UC Riverside, School of Medicine Policies and Procedures
Policy Title: Vendor Security Risk Management
Policy Number: 950-02-208

Responsible Officer:	Information Security Officer
Responsible Office:	SOM Office of Information Technology
Origination Date:	4/26/2022
Date of Revision:	
Scope:	Any vendor service, hardware, or software, or combination thereof, which may access (collect, create, store, maintain, process, transmit, receive, etc.) Institutional Information or IT Resources. Any authorized user or coordinator of vendor goods and/or services contributing to SOM business.

I. Policy Summary

UCR SOM utilizes vendor goods and services to support our mission and goals. Vendor relationships carry inherent and residual risks that must be addressed as a part of SOM due care and diligence. The cost, benefit, sustainability, and security risk of goods and services should be considered and addressed throughout the lifecycle of vendor relationships. This Policy outlines the requirements, supported by the *NIST Cybersecurity and Privacy Frameworks*, for how UCR SOM will conduct vendor information security due diligence, while bridging, clarifying, and expanding on *IS-3 Electronic Information Security* Sections 6: *Risk Management Process* and 15: *Supplier Relationships*, *BFB-BUS-43 Purchases of Goods and Services; Supply Chain Management* regarding Procurement Card Program, *UC Policy on Sustainable Practices, UC Health Care Vendor Relations* policy and SOM policy *950-02-005 Vendor Relations*. As stewards of UC resources, SOM must responsibly handle data and systems to holistically manage vendor security risk.

IS-3 simplifies the process of cyber risk management at a systemwide level and prepares UC for a world in which information security is increasingly critical.

Goals

1. *Preserve academic freedom and research collaboration.*
2. *Protect privacy.*
3. *Follow a risk-based approach.*
4. *Maintain confidentiality.*
5. *Protect integrity.*
6. *Ensure availability.*

Principles

1. *Policy goals guide decisions.*
2. *[SOM] is accountable for implementing information security.*
3. *Risk level determines the position that is assigned decision-making rights.*
4. *Security is a shared responsibility.*
5. *Security is embedded in the lifecycle of systems, services, and software.*

II. Definitions

Please refer to University of California Systemwide IT Policy Glossary.

III. Policy Text

SOM must contemplate the selection of and ongoing use of vendor goods and/or services with the intention of meeting all UC specifications, including during selection and procurement processes, and in meeting security and privacy requirements. Departments must address vendor security risk holistically, balancing cost, benefit, sustainability, and security risk of goods and/or services. This Policy reiterates the goal of reducing unnecessary purchasing and mitigating security risk throughout the lifecycle of vendor relationships. As a result, SOM will better meet the goals and principles of IS-3 and other vendor management policies.

A. Defining Need and Product Selection

When considering a vendor good and/or service to address an identified business need, it is important to define what Institutional Information and/or IT Resources are likely to be accessed throughout the full lifecycle of the relationship and plan to address risk accordingly. Vendor goods and/or services classified as essential to SOM operations should be included in response and recovery planning and testing.

Departments must leverage the resources available to understand information technology and services under consideration, including considering OIT/Security and Compliance as a partnership. For example, a vendor Privacy Policy review may be needed to better understand how the use of a website will constitute access to Institutional Information or IT Resources. It is an industry standard for equipment and software licensing to include technical support services which are likely to constitute access to Institutional Information and/or IT Resources. Even the process of testing software, such a conducting a Proof-Of-Concept[1] to evidence vendor selection, constitutes a measurable degree of security risk to consider and manage. If a viable solution posed requires resources from other departments, departments must communicate, and negotiate where applicable, with each other for support and in defining roles and responsibilities; for example, OIT regularly hosts enterprise applications.

Notwithstanding other UC procurement requirements such as sole source justification, competitive bids, or RFQ/RFP, SOM must make compliance with security needs a minimum requirement. Select a vendor that meets compliance requirements, including security and privacy. Before engaging a vendor, make sure it is clear that they understand and have a plan for protecting UC. Vendors must be selected by considering a broad range of functional and performance capacities, including the ability to protect UC and to carry out vendor

[1] Proof-of-Concept is a demonstration to verify that certain technologies have the potential for real-world application. It represents the evidence demonstrating that a project or product is feasible and worthy enough to justify the expenses needed to support and develop it.

responsibilities. SOM must include security planning in the entire solution lifecycle. For example, a vendor that cannot evidence the adoption of formalized information security practices should not be trusted with handling sensitive data.

Being proactive in Contract Management through an early and upfront discussion with vendor on security and compliance requirements will help alleviate delays in procuring goods and/or services. Purchasing departments should engage the vendor to prepare all the necessary security, compliance, and privacy review documents. For example, vendors should be made aware early about use case(s) and Service Delivery needs and partnering departments may have tools available to support communication (e.g., Intake Form).

B. Service Delivery

Vendors play an important role in protecting UC's Institutional Information and IT Resources. When selecting and working with vendors, it is important to manage cybersecurity risks related to that vendor and the anticipated use case(s).

1. Contract Management

Procurement and continued use are both dependent on having an active contract. SOM must include the proper agreements and appendixes in agreements. Vendor contracting plans must include the appropriate documents and appendices to ensure security, compliance, and privacy. UC Terms and Conditions include many potentially applicable elements. Appendix Data Security (Appendix-DS) is required whenever a vendor accesses, collects, processes, or maintains Institutional Information. It is also required when a vendor accesses and/or provides IT Resources. Other types of appendices may be necessary for specific cases, including BAA (Business Associate Agreement), GDPR (General Data Protection Regulation), or Cloud Services, among others. If procuring through a reseller is the only method of acquiring a good and/or service, an underlying agreement directly with Original Equipment Manufacturer[2] is best practice and may be required to address the implementation of UC Procurement requirements.

Handling Unmodified Vendor Contracts

Some vendors are unwilling to negotiate or evidence following information security practices. These circumstances are often encountered when software or equipment is available Online and the vendor accepts only Credit Card as payment. Low value purchases do not necessarily constitute low risk when vendor may access Institutional Information or IT Resource(s). These vendors typically require users to hold them harmless and are not incentivized to adhere to information security best practices or legal requirements. Between industry standard practices being described as a risk to national defense and potential noncompliance with IS-3, these

[2] Original Equipment Manufacturer (OEM) is a company whose goods are used as components in the products of another company, which then sells the finished item. The second firm is referred to as a value-added reseller (VAR) because by augmenting or incorporating features or services, it adds value to the original item. The VAR works closely with the OEM, which sometimes customizes designs based on the VAR company's needs and specifications.

situations should be handled with a heightened level of care and diligence. Circumstances where the vendor will largely not meet UC requirements are more likely to require exceptional approval and will require due diligence to remain in compliance with underlying goals and objectives. An evaluation of security risk should be weighted heavily when balancing cost, benefit, sustainability, and security risk.

2. **Using Products and Services**

   As many vendors are likely to access Institutional Information and/or IT Resources and SOM regularly handles sensitive data, due diligence and due care consistent with risk must be observed to prevent and detect unauthorized access. When applicable, vendors must be notified of terminated and transferred employees and users, with the intention of removing access immediately. Vendor systems considered essential to SOM business must be clearly documented and included in response and recovery planning and testing.

   Service Handling

   Users must not provide vendor access to Institutional Information (e.g., PHI, PII) or IT Resources without specific direction otherwise. Vendor services, such as providing technical support, must be documented and recorded as evidence in the case of security incident or breach.

   Using Technology

   Users must not process sensitive data in software without specific direction otherwise. Software must be configured and used securely and in accordance with IS-3 and supporting standards, legal, export control, and contractual or other policy requirements. Software to support SOM business should be used in accordance with SOM policy *950-02-207 Bring Your Own Device*. For example, role-based access and single sign-on should be implemented whenever possible, configuration through MDM (Mobile Device Management) program, access vendor web applications securely (e.g., via OIT provided virtual desktop infrastructure or in the office), or other added safeguards or restrictions may be necessary based on risk assessment or as directed by ISO.

3. **End Of Relationship**

   SOM must prepare for the eventual end of vendor relationships. Renewal periods are an opportunity to resolve contractual falters and create the potential for relationship end. If a vendor provided an essential service or accessed sensitive data, additional diligence may be necessary. The standard implementation of the Appendix-DS outlines appropriate requirements for disposal of Institutional Information at the end of agreement; acquiring vendor certification or attestation of proper disposal of Institutional Information is a best practice. Any essential services or data must be replaced or acquired before the end of an agreement.

IV. Responsibilities

A. User

Handle vendor relations with due care.

- Seek direction from department management about appropriate vendor access and software use, for example in complying with a vendor Acceptable Use Policy. By default, sensitive data should not be provided to vendors or entered into software. Never share UC credentials with anyone for any reason.
- Vendors not operating as independent contractors may not be left unattended with access to non-public Institutional Information or IT Resources without expressed authority permission.
- Promptly report any vendor suspicious activity or abnormal behavior.
- Comply with other department expressed requirements and published procedures (e.g., supporting procedures, BYOD specifications, supervisor directives, etc.) to facilitate this or other policy, law, or contractual requirement, including in supporting the implementation of identified security controls.
- Access or use vendor-hosted web-based applications via OIT-provided virtual infrastructure or in the office on business equipment to limit vendor access to user personal data. Employ CCPA-afforded protections to limit cookies and delete user data whenever available and when operationally feasible.
- Whenever available, vendor mobile applications should be accessed or used via MDM.

Reasonably prevent specific prohibited vendor activity:

- Share passwords or authentication secrets that provide access to Institutional Information or IT Resources.
- Use passwords or other authentication secrets that are common across customers or multiple unrelated UC sites.
- Create backdoors or alternate undisclosed access methods for any reason.
- Access systems when not authorized to do so.
- Make unauthorized changes.
- Reduce, remove, or turn off any security control without approval from ISO (e.g., anti-virus exceptions).
- Create new accounts without approval from an appropriate authority.
- Store, harvest or pass-through UC credentials (username, password, authentication secret or other factors).
- Use or copy Institutional Information for non-authorized purposes.

Procedures when receiving vendor technical support remotely:

1. Close all applications not needed by vendor before beginning support session.
2. Record support sessions and store in department folders with file name: [YYYY]-[MM]-[DD]_[approximate military timestamp 00:00]_[your netid]_[Vendor/Product]
3. Report occurrence of support session to supervisor and OIT.

Procedures when receiving vendor support in-person:

1. Observe a clean desk protocol, meaning sensitive data in physical form should be put away and not visible to unauthorized personnel.
2. Supervise vendor representatives and continuously monitor for suspicious behavior or unauthorized access. For example, diagnostic logs from software or equipment are considered Institutional Information and may contain sensitive data.
3. Follow other policies and requirements for vendor handling, such as SOM policy 950-02-005 Vendor Relations and SOM policy 950-02-008 *Observers and Vendors in Clinical Areas*.
4. Report occurrence of support session to supervisor and OIT.

B. Department Management (Head, FAO, Supervisors)

Handle vendor relations with due care and due diligence.

Defining Business Need, Selecting a Product, and Managing Contracts

1. Solicit a work order (e.g., quote, SOW) and agreement from vendor as appropriate, keeping in mind maintaining compliance with all Finance and Administration policies (e.g., *BFB-BUS-43 Purchases of Goods and Services; Supply Chain Management*).
2. Employ a least privilege approach to define what is authorized use of and vendor access to Institutional Information and/or IT Resource(s). By default, access to Institutional Information and/or IT Resource(s) should not be provided to vendors unless permitted in contract.
3. Ensure that the vendor will agree to the UC T&Cs and Appendix-DS and BAA where appropriate.
4. Consult and partner with departments supporting this Policy to meet compliance requirements including reviewing published documentation from supporting departments.
5. Comply with other department expressed requirements and published procedures (e.g., supporting procedures, department specific, etc.) to facilitate this or other policy, law, or contractual requirement, including in supporting the implementation of identified security controls.

Security Authorization of Procurement Card or non-purchase use of good and/or service

1. Vendor must be providing a product classified as Commercial-Off-the-Shelf Software[3] and an alternative non-exceptional vendor product is not available or suitable.
2. Vendor has rejected agreement to UC procurement requirements or significantly fails to comply with IS-3 Section 15. Rejection can be determined through an affirmative response or clear and evidenced lack of cooperation. An example is a refusal to accept a Purchase Order.
3. Do not process or store sensitive data in the software or provide vendor access to non-public data.

[3] Commercial-Off-the-Shelf Software is software and hardware that already exists and is available from commercial sources (NIST SP 800-161).

- Generally, sensitive data is classified under IS-3 as P3 or P4 and examples of this include data protected by HIPAA, PCI, GLBA, FERPA, and data sets of PII. Users must be made aware of any potential breach via inappropriate access to or disclosure of protected data (e.g., unauthorized vendor access or data transmission). Consider following a standard documented practice of deidentification if human-related data should be processed in software. A recommended practice is to involve an OIT representative as supporting supervision when receiving vendor technical support. When in doubt about data sensitivity, you must seek guidance from an appropriate authority prior to disclosure (e.g., Compliance, OIT/Security teams).

4. Collaborate with authorities to maintain information security and privacy and keep in mind that exceptional approval may be rescinded at any time; authorities may take unilateral action to remove risk if necessary. These exceptional uses are more likely to be subject to audit for compliance with this policy.

Using Vendor Products and Services

1. Ensure that SOM use of vendor complies with policy, contract, legal requirements, security risk assessment recommendations or authority directives where appropriate, including instructing users as appropriate.

   Configure and use software securely and in accordance with IS-3 and supporting standards.

   - This includes adhering to the following security requirements: *UC Minimum Security Standard*, *UC Secure Software Configuration Standard*, *UC Account and Authentication Management Standard*, *UC Electronic Communications Policy*, and other SOM security policies or ISO requirements. When in doubt about adherence, you should seek guidance from an appropriate authority (e.g., Compliance, OIT/Security teams) to determine reasonable and appropriate configuration; for example, you may need to collaborate with OIT to ensure that security patches are applied monthly, mobile applications are managed via MDM, and Single Sign-on is configured.

   Review the applicable vendor agreement, (e.g., Licensing) and any supporting agreement or vendor policy, and implement operational controls as appropriate.

   - If the agreement allows for unilateral changes, responsible parties must review for updates at least annually. Users should be made aware of and held accountable to adhere to procedures as a part of their job requirements under IS-3, such as software being loaded onto only a single computer or to adhere to a vendor Acceptable Use Policy. Acknowledgement and adherence to this requirement can be shown through a DocuSign agreement by these parties and supporting department procedural documentation. When in doubt about contract implications, you should seek guidance from an appropriate authority (e.g., Compliance, OIT/Security, Business Operations, or Business Contracts/Procurement teams); for example, references to jurisdiction, arbitration, liability, and others may need input from relevant legal experts.

2. Include vendor goods and/or services in security incident response and recovery planning and testing to ensure confidentiality, integrity, and availability as appropriate.
3. Oversee vendor operations to ensure that representatives comply with all applicable UC policy, contract, and legal requirements. Conduct and maintain inventory of vendor access to Institutional Information and IT Resources, maintaining detailed records of vendor identified access and support sessions to evidence continued appropriate care; this should include creating and maintaining data inventory to support and justify data classification. Report incidents of unauthorized vendor access. Submit to appropriate authority vendor attestation of proper disposal of Institutional Information when vendor maintained sensitive data.
4. Maintain records of software licensing assignment, ideally by user and equipment. Software licensing belongs to UC and departments act as custodians. For example, perpetual licensing should be treated as a CapEx asset owned by SOM.

C. Central Procurement (i.e., Buyer)

1. Delegated authority to bind vendor contracts.
2. Ensures that purchases and agreements meet UC procurement and contracting requirements.
3. Coordinates with ISO and campus Information Security to process exceptions to IS-3 as needed, such as when the Appendix-DS cannot be implemented.

D. Business Operations (and Departments with Procurement Card authority)

1. Designate to coordinate with Central Procurement to process contracts and agreements.
2. Acquire necessary purchasing pre-approvals in accordance with Central Procurement and SOM protocols. Consult published documentation from other departments (e.g., Compliance BAAs, OIT Authorized Software and Standard Equipment).
3. As outlined under the UCR/UC policy, ensures that all Procurement Card transactions are processed in accordance with policy and relevant protocols. Coordinates with and/or routes procurement requests to ISO to ensure proper security review is completed.

E. Office of Information Technology (OIT)

1. Partner with departments in Defining Need and Product Selection, in secure software configuration, and consult on resource needs or commitments. Provision and manage technical resources to support software as appropriate, including testing (e.g., Proof-of-Concept, security testing, etc.).

2. Support department efforts in and coordinate data and system classification. Facilitate periodic security risk assessment in accordance with ISO specifications.
3. Implement and manage relevant software security controls, key controls:
    - Privilege Access Management
    - Network Segmentation and Monitoring (Network-based)
    - Network Connection Restrictions and Monitoring (Host-based)
    - Vulnerability and Configuration Management
    - Virtual Desktop Infrastructure
    - Mobile Device Management (MDM)
4. Maintain a log of vendor technical support sessions.
5. Publish lists of standard equipment and of authorized software (including software-as-a-service), ideally indicating authorized users, type or category, and specified security requirements.
6. Monitor access to Institutional Information and IT Resources for compliance with legal requirements, contractual obligation, applicable policy, and security incident and remove or block access to unauthorized software as needed.

F. Information Security Officer (ISO)

1. Provide security consultation when departments are selecting vendors and support departments to collect necessary information for security review.
2. Review and approve vendor security plans and conduct vendor risk assessments in accordance with IS-3 Sections 6 and 15.
    - Vendor risk assessment should typically be scoped to intended use with the purpose of expanding risk visibility, including communicating about and mitigating security risk. As a general guide for processing, verified P1 and P2 data and system classification requires no or minimal risk assessment, relying on other Policy requirements, whereas P4 requires extensive effort and may include consideration of 4th-party risk. When relevant third-party certifications are unavailable, vendor attestations about security risk management and incident response practices may be relied upon. Perform non-intrusive software security testing where appropriate. The focus should be on improving visibility into the risk, adding controls to reduce said risk, and on ways to reduce the scope, penetration, and access to acceptable levels.
3. Consult and partner with departments to ensure that appropriate security language is included in contracts, including coordinating with Proprietors to verify data classification and law in Appendix-DS Exhibit 1, in accordance with *UC Institutional Information and IT Resource Classification Standard.*
4. Designate to coordinate with Buyer to process redlines to Appendix-DS and/or verify security language included in contracts is appropriate.

5. Oversee the processing of SOM exceptions to IS-3, including Section 15 requirement to include Appendix-DS or comparable security language in contracts.
6. Consult and coordinate with campus Information Security and Export Control as appropriate.

G. Chief Compliance and Privacy Officer

1. Consult with departments about privacy and billing issues.
2. Support the identification of data classification and law in agreements (e.g., Appendix-DS Exhibit 1). Where appropriate, assess processes of deidentification to reduce data classification. This may include reviewing vendor Privacy Policy if requested.
3. Determine whether vendor qualifies as Business Associate under HIPAA/HITECH.
4. Process exceptions to the BAA requirement.
5. Maintain a list of known SOM authorized Business Associates, thus indicating that PHI may be disclosed if appropriate.
6. Audit for compliance with IS-3 and other applicable policy and prepare sanctions for non-compliance as appropriate.
7. Serve as security incident and breach contact in vendor agreements.

Chief Compliance and Privacy Officer
951-827-4672
compliance@medsch.ucr.edu
UC Riverside School of Medicine
14360 Meridian Parkway, UCPath Center
Riverside, CA 92518

V. References

UC Systemwide Information Security Policies and Standards (ucop.edu)

UC Systemwide IT Policy Glossary (ucop.edu)

BFB-IS-3: Electronic Information Security (ucop.edu)

UC Systemwide Information Security Resources (ucop.edu)

UC Procurement Forms & Policies (ucop.edu)

BFB-BUS-43 Purchases of Goods and Services; Supply Chain Management (ucop.edu)

Sustainable Practices (ucop.edu)

Business Contracts | Procurement (ucr.edu)

Policies & Procedures | School of Medicine Compliance (ucr.edu)

NIST Cybersecurity Framework, Version 1.1 (nist.gov)

NIST Privacy Framework, Version 1.0 (nist.gov)

NIST SP 800-161 Supply Chain Risk Management (nist.gov)

Approvals:

Compliance Committee (04/26/2022)

Paul Hackman Digitally signed by Paul Hackman
Date: 2022.05.09 10:42:42 -07'00'

05/09/2022

Paul Hackman, J.D., L.LM.
Chief Compliance and Privacy Officer,
School of Medicine

Date

Deborah Deas Digitally signed by Deborah Deas
Date: 2022.05.09 11:15:16 -07'00'

05/09/2022

Deborah Deas, M.D., M.P.H
Vice Chancellor, Health Sciences
Dean, School of Medicine

Date