STANDARD

1) To ensure the appropriate safeguards are in place to protect information and systems, risk assessments must be performed on systems and applications when they are initially implemented and after any significant changes in functionality or types of data used.

2) IT Security Risk Management will ensure processes are in place to identify systems that require risk assessments and determine whether the risk assessment level will be high, moderate or low.

3) High-level detailed risk assessments will be performed whenever any of the following circumstances are met and the exceptions listed above do not apply:

   a) Restricted Information, including PHI, is involved, which includes, but is not limited to:
      i) Patient, employee, student, and research subject information
      ii) PHI, see the list of 18 PHI identifiers
      iii) Genetic information
      iv) Passwords or other authentication credentials
      v) Financial account information, including credit card data
      vi) Animal research information (photos, protocols, locations)
      vii) Intellectual property
      viii) Proprietary information
      ix) Information for which there are contractual requirements for protection.
      x) Information for which the unauthorized disclosure would damage the reputation of the University

   b) Data that would be classified at Protection Level 3 or 4 according the UC Institutional Information and Data Classification Standard is involved. Note that Protection Level 3 and 4 map to what we consider Restricted Information. Thus, the examples for P3 and P4 data types in the UC Protection Level Classification Guide can also be used as a reference for the types of data that require risk assessments. Note that this keeps us in sync with the UC information security policy, IS-3: Electronic Information Security, as IS-3 requires risk assessments for Institutional Information and IT resources classified at Protection Level 3 or higher.

   c) Critical IT infrastructure is involved. Examples include, but are not limited to:
      i) Firewalls
      ii) Authentication systems

   d) The project involves systems, applications, or data that are hosted offsite by a 3rd party.

e) The project involves an Internet-accessible service or system, including but not limited to web applications, SFTP, and SSH.

f) The CISO, Chief Compliance Security Officer, Risk Assessor Manager, other Security/Compliance Leadership, etc. determines that aspects of a project beyond those listed above may pose significant risk and so a high-level risk assessment must be performed.

4) Moderate. Moderate-level risk assessments will be performed for systems that do not directly involve PHI/RI or IS-3 P3/P4 data, but that still may be important for operations and/or will be connected to the network.
   a) Examples would include, but are not limited to, servers/applications that would need to be included in Disaster Recovery planning or IoT devices that will connect to UCLA Health networks. This could also include minor upgrades to systems that have recently had a high-level risk assessment.
   b) Vulnerability scans will be performed and remediation will be completed for all Critical and Severe vulnerabilities as well as for moderate vulnerabilities for which an exploit exists. Hardware must meet all hardening standards before go live is approved

5) Low. This category will generally be for infrastructure projects that do not directly involve systems/applications that would require high- or moderate-level risk assessments such as cabling, or equipment moves/installs, new office space, etc. for which no vulnerability scans or technical review are necessary.

6) The risk assessment must be completed before the system/application goes live.

7) UCLA Health IT Security will develop and maintain SOPs for the risk assessment process.

EXCEPTIONS

Any exceptions from this standard must be approved by the UCLA Health Sciences Chief Compliance Security Officer in conjunction with the Chief Information Security Officer.

QUESTIONS

1) If you have questions on Risk Assessment forms and process, please contact the IT Security team (ITSecurityAll@mednet.ucla.edu).
2) If you have questions about this Standard, when a risk assessment is needed, or the Risk Assessment Approval process, please contact the Office of Compliance Services – Information Security (InfoSecAll@mednet.ucla.edu).

REFERENCES

HS Policy No. 9457, "*Minimum Security Standards*"

CONTACT

Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY

Created Date: May 18, 2019