

SERVICE PROVIDER facilities processing County Information must:

- Be located in secure areas with controlled access
- Maintain environmental controls consistent with hardware specifications

14.0 OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY

The **SERVICE PROVIDER** must:

- Monitor and manage information processing facilities
- Maintain antimalware and backup systems
- Maintain business continuity and disaster recovery plans
- Use a geographically separate backup location
- Encrypt all backup media
- Meet County specified RTO and RPO requirements as specified in the proposal
- Conduct annual testing of continuity plans

15.0 AUTHENTICATION AND ACCESS CONTROLS

The **SERVICE PROVIDER** must implement:

- Authentication mechanisms that follow industry standards such as NIST SP 800-63 or CIS Controls
- Role-based access controls (RBAC) with the ability to define granular permissions
- Single Sign-On (SSO) integration and utilize industry-standard secure authentication protocols, including **SAML 2.0, OpenID Connect (OIDC), and/or OAuth 2.0**
- County-approved VPN for remote access
- The ability to restrict the storing, processing, or transmitting of Gwinnett County user passwords outside of the approved SSO authentication process.
- Industry-standard best practices, including encryption in transit and at rest to protect authentication tokens and session credentials

Any inability to meet Gwinnett County SSO shall be disclosed in writing during the RFP process and must be approved in writing by Gwinnett County prior to contract award or execution.

16.0 SYSTEM HARDENING, CONFIGURATION MANAGEMENT, AND VULNERABILITY MANAGEMENT

The **SERVICE PROVIDER** must:

- Follow secure configuration baselines such as CIS Benchmarks
- Maintain an inventory of all hardware, software, and cloud services supporting County operations
- Follow a documented change management-process with rollback procedures
- Conduct regular vulnerability scanning
- Remediate vulnerabilities within required timelines:
 - Critical: 15 days
 - High: 30 days
 - Medium: 60 days
- Notify the County's designated security contact when vulnerabilities cannot be remediated within the required timelines, in accordance with the County's established security notification procedures.
- Conduct annual penetration testing for externally accessible systems

17.0 LOGGING, MONITORING, AND AUDITABILITY

The **SERVICE PROVIDER** must implement comprehensive logging and monitoring controls that support security investigations, incident response, and regulatory compliance. At a minimum, the **SERVICE PROVIDER** must:

- **Generate and retain logs** for all authentication events, administrative actions, privileged activity, configuration changes, data access, and other security-relevant events.
- **Retain logs for a minimum of twelve (12) months**, or longer if required by applicable law or regulation.
- **Protect all logs against unauthorized access, alteration, and deletion**, including through access controls, integrity protections, and secure storage.
- **Continuously monitor logs** and support automated alerting for anomalous, suspicious, or policy violating activity.

If the solution processes sensitive County data:

- **Provide real-time or near-real-time log forwarding** to the County's Microsoft Sentinel SIEM upon request, using standard, industry-accepted protocols (e.g., syslog, HTTPS API, or equivalent).
- **Ensure logs are provided in an open, structured, and easily exportable format** that does not require proprietary tools for ingestion or analysis.

18.0 SECURITY POINT OF CONTACT (SPOC) AND ESCALATION CONTACT

The **SERVICE PROVIDER** must designate a primary **Security Point of Contact (SPOC)**, who will serve as the main liaison with the County for all security-related matters under this contract. The SPOC must be authorized to respond to inquiries regarding incident response, policy compliance, access coordination, and risk mitigation.

In addition to the SPOC, the **SERVICE PROVIDER** must also designate a 24/7 Emergency Security Escalation Contact who is reachable outside of normal business hours in the event of urgent incidents that may impact County systems, data, or operations. This escalation contact may be the same as the primary SPOC, provided they are available at all times.

The following information must be submitted for both contacts at the time of proposal:

- Full name and title
- Email address
- Office and mobile phone numbers
- Escalation hierarchy (if applicable)

The **SERVICE PROVIDER** is required to keep this information accurate and current throughout the duration of the contract. Any changes to contact assignments must be reported to the County in writing within **ten (10) business days**.

19.0 SECURITY AND PRIVACY INCIDENTS

The **SERVICE PROVIDER** must notify the County within **24 hours** of discovering any actual or suspected Security Incident involving County Information.

Notifications must include:

- Date/time of discovery
- Approximate date/time of incident
- Description of affected County Information
- Summary of facts and remediation steps

The **SERVICE PROVIDER** must provide the County with a written incident report no later than **ten (10) business days** after discovering any data or security breach, or earlier if mandated by applicable law.

Regulatory specific- timelines (HIPAA, PCI-DSS, CJIS, GovRAMP) supersede these requirements where stricter.

20.0 CLOUD AND HOSTED SERVICES REQUIREMENTS

Cloud services must comply with:

- GovRAMP Moderate or High (as applicable)
- FIPS validated- cryptographic modules
- Disclosure of all data storage locations and sub processors

The County retains ownership of all data and must be able to export data in a non-proprietary format at any time.

21.0 BUSINESS SUPPORT HOURS AND SERVICE-LEVEL AGREEMENTS (SLAs)

21.1 Business Support Hours

The **SERVICE PROVIDER** must provide business and technical support services consistent with the operational needs of the County. At a minimum:

- **Standard Support Hours:** The **SERVICE PROVIDER** shall provide support during the County's standard business hours, defined as **Monday through Friday, 8:00 a.m. to 5:00 p.m. Eastern Time**, excluding County recognized- holidays, unless otherwise specified in the Contract or Statement of Work (SOW).
- **Extended or 24/7 Support (If required):** If the services provided are mission critical, public facing, or otherwise designated by the County as requiring continuous availability, the **SERVICE PROVIDER** shall provide **24/7/365 support**, including weekends and holidays.
- **Support Channels:** The **SERVICE PROVIDER** must provide at least two of the following support channels:
 - Telephone support
 - Email support
 - Web based- ticketing system
 - Secure customer portal
- **Response Expectations:** The **SERVICE PROVIDER** must acknowledge receipt of all support requests within the timeframes defined in the SLA.

21.2 Service Level Agreements (SLAs)

The **SERVICE PROVIDER** must specify SLAs in the Contract or SOW. At a minimum, SLAs must address:

- **Incident Response Times Defined response times for:**
 - Critical incidents
 - High severity incidents
 - Medium severity incidents
 - Low severity incidents
- **Resolution Timeframes:** Maximum allowable time to resolve incidents based on severity.
- **System Availability/Uptime:** If hosting or cloud services are provided, the **SERVICE PROVIDER** must meet the minimum uptime requirement specified by the County, which shall not be less than:
 - **99.9% uptime for mission critical systems**, or
 - As otherwise defined in the SOW.
- **Maintenance Windows:** The **SERVICE PROVIDER** must coordinate planned maintenance with the County and provide at least **ten (10) business days' notice**, unless emergency maintenance is required.
- **Escalation Procedures:** The **SERVICE PROVIDER** must maintain documented escalation paths and ensure timely involvement of senior technical staff when required.

22.0 REGULATORY-SPECIFIC REQUIREMENTS

22.1 CJIS

If the **SERVICE PROVIDER** processes CJIS data, it must complete the FBI's CJIS Security Addendum and comply with the FBI CJIS Security Policy, including:

- Personnel background checks
- Advanced authentication
- Encryption and physical security controls
- CJIS compliant- audit logging

22.2 HIPAA

If the **SERVICE PROVIDER** processes PHI, it must:

- Comply with HIPAA Security, Privacy, and Breach Notification Rules
- Execute a Business Associate Agreement (BAA)
- Implement safeguards appropriate for PHI

22.3 PCI-DSS

If the **SERVICE PROVIDER** processes payment card data, it must:

- Maintain PCI-DSS compliance
- Provide annual Attestation of Compliance (AOC)
- Provide a PCI-DSS Responsibility Matrix defining each party's responsibilities

- Segregate cardholder data environments

22.4 GovRAMP

Cloud systems hosting sensitive County Information must:

- Maintain GovRAMP Moderate or High authorization
- Provide continuous monitoring reports upon request

Sensitive County Information is defined as data that falls into categories which are subject to legislative regulations and/or regulatory compliance requirements including but not limited to, Personally Identifiable Information (PII), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and Criminal Justice Information Services (CJIS).

When determining if data is considered Personally Identifiable Information (PII), Gwinnett County will employ the definition of “Personal Information” found in **Georgia code § 10-1-911**. Data classification will be further guided by **Georgia code § 50-18-72**, which defines exclusions to the **Georgia Open Records Act**.

23.0 AUDIT AND COMPLIANCE

The County may audit the **SERVICE PROVIDER’s** compliance with this Exhibit **once during any twelve-month period for the full duration of the contract**.

The **SERVICE PROVIDER** must maintain, update, and deliver current annual compliance documentation **to the extent applicable to the systems, environments, or services used to provide the proposed solution**, including:

- **SOC 2 Type II, ISO 27001 certification, or equivalent** for any in scope systems or processes that store, process, or transmit sensitive County Information
- **GovRAMP continuous monitoring reports**, if applicable
- **PCI-DSS Attestation of Compliance (AOC)**, if applicable
- **HIPAA compliance attestations**, if applicable
- **CJIS Addendum and/or audit documentation**, if applicable
- **VPAT**, if the technology solution is made available, or provides a digital service, to the public on behalf of the County

Failure to maintain continuous compliance or to provide required annual documentation **constitutes a material breach of contract**. The County may, at its sole discretion, impose enforcement actions, including but not limited to withholding of payment, suspension of services, termination for cause, or disqualification from current or future County procurements.