GUIDANCE FOR RFP's

IT Security understand that the University will work with external vendors for solutions to complex healthcare related initiatives.

This document outlines the recommended minimum security framework for all vendors to comply with, in relation to security.

UT Health IT Security Group

Contents

Scope 3
Background 3
Key Assumptions 3
Purpose 3
Terminology 3
Note on Security & Privacy 4
Information Security Policies 4
Privacy & Confidentiality 5
Application Development 5
Authentication & Identity Management 6
Confidential Information Authorization 7
Incident Response 7
Audit & Inspection 8
Availability 9
Encryption 9
Data retention 10
System Configuration & Maintenance 10

Scope

The scope of this project is strictly limited to any vendor who is submitting a RFP for IT work that will be consumed by the UTHealth network.

Background

IT Security has been increasingly reviewing and evaluation vendors for implementation at UTHealth. We have determined that placing our minimums requirements from an IT Security perspective will help vendors evaluate their solutions to ensure adherence to UTHealth policies prior to submitting them for evaluation. This document will help vendors develop solutions that can be approved for use at UTHealth.

Key Assumptions

IT Security will work with vendors to evaluate and make recommendations on an as needed basis.

IT Security reserves the right to perform its own evaluation to ensure standard and minimum requirements are met.

Purpose

The purpose of this document is to define the UTHealth information security requirements for vendors who wish to provide IT products, services or support to UTHealth. All vendors awarded a contract to provide such services must comply with the policies set forth in this document. At its discretion, IT Security may require vendors to implement, comply with, and/or provide proof of one or more of the requirements laid out in this document.

Terminology

A. **Application** – means software that performs a user-facing function, such as a web application

B. **Confidential Information** – means any personally identifiable information related to UTHealth students, student families/guardians, UTHealth employees, agents and/or volunteers obtained by or furnished to the Vendor; including HIPAA and FERPA data. All findings, analysis, data, reports or other information learned or developed and based thereon, whether in oral, written, graphic, or machine-read-able form; and all information marked "confidential"

C. **HIPAA Data** - Protected Health Information (PHI) is defined by the Health Insurance Portability and Accountability Act (HIPAA). PHI is individually identifiable health information that relates to the. Past, present, or future physical or mental health or condition of an individual.

D. **FERPA** – means the Family and Educational Rights and Privacy Act (20 U.S.C. 1232g) and any applicable regulations promulgated thereunder, including but not limited to 34 C.F.R. Part 99.

E. **PII** – means personally identifiable information, as defined under FERPA.

F. **System** – means any information technology processing device, including routers, servers, Applications, workstations and mobile devices.

G. **Vendor** – means an entity awarded a contract by the UTHealth to provide a product, service or work for UTHealth

Note on Security & Privacy

UTHealth systems and applications may contain sensitive data, including records of academic performance, medical, legal, and family details and proprietary and confidential internal records concerning UTHealth students and/or patients, in addition to information that is confidential by law.

Failure to protect Confidential Information from unauthorized disclosure or abuse can have severe legal, financial and reputation consequences for the UTHealth, its students, patients, employees and the Vendor.

Information Security Policies

A. Vendors must have, and upon request by UTHealth shall promptly provide UTHealth with copies of its, information security policies that cover the following elements:
    1. Data classification and privacy
    2. Security training and awareness
    3. Systems administration, patching and configuration
    4. Application development and code review
    5. Incident response
    6. Workstation management, mobile devices and antivirus
    7. Backups, disaster recovery and business continuity
    8. Regular audits and testing
    9. Requirements for third-party business partners and contractors
    10. Compliance with information security or privacy laws, rules, regulations or standards
    11. Downstream Business Associate Agreements, if applicable.
    12. Any other information security policies

B. Policy Requirements: In addition to addressing the elements set forth above:
    1. Vendor must indicate in their policies the date of the most recent revision.
    2. Vendor must include a certification from its Chief Operating Officer, or individual with an equivalent title with authority to represent the Vendor, with Vendor's proposal/response to the RFP that all of the above elements are addressed in Vendor's security policies, and that such policies are at least as rigorous as the policies set forth in this document. If Vendor cannot make such certification for any reason (e.g. Vendor's policies do not address an element listed above), Vendor must notify UTHealth of the

deficiency in its proposal/response to the RFP.

3. Vendor shall maintain compliance with such policies and, unless the vendor receives UTHealth's prior written approval, Vendor shall not make any changes to such policies that would result in in such policies (i) not addressing one or more elements set forth above

Privacy & Confidentiality

A. The Vendor must hold Confidential Information in strict confidence and not disclose it to any third parties nor make use of such Data for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon.

B. The Vendor shall use commercially reasonable efforts to secure and defend any System housing Confidential Information against third parties who may seek to breach the security thereof, including, but not limited to breaches by unauthorized access or making unauthorized modifications to such System.

C. The Vendor shall protect and secure all Confidential Information in transit (collected, copied and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer.

D. The Vendor shall maintain all copies or reproductions of Confidential Information with the same security it maintains the originals. At the point in which the Information is no longer useful for its primary or retention purposes, Vendor must destroy such Data, making it unusable and unrecoverable.

E. For all Application screens, front pages of reports, and landing pages of web Applications that contain Confidential Information, Vendor must include prominent confidentiality notices in legible-sized font on each page (e.g. a prominent notice that the information on such screen or report is confidential on the bottom of a web screen or the footer of a report page).

F. All web Application screens that contain Confidential Information must be non-cacheable.

G. Confidential Information should not appear in URLs.

H. Vendor's development, test and QA environments shall not use real Confidential Information.

Application Development

A. Vendors shall have a comprehensive secure development lifecycle System in place consistent with industry standard best practices, including policies, training, audits, testing, emergency updates, proactive management, and regular updates to the secure development lifecycle System itself.

B. Vendor must review and test all application code for security weaknesses and backdoors prior to deployment with UTHealth.

C. All high risk findings and exploitable vulnerabilities must be resolved before the Application is released. A development manager of Vendor must certify in writing to UTHealth that a security review has been conducted and that all risks are acceptable before every release.

D. Vendors that handle Confidential Information must respond to and resolve security-related bug reports, inquiries and incidents in a timely and professional manner. The Vendor must notify UTHealth within 24 hours of when Vendor becomes aware of any such incident that poses a potential risk to UTHealth data.

Authentication & Identity Management

A. If an application requires Single Sign-On (SSO) integration with UTHealth, the Vendor must support authentication for UTHealth Users.
    a. Vendors will not have the ability to make any changes to UTHealth Identity Management Systems.
    b. If new UTHealth Users need to be enrolled or register in order to use a Vendor's System, the plan for registration process and ownership of identity management must be agreed upon in writing by UTHealth Information Security.

B. If the Vendor maintains its own identity management system for its users, it must:
    a. Enforce a one user, one account policy in which shared/ group accounts and duplicate accounts are not permitted
    b. Be free of testing, development and non-production accounts.
    c. Maintain accurate legal name, address, phone number information for all users who are permitted to access Confidential Information, and upon request from UTHealth, produce lists of users who will have access to Confidential Information.
    d. Enforce a strong password policy of eight characters minimum, with mixed case and at least one number or special character.
    e. Store all passwords in non-reversible one-way cryptographic hash.
    f. Log all successful and failed authentication attempts, including date, time, IP address, and username.
    g. Offer a secure password reset feature, including verification of identity, email or

text notification and a one-time-use password link that expires after 24 hours.

h. Automatically de-provision accounts for terminated employees of Vendor and UTHealth.

C. Temporarily lock accounts with repeated failed login attempts and provide support to affected users.

D. Keep attributes and group structures that support authorization accuracy.

Confidential Information Authorization

A. Applications that Handle Confidential Information must have explicitly defined authorization controls that prevent users from exceeding their intended privileges.

B. Applications must perform authorization checks before performing any action that creates, views, updates, transmits or deletes Confidential Information. Authorization logic must be highly configurable and alterable without code changes.

C. Authorization checks must verify the user has appropriate role to perform the requested action, and also the correct scope.

D. Whenever possible, authorization checks will use UTHealth framework, UTHealth identity management system and other UTHealth Systems of record. Access to these Systems may be either via a web service or replicated database, at UTHealth's discretion. The Vendor Application will not be able to make any changes to the contents of these Systems.

E. Any non-UTHealth accounts that are managed locally by the Vendor must follow the principal of "Least Privileged Access" whereby those user accounts are provided the most restrictive access necessary to perform the required business function. "Super users" (i.e. application administrators) must be avoided unless absolutely necessary due to a legitimate administrative or educational need for such access in order to provide the Services.

Incident Response

A. Vendors must have a plan for compliance with all applicable breach notification laws.

B. UTHealth must be notified in writing within 24 hours of the earliest indication or report of a potential breach or unintended disclosure of Confidential Information or a System that supports it.

C. Response actions to incidents that might affect Confidential Information or Systems must be conducted quickly and with ample resources. Vendor will hire a professional third-party incident response team if in- house resources do not have sufficient skill or availability.

D. UTHealth shall have the right to view all incident response evidence, reports, communications and related materials upon request.

E. If requested by UTHealth, or if required by law, the Vendor shall notify in writing all persons affected by the incident, at its own cost and expense.

Audit & Inspection

A. The Vendor shall allow UTHealth, upon reasonable notice, to perform security assessments or audits of Systems that Handle or support Confidential Information. Such an assessment shall be conducted by an independent 3rd party agreed upon by the Vendor and UTHealth, and at UTHealth's own expense, provided that the Vendor cooperate with any such assessment/audit and shall, at its own expense, provide all necessary support, personnel and information needed to ensure the successful completion of the assessments or audits.

B. The Vendor shall provide UTHealth, upon UTHealth's request, with a SSAE 16 or similar report as agreed to by UTHealth for critical business processes relating to protection of Confidential Information and safeguards implemented in its organization.

C. Vendors must engage an independent third party annually to assess the practical security of Vendor's Systems. These reviews must include penetration tests from the perspective of an external attacker and an internal user with common privileges. The penetration tests must include all Systems exposed to the internet and any Systems, internal or external, that Handle Confidential Information. Such annual assessment shall be at Vendor's sole expense.

D. Audit logs must be implemented for all Systems that Handle Confidential Information. All attempted violations of System security must generate an audit log. Audit logs must be secured against unauthorized access or modification.

E. In the event of adverse findings through a UTHealth or Vendor audit, the Vendor

shall cooperate with UTHealth in remediating any risks to Confidential Information, including complying with request to temporarily taking the system offline or otherwise limiting access to the system, and any other follow up actions reasonably necessary to secure the Confidential Information.

Availability

A. Vendor Systems that Handle Confidential Information shall be available and fully functional 24x7x365 with 99.99% uptime, unless otherwise agreed upon in writing with UTHealth. Vendor shall make plans for colocation, backups and any other Systems necessary to ensure continuity.

B. Vendor must notify and obtain agreement from UTHealth for any planned interruptions in service, with the exception of emergency security updates. Vendor must notify UTHealth immediately of any unintended service interruption.

Encryption

A. All Systems that Handle Confidential Information must encrypt UTHealth data that include Confidential Information in transit using algorithms and key lengths consistent with the most recent NIST guidelines.

B. For HTTP and other protocols that use SSL/TLS, Vendor shall use the TLS 1.1 or later protocol with 128-bit or larger key size, and shall make previous protocols and smaller keys unavailable.

C. Vendor shall utilize a third party provider that is a recognized and trusted authority in the industry to generate any certificates that are used for authentication between two parties (e.g., Vendor and UTHealth or Vendor and any other party).

D. Web Applications that contain Confidential Information must be available only over Transport Layer Security ("TLS"). Attempts to use the Application without encryption shall be rejected. Encrypted and non-encrypted content shall not be mixed.

E. Data at rest that is stored outside of hardened Application or database production Systems must be protected by encryption consistent with NIST recommendations.

F. The Vendor shall keep private keys confidential, implement key lifecycle

management and protect all keys in storage or in transit.

G. The Vendor shall choose keys randomly from the entire key space and ensure that encryption keys allow for retrieval for administrative or forensic use.

H. Encryption of UTHealth data in production databases is required. Any database encryption system must be approved by UTHealth, which approval shall not be unreasonably withheld. UTHealth must be provided with a complete set of decryption keys. All UTHealth data must be recoverable.

I. In the event that Vendor will store UTHealth data outside of the United States, Vendor shall notify UTHealth of the locations outside the U.S. by providing notice either in its proposal to the RFP if known by Vendor prior to award, or if known after award, to appsecurity@schools.nyc.gov; provided that UTHealth reserves the right to require that the use, storage, or handling of UTHealth data occur within the contiguous United States or similar regional boundary as defined by UTHealth, which, if applicable, shall be specified in the RFP.

Data retention

A. Vendors may be required to support retention of Confidential Information as agreed upon.

B. Retention requirements for UTHealth data may be specified in the RFP. If applicable, the Vendor must acknowledge in its proposal to the RFP that it can meet the requirements and, upon request by UTHealth, demonstrate that retention requirements are being implemented.

C. Record retention systems must comply with all security and privacy controls set forth in this document.

System Configuration & Maintenance

A. All operating Systems, servers, and network devices that support UTHealth Systems or Confidential Information must be kept hardened and patched.

B. All Vendor Systems that are used to host, transfer, or otherwise interact with Confidential Information must enforce strict separation from any non-UTHealth

Systems. This can be achieved through physical and/or logical separation. The separation must be auditable and able to be proven at the request of UTHealth.

C. Vendors must maintain technical best security practices configuration guidelines for all such Systems and update them at least twice per year.

D. All security-related patches must be installed on Systems within 24 hours of their release. Vendor will maintain a testing lab in order to support this.