**Date of Request:** *{MM/DD/YYYY}*

# **Contact Information:**

|  |
| --- |
| **Requestor Name:***{First Name and Last Name}* |
| **Requestor Contact Information**: *{Enter phone and email address}* |
| **Unit Name**: *{Select Unit}* |
| **Unit Head**: *{First Name and Last Name}* |
| **Unit Head Contact Information**: *{Enter phone and email address}* |
| **Unit Information Security Lead (**[**UISL**](https://security.uci.edu/isc.html)**)**: *{First Name and Last Name}* |
| **UISL Contact Information**: *{Enter phone and email address}* |
| **Additional Stakeholders**: *{Enter any additional key stakeholders and their contact information}* |

# **Exception Request Summary:**

|  |  |
| --- | --- |
| **Summary of Exception Request:** *{Summarize and provide details about the exception request that you are making.}* | |
| **Exception Expiration Date:** *{List out how long you need this exception and the date the exception will be needed until. Max 1 year}* | |
| **Why is this Exception Request needed:** *Describe any benefits/advantages or challenges it brings to the Campus or Unit.* | |
| **Security Risks with Accepting Exception:** *{List out the security risks this exception is exposing to the Campus or Unit.}* | |
| **Proposed/Current Compensating Controls to Mitigate Risks:** *{Describe any compensating controls that are in place or that will be implemented to mitigate the risk associated with this exception}* | |
| **Original Risk:** *{Select Risk Level}* | **Residual Risk:** *{Select Risk Level}* |
| **Additional Comments:** | |

# **Institutional Information & IT Resource Information:**

|  |
| --- |
| **Type of Institutional Information Impacted:** *{Describe the type of data that is being impacted by this request. For example, student information, research data, SSNs, financial records, etc.}* |
| **Highest** [**Protection Level**](https://security.uci.edu/security-plan/plan-classification-protection.html#P1) **Impacted:** *{Select a Protection Level}* |
| **Impacted IT Resource(s)**: *{Describe the IT Resource(s) impacted by this request}* |
| [**Availability Leve**l](https://security.uci.edu/security-plan/plan-classification-availability.html): *{Select an Availability Level}* |
| **Summary and Purpose of IT Resource(s)**: *{Summarize the description, function, and purpose of the impacted IT Resource(s)}* |

***\*\*\*Please reference*** [***Appendix A***](#_Appendix_A:_Impacting) ***to review Impacting Security Policies and Standards\*\*\****

# **OIT Security Analysis:**

The CISO or designate will review the exception and determine if the request is granted to move forward for Unit acceptance. The CISO will identify the risk accepter, who is a Unit Head with the level of authority that matches the risk identified. The identified Unit Head determines unit acceptance which includes acceptance of risks and potential financial loss in the event of a security incident.

- The exception request is granted as submitted, Initial: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- The exception request is granted subject to limitations, Initial: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- The exception request is rejected, Initial: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| **Limitations or stipulations:** *{Security notes any requirements, limitations or stipulations on granting the exception. Link to other documents if needed}* |
| **Rejection explanation:** *{Security explains why the request was rejected. Link to other documents if needed}* |
| **Additional Comments:** |
| **Effective date:** *{Security - When does the exception begin or take effect?}* |
| **Expiration date:** *{Security - When does the exception expire?}* |

|  |  |  |
| --- | --- | --- |
|  | | |
|  |  |  |
| Signature |  | Date |
|  |  |  |
| Printed Name |  | Title |

# **Unit and Responsible Officer(s) Risk Acceptance:**

I understand that compliance with UC {*and Location*} Information Technology policies and standards is expected for all Units (e.g., schools and departments), Institutional Information and IT Resources. I assert that the control(s) required by policies and standards cannot be implemented for the reason(s) documented in this form. My Unit accepts responsibility for the risks associated with this exception to information security policy. I also understand that this exception may be revoked by the Chief Information Security Officer and may be subject to follow-up by Internal Audit. My Unit understands and will adhere to all other requirements.

I understand that my Unit could be responsible for some costs incurred due to incidents related to the identified risks or my Unit may not be eligible for cyber insurance coverage if the agreed upon alternatives and compensating controls, plus other required controls, are not implemented and maintained.

|  |  |  |
| --- | --- | --- |
|  | | |
|  |  |  |
| Signature |  | Date |
|  |  |  |
| Printed Name |  | Title |

|  |  |  |
| --- | --- | --- |
|  | | |
|  |  |  |
| Signature |  | Date |
|  |  |  |
| Printed Name |  | Title |

|  |  |  |
| --- | --- | --- |
|  | | |
|  |  |  |
| Signature |  | Date |
|  |  |  |
| Printed Name |  | Title |

# **Appendix A: Impacting Security Policies and Standards**

|  |
| --- |
| **Impacting Policy and Standard Control(s):** *{List out the IS-3 Policy and/or Standard section(s) related to this request.* |