HARRIS COUNTY MINIMUM INFORMATION TECHNOLOGY SECURITY VENDOR CONTROLS LIST

Section 1: All Vendors

The following controls are required for all vendors developing, hosting, or supporting a Harris County IT solution.

Controls

1. Annual cybersecurity training is required for vendor's employees and contractors.
2. Background checks are required for personnel who support or have access to Harris County's data and systems.
3. Secure coding practice is in place based on industry standards.
4. All code is checked for back doors / trojan horses.
5. All buffers in the application have error handling which governs buffer resources.
6. The system supports Multi-factor Authentication (MFA).
7. Privileged / Administrative user access is logged and monitored.
8. Vendor has a network Intrusion Detection System (IDS) in their infrastructure.
9. Vendor has a host-based Intrusion Detection System (IDS) in their infrastructure.
10. Vendor has an active internal cybersecurity program and written policies that include secure coding and system development practices, network security, physical security, user account management, vulnerability detection and management, incident detection and response, and business continuity/disaster planning.

Artifacts

Vendor to provide Harris County with the following:

1. Signed document confirming that there are no critical, high or moderate security flaws in their developed code.
2. Current SOC2 Type 2 Report (Include Bridge Letter for reports over 12 months old); If SOC2 report is not available, submit signed vendor attestation letter.
3. Most recent Penetration Test Report for the applicable product (if available)

HARRIS COUNTY MINIMUM INFORMATION TECHNOLOGY SECURITY VENDOR CONTROLS LIST

Section 2A: Cloud Vendors (Software as a Service – SaaS)

The controls listed in this section are required for all vendors developing or providing cloud computing services that:

- Process, store, or transmit Harris County data including among other confidential data:
  - Personally Identifiable Information (PII)
  - Payment Card Information (PCI)
  - Protected Health Information (PHI)
  - Criminal Justice Information (CJI)
- Are classified as Business critical, i.e., having a severe impact on people, the environment, assets and reputation
- Are internet accessible and Harris County branded OR
- Are internet accessible and connected to resources on the Harris County Enterprise Network

Controls

1. Vendor completes annual third-party testing and obtains attestations and certifications from reputable organizations.
2. Vendor regularly performs vulnerability scans, assessments, and penetration testing.
3. Vendor completes Harris County provided questionnaires.
4. Vendor complies with local laws and regulations in jurisdictions applicable to the vendor and Harris Count.
5. Comply with all industry security standards relevant to your business such as NIST, CJIS, HIPAA, PCI, DSS, HITRUST, ISO27001, and SSAE 18.
6. Vendor complies with data localization requirements.
7. The system does not store database connection information, passwords, and any other sensitive credentials in plain text.

Artifacts

- SOC2 Type 2 Report (Include Bridge Letter for reports over 1 year old)
- ISO 27001 certificate for providers operating from a private data center
- HiTrust Certificate – for providers handling PHI
- Last OWASP scan report
- Last penetration test report (including automated and manual / human testing)
- Harris County (HC) Vendor Technical Questionnaire
- Harris County (HC) Vendor PII/SPII Questionnaire

Note: Comply with all controls in Section 1: All Vendors.

Section 2B: Cloud Vendors (Software as a Service – SaaS)

The controls listed in this section are required for all vendors developing or providing cloud computing services that process, store, or transmit Harris County data that is non confidential or non PII, non PCI, non PHI, non CJI, or non business critical.

Controls

1. Vendor completes Harris County provided questionnaires.
2. Vendor complies with local laws and regulations in jurisdictions applicable to the vendor and Harris County.

Artifacts

- Vendor Attestation letter or SOC2 Type 2 Report (Include Bridge Letter for reports over 12 months old)
- ISO 27001 certificate for providers operating from a private data center

Note: Comply with all controls in Section 1: All Vendors.

HARRIS COUNTY MINIMUM INFORMATION TECHNOLOGY SECURITY VENDOR CONTROLS LIST

Section 3: Custom Application Design Vendors

The controls in this section pertain to vendors who provide custom development for Harris County solutions

Controls

1. Vendor designs and develops application that:

    - Enables and enforces Multi-Factor Authentication (MFA) wherever and when applicable.
    - Enables complex passwords that meet or exceed National Institute of Standards and Technology (NIST) password guidance.
    - Enables encryption (FIPS 140-2 compliant) to protect sensitive data in transit between systems and at rest in online data storages and backups capability.
    - Generates and maintains logs of user access, user activity, system activity including privileged identities
    - Utilizes single sign-on using modern and industry standard protocols, if applicable to the solution being procured.

2. Vendor monitors threats and produces and deploys patches to address application vulnerabilities that materially impact security.
3. Vendor trains developers and implements development guidelines to prevent the OWASP top 10 vulnerabilities or at least the following vulnerabilities:

    - Authorization bypass. Example: Accessing other customers' data or admin features from a regular account.
    - Insecure session ID. Examples: Guessable token; a token stored in an insecure location (e.g., cookie without secure and HTTP Only flags set).
    - Injections. Examples: SQL injection, NoSQL injection, XXE, OS command injection.
    - Cross-site scripting. Examples: Calling insecure JavaScript functions, performing insecure DOM manipulations, echoing back user input into HTML without escaping.
    - Cross-site request forgery. Example: Accepting requests with an Origin header from a different domain.

- Use of vulnerable libraries. Example: Using server-side frameworks or JavaScript libraries with known vulnerabilities.

4. Vendor maintains a list of sensitive data types that the application is expected to process.

5. Vendor maintains up-to-date system architecture and data flow diagrams indicating system components and data transmission.

6. Vendor's build processes must be fully scripted/automated and generate provenance.

<u>Artifacts</u>

- Vendor Attestation Letter
- Vendor Software Development LifeCycle (SDLC) Policies
- Proof of Cybersecurity training for vendor's staff accessing the Harris County network
- Usage of county issued devices to access the Harris County network or usage of vendor issued devices with vendor managed anti-virus and local firewall by vendor's staff or consultants
- Proof of corporate managed anti-virus and firewall on computers used by the vendor's staff accessing the Harris County network

Note: Comply with all controls in Section 1: All Vendors.

Section 3: Commercial Off The Shelf Software

The controls listed in this section are required for all vendors providing commercial off the shelf software (COTS) to Harris County.

<u>Controls</u>

1. Vendor completes Harris County provided COTS questionnaire.

2. Vendor provides third-party penetration testing report (if available)

3. Vendor provides report/s from independent / external audit firm (if available).

<u>Artifacts</u>

- Vendor Attestation letter (Note: SOC2 Type 2 Report (Include Bridge Letter for reports over 12 months old) is acceptable.)

- Most recent penetration test report (including automated and manual / human testing) if available

Note: Comply with all controls in Section 1: All Vendors.