University of California
San Francisco
advancing health worldwide

UCSF Security Exception Request Form Instructions

Security Exception Requests are required for any devices that do not meet UCSF Minimum Security Standards[1].

- Security exceptions are only valid for a maximum of 12 months
- Security exception can be renewed after 12 months if extenuating circumstances still require being out of compliance with UCSF policy. Renewal requests will require more compensating controls (ways to minimize risk) and a higher level of scrutiny will be applied.
- Separate Requests should be filed for sets of devices serving different functions.

Why would someone need to file for an IT Security Exception?

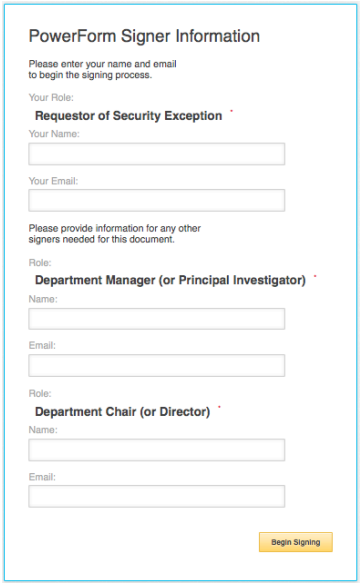
The Security Exception Request Form[2] is designed to sufficiently document any risks, along with relevant compensating controls, associated with not meeting UCSF Minimum Security Standards[1]. In the event of an audit, either by an internal entity or an external one (e.g., Office of Civil Rights, or Health and Human Services), this documentation is used to demonstrate due diligence on ensuring UCSF data is kept safe and secure.

Recent compliance fines levied against the University have been substantial and resource intensive to remediate. Having all the information requested in the Security Exception Request Form[2] assists the University with minimizing any impacts that may be caused by an audit, and more importantly, provide the institution sufficient insight into our environment to reduce the likelihood of a security incident and/or security breach.

The UCSF Minimum Security Standards Checklist[6] (worksheet) can be also used to determine if a device requires a Security Exception.

Who needs to fill out the Security Exception Request Form[2]?

The Security Exception Request Form[2] should be filled out by the resource owner, proprietor, or custodian of the devices(s) as defined by UC IS-2 Policy[7]. This person, along with their Manager and Director, take responsibility of any risks associated with putting the device(s) on the network.


PowerForm Signer Information

Please enter your name and email to begin the signing process.

Your Role:
Requestor of Security Exception *
Your Name:
Your Email:

Please provide information for any other signers needed for this document.

Role:
Department Manager (or Principal Investigator) *
Name:
Email:

Role:
Department Chair (or Director) *
Name:
Email:

Begin Signing

To begin, follow the 'Security Exception Request Form'[2] link found on the UCSF Minimum Security Standards[1] web page. This will take you to a webform on the Docusign website labeled 'PowerForm Signer Information'.

Enter the name and email addresses of 3 different individuals in a Department that will fill out, review, and sign the form.

1. Requestor – typically the service owner of the device
2. Manager, or Principal Investigator, of the Requestor
3. Department Chair, MSO, or Director, of the Requestor

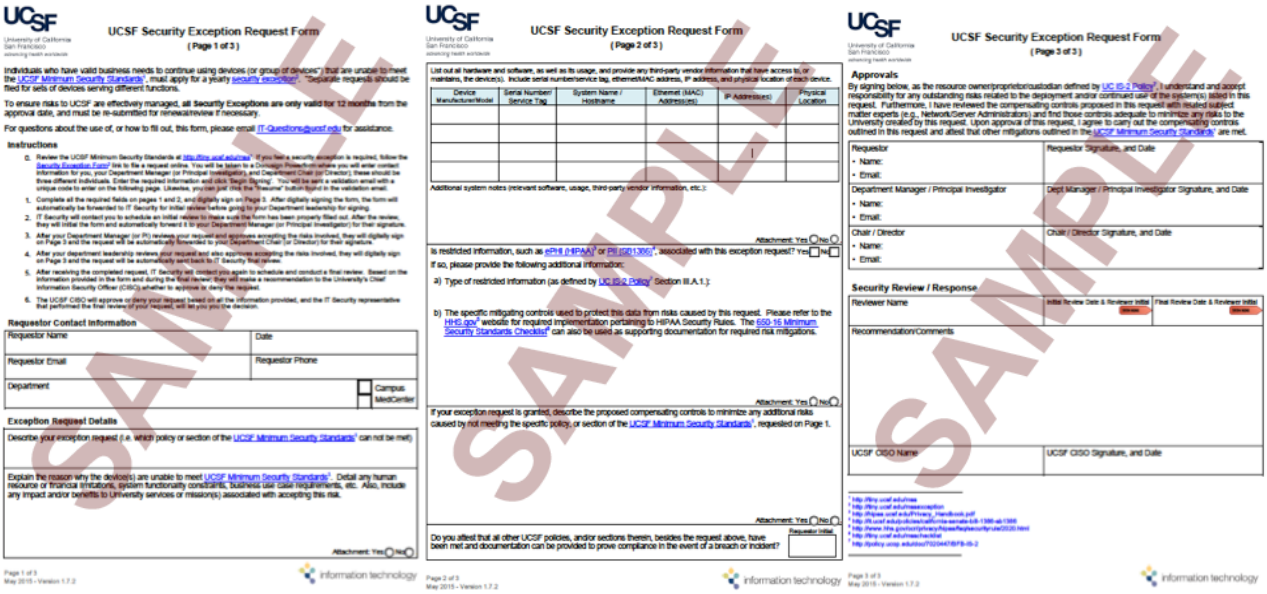
Note: Please make sure to enter the name and e-mail address of the individual as they appear in the UCSF Directory.

UCSF Security Exception Request Form Instructions

After entering the necessary names and e-mail addresses, and clicking on the 'Begin Signing' button, the Requestor will receive an email address from "UCSF Security sent by Docusign System" (security@ucsf.edu) with instructions on how to access the actual form on the Docusign website to begin filling out the form.

Note: The Requestor will need to complete the form and receive all necessary approvals within 30 days before the form auto-expires. If the form expires before all approval signatures are obtained, a new request must be initiated.

While filling out the form, if you have to stop and continue at a later time, click on the 'More' button at the top of webpage and select 'Finish Later' to save you progress.



What information is required to fill out a Security Exception Request Form[2]?

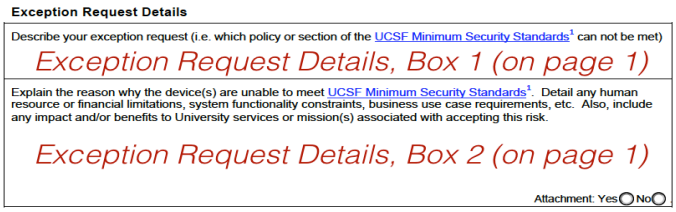
Note: **Every section and field on the Security Exception Request Form[2] is mandatory.**

On the first page, under 'Requestor Contact Information', the Requestor's name, Email address, and the date the request was initiated, should already be auto-filled. Complete this section by entering your University phone number and Department, and then selecting "Campus" or "MedCenter" based on the funding source of the device(s) listed under this request.

The next section, 'Exception Request Details', contain 6 different boxes asking for 6 sets of information necessary to sufficiently document the risks and mitigations involved.

The Requestor, Manager/MSO/PI, and Department Chair/Director, should consult with any related subject matter experts to properly obtain all information necessary to fill out the this section. Related subject matter experts can include, but not limited to: Server Administrators, Web Designers, Application Programmers, 3rd Party vendor Engineers, Network Administrators, etc.

UCSF Security Exception Request Form Instructions



Box 1. 'Describe your exception request':

This section is asking which UCSF (or UC) policy are you asking that these devices be exempted from. Typically, this will be a specific requirement found under the UCSF Minimum Security Standards[1] that the device(s) cannot meet.

The UCSF Minimum Security Standards Checklist[6] (worksheet) can be used to determine what should go in this box. Anything marked 'No' on the checklist, should be listed in this box.

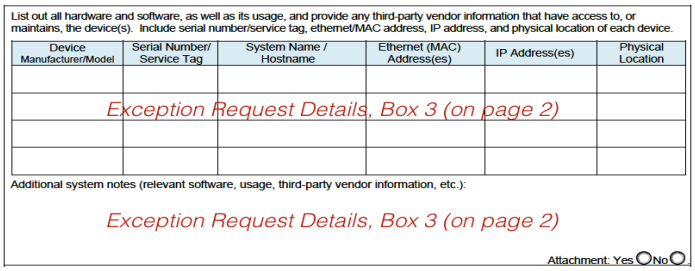
Box 2. 'Explain the reason why the device(s) are unable to meet UCSF Minimum Security Standards[1]…' [Box 2 on Page 1]:

This section is asking for your justification for being exempted from having to comply with UCSF Minimum Security Standards[1]. Justifications can include (but not limited to):

- Financial constraints (how much would it cost to replace the system to meet University standards? Is that amount greater than any fines/fees/losses the University may incur in the event of the device(s) being compromised, hacked, or stolen?)
- Human resource constraints (is your department short staffed and require additional time to meet compliance?)
- System functionality constraints (e.g. the vendor of the application or device cannot meet UCSF Minimum Security Requirement and will make a compliant version available in the future; official vendor documentation is required)
- Business use case requirements (e.g. devices are used for academic enrollment that and are require critical availability between July-August so your department will take care of compliance issues after that time).
- Impact and/or benefits to the University services or mission

You can also attach any supporting documentation (such as vendor release notes) by selecting 'Yes' next to "Attachment". Additionally, if you need more space than what is provided on the form, you can use the attachment to attach a Word document with further details.

Box 3. 'List out all hardware and software, as well as its usage, and provide any third-party vendor information…' [Box 3 on page 2]



List out all hardware and software, as well as its usage, and provide any third-party vendor information that have access to, or maintains, the device(s). Include serial number/service tag, ethernet/MAC address, IP address, and physical location of each device.

Device Manufacturer/Model	Serial Number/ Service Tag	System Name / Hostname	Ethernet (MAC) Address(es)	IP Address(es)	Physical Location

Exception Request Details, Box 3 (on page 2)

Additional system notes (relevant software, usage, third-party vendor information, etc.):

Exception Request Details, Box 3 (on page 2)

Attachment: Yes ○ No ○

This section has 2 parts: 1) a table to provide specific system information of each and every device, and 2) a field to enter 'Additional system notes' about the device(s).

If you are not a technical person, you should consult your system administrator, computer support coordinator, or the IT Service Desk for assistance in gathering this information. Again, every field is required.

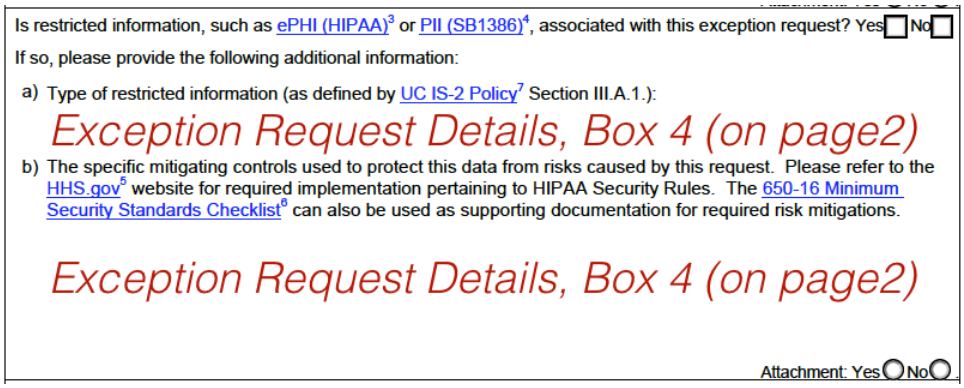
- A table for system(s) information of each and every device:
  - Device Manufacturer/Model - (e.g. 'Dell Optiplex GX240', or 'VM')
  - Serial Number/Service Tag - This is typically found on a sticker attached to the device itself. If this is a VM, please just write "VM".
  - System name / hostname
  - Ethernet (MAC) Address(es) – Every network device has a unique ethernet address (wired or wireless)
  - IP Addresses
  - Physical Location (USPS or University Address, with Room #)

  If your request includes more than 4 devices, you can also attach a document (Excel file) that provides the same information for each of the devices by selecting 'Yes' next to "Attachment".

- Under 'Additional system notes', include usage information as well any other relevant information such as (but not limited to):
  - any dependent software/application causing the need for a security exception
  - any 3rd party vendor that maintains, or has access to, the device(s)

  Additionally, if you need more space than what is provided on the form, you can use the attachment to attach a Word document.

Box 4. 'Is restricted information associated with this exception request?' [Box 4 on Page 2]:


Is restricted information, such as ePHI (HIPAA)[3] or PII (SB1386)[4], associated with this exception request? Yes ☐ No ☐

If so, please provide the following additional information:

a) Type of restricted information (as defined by UC IS-2 Policy[7] Section III.A.1.):

Exception Request Details, Box 4 (on page2)

b) The specific mitigating controls used to protect this data from risks caused by this request. Please refer to the HHS.gov[5] website for required implementation pertaining to HIPAA Security Rules. The 650-16 Minimum Security Standards Checklist[6] can also be used as supporting documentation for required risk mitigations.

Exception Request Details, Box 4 (on page2)

Attachment: Yes ○ No ○

A more thorough explanation of 'restricted information' can be found in the UCOP IS-2 Policy[7] Section III ('Inventory and Classification of Electronic Information Resources').

Restricted information can include (but not limited to):

- ePHI (HIPAA)[3]
- PII (SB1386)[4]
- FERPA (Family Educational Rights and Privacy Act)
- PCI (Payment Card Information)
- Intellectual Property

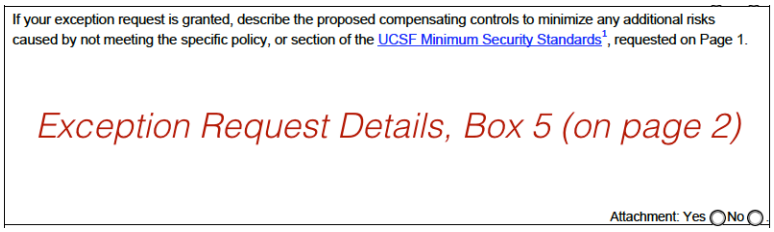
If any of the devices listed in section 3 store or handle the above information, please select 'Yes' and list the type(s) of restricted information under 'a)'.

Under 'b)', list any mitigating controls (ways to minimize risk) used to protect the data listed under 'a)'. This could include encryption at rest, encryption in motion, restricting access to within the UCSF network only through hardware firewalls, etc.

Typically you would employ multiple mitigating controls simultaneously to cover various attack vectors that may be used to compromise the data. Mitigating controls listed under this section should specifically address protecting the data listed under 'a)', additional mitigating controls should be documented under Box 5.

You can also attach any supporting documentation (such as vendor release notes), by selecting "Yes"' next to 'Attachment". Additionally, if you need more space than what is provided on the form, you can use the attachment to attach a Word document.

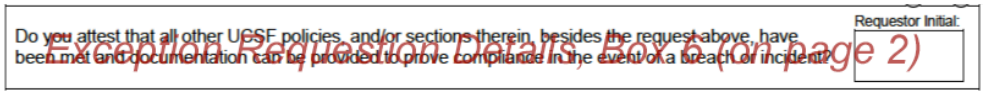
Box 5. 'If your exception request is granted, describe the proposed compensating controls to minimize any additional risks…'



This section is separate from '4.b)' in that this is specific to compensating controls to minimize the risk to the systems caused by the item(s) you listed in 'Section 1' above. List any and all controls used to protect the physical device(s) itself, the data stored on the device(s), and information transmitted to/from the device(s).

If you are unsure what compensating controls are available, or already implemented, for the device(s), please consult with your system administrator, computer support coordinator, or the IT Service Desk.

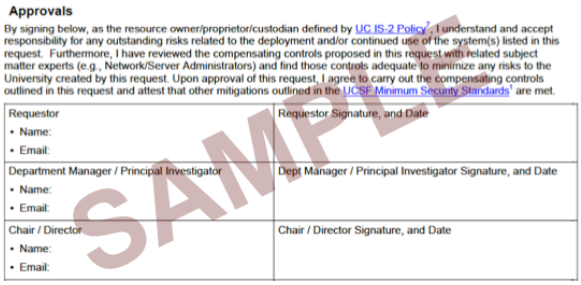
Box 6. 'Do you attest that all other USCF policies, and/or sections therein, besides the request above, have been met…' [Box 6 on Page 2]



This attestation records that, besides the items listed in 'Box 1', the devices listed under this request meet all other UCSF Minimum Security Standards[1] (i.e. the other items listed in the UCSF Minimum Security Checklist[6] can be marked 'Yes').

Who needs to approve this request?

- Departmental approval (3 different individuals accepting responsibility, including any financial repercussions, for the risks associated with the request)



  - Requestor
    - After the Requestor has signed their own request, an IT Security Reviewer will conduct an initial review to ensure all fields in the form have been sufficiently completed and initial the form; the document will then be automatically forwarded to the next approver for their review and signature.

- Department Manager, or MSO, or Principal Investigator
  - After the Requestor's Department Manager, MSO, or Principal Investigator has reviewed and signed the form accepting responsibility for risks associated with the request, the document will be automatically forwarded to the next approver for their review and signature.
- Department Chair, or Director
  - After the Requestor's Department Chair or Director has reviewed and signed the form accepting responsibility for risks associated with the request, the document will be automatically forwarded to the next approver for their review and signature.

• UCSF IT Security

- IT Security Reviewer
  - Upon receipt of all necessary Departmental signatures, the IT Security Reviewer will contact the Requestor to conduct a final review.
  - The IT Security Reviewer ensures sufficient justifications commensurate with the risk associated with the request, as well as sufficient compensating controls to minimize any risk(s) associated with the request, are documented within the form.
  - Any additional information provided during the final review, as well as a recommendation for approval or rejection, will be passed onto UCSF's Chief Information Security Officer (CISO) for final approval.
- Chief Information Security Officer (CISO)
  - The UCSF CISO will review all information provided on the form to determine if due diligence has been met in ensuring UCSF's data and its assets are kept safe and secure.

After the University CISO has approved and signed the request, the Requestor and their Department leadership take responsibility for ensuring any compensating controls documented in the request are implemented and continue to operate as intended during the duration of the Security Exception's validity (typically 12 months or less). If any information documented within the request form changes at any time during the Security Exception's validity, the exception becomes invalid and a new request should be filed to ensure UCSF data is kept safe and secure.

[1] http://tiny.ucsf.edu/mss
[2] http://tiny.ucsf.edu/mssexception
[3] http://hipaa.ucsf.edu/Privacy_Handbook.pdf
[4] http://it.ucsf.edu/policies/california-senate-bill-1386-sb1386
[5] http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2020.html
[6] http://tiny.ucsf.edu/msschecklist
[7] http://policy.ucop.edu/doc/7020447/BFB-IS-2