

[[RT #]] Security and Vulnerability Scan Report

# Scan Request Information

|  |  |
| --- | --- |
| RT # | [[The RequestTracker ticket number in the NETS\_Security RT queue being used to track this security review and vulnerability scan activities. To be completed by reviewer]] |
| Request and Report Date | [[Date review requested. To be completed by requestor]]  [[Date report created. To be complete by reviewer]] |
| Product or Service Under Review | Identify service, URL, hostname, application involved in this security review or scan request. To be completed by requestor. |
| Organization | University of Victoria |
| Administrative Authority | [[As defined in the UVic IT Security Operations Methodology.]]  Name:  Title:  Department:  Phone number:  Email: |
| System Provider and Support Contacts | [[The unit and leaders responsible for administering the impacted system(s) as defined in Policy IM7800. Include all emergency or support contacts in the event of unexpected outages, etc. to the services while reviewing or scanning. ]] |
| Review or Scan Requestor | Who has initiated this review or scan? Name contact and reason for request. E.g. Project Manager, Internal Audit, etc. |
| Information Security Analyst | [[As defined in the UVic IT Security Operations Methodology.]]  Name:  Title:  Supervisor:  Department:  Phone number:  Email: |
| Linkage |  |

Table of Contents

[1. Scan Request Information 1](#_Toc449961032)

[2. Scope of the Vulnerability Assessment or Review 3](#_Toc449961033)

[3. Summary of Recommendations 4](#_Toc449961034)

[4. Detailed Observations and Recommendations 5](#_Toc449961035)

[5. Vulnerability Mitigation and Reduction Activities 6](#_Toc449961036)

[Appendix A: Definitions of Likelihood and Consequence Matrix 7](#_Toc449961037)

[Appendix B – Supplemental Scan and Review Details 8](#_Toc449961038)

# Scope of the Vulnerability Assessment or Review

[[Identify clearly all aspects of service, host or application that will be considered in the review.

Is there a particular focus to the scan or review request? i.e. Components, new add-ons, etc.

Provide the reason for Scan: <Project or Ticket Request? Vulnerability Report or Exploit? Other?

Backup and recovery procedures or scheduling constraints

Does this scan require any backup and recovery procedures or scheduling constraints e.g. Out of business /peak hours?

Other considerations?]]

# Summary of Recommendations

[[Provide a brief bullet point list of the recommendations identified in next section (F).]]

# Detailed Observations and Recommendations

Note: Impact classification is based on grid at bottom of this section.

|  |
| --- |
| Observation #x |
| Finding |
|  |
| Impact |
| Extreme, High, Medium or Low - Explain |
| Recommendation(s) |
| 1.  2. |
| Client Response: (Date) |
|  |
| InfoSec Review Feedback: (Date) |
|  |

|  |
| --- |
| Observation #x |
| Finding |
|  |
| Impact |
| Extreme, High, Medium or Low - Explain |
| Recommendation(s) |
| 1.  2. |
| Client Response: (Date) |
|  |
| InfoSec Review Feedback: (Date) |
|  |

[[Insert copies of individual grids for any additional findings, as needed.]]

# Vulnerability Mitigation and Reduction Activities

1. Describe the immediate steps taken to address or reduce risks/issues identified:

|  |  |  |
| --- | --- | --- |
| Description | Completed By | Completion Date |
| 1. | <who> | <when> |
| InfoSec Review Comments: <to be completed by security analyst> |  |  |
| 2. |  |  |
| InfoSec Review Comments: <to be completed by security analyst> |  |  |
| 3. |  |  |
| InfoSec Review Comments: <to be completed by security analyst> |  |  |
| 4. |  |  |
| InfoSec Review Comments: <to be completed by security analyst> |  |  |

1. Describe long-term strategies to correct the situation (e.g. staff training, policy development, privacy and security audit, contractor supervision strategies, improved technical security architecture, improved physical security):

|  |  |  |
| --- | --- | --- |
| Description | Assigned To | Target Completion |
| 1. | <who> | <when> |
| 2. |  |  |
| 3. |  |  |

# Appendix A: Definitions of Likelihood and Consequence Matrix

|  |  |  |
| --- | --- | --- |
| Likelihood Rating | | |
| Level | **Descriptor** | **Description** |
| 5 | Expected | The risk is expected to occur one or more times in the next four (4) years |
| 4 | Probable | The risk is likely to occur at least once in the next four (4) years |
| 3 | Possible | It is possible that the risk could occur in the next four (4) years |
| 2 | Unlikely | The risk is unlikely to occur in the next four (4) years |
| 1 | Rare | There is a very remote chance the risk will occur – no notice of the risk manifesting itself elsewhere in the industry |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Consequence Matrix | | | | | | |
| Level | **Descriptor** | **Impact On[[1]](#footnote-1)** | | | | |
| **People (Staff)** | **Stakeholders** | **Mandate / Objectives** | **Financials** | **Reputation** |
| 5 | Catastrophic | Extreme impact on people resulting in a significant loss of personnel. Major business units will be adversely impacted. | Very significant loss to stakeholders, and will severely impact the long term relationship. | Risk will render UVic unable to achieve its overall objectives or mandate. | Critical (>$10M) net asset or revenue loss or >40% impact on business unit budget (revenue or expense). | Critical loss of trust/credibility. Significant media attention. UVic will be subject to inordinate increase in oversight. |
| 4 | Major | Major impact on people and will result in the loss of personnel. Could cause long term dissatisfaction amongst existing staff. | Somewhat significant loss to stakeholders, and could have a long term impact on relationship. | Significant impact on UVic’s and/or business unit’s ability to achieve its objectives. | Significant (>$2.5M) net asset or revenue loss or >30% impact on business unit budget (revenue or expense). | Significant loss of trust/credibility. Guaranteed to generate media attention and increased scrutiny. |
| 3 | Moderate | Moderate impact on people. Morale will be impacted. Loss of key personnel not expected. | Moderate impact on stakeholders, but without any significant long term consequences. | Moderately impacts UVic’s and/or business unit’s ability to achieve its objectives. | Significant (>$1M) net asset or revenue loss or >15% impact on business unit budget (revenue or expense). | Potential for lost trust/credibility. May generate some media attention and result in increased scrutiny. |
| 2 | Minor | Minor impact. Morale could be affected for a short period of time. | Negligible short-term impact on some stakeholders. | Minor impact on the business unit’s ability to achieve its objectives. | Minor negative financial impact for the business unit. | Could have minor impact on business unit credibility. No increase in scrutiny is expected. No media attention. |
| 1 | Insignificant | Little or no impact on people and likely very little awareness of the event. | No impact on stakeholders. | Little or no impact on the business unit’s ability to achieve its objectives. | Impact is within normal operating budget margin fluctuations. | No impact on reputation. |

Likelihood of Potential Harms and Consequence Grid

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Likelihood | Consequence | | | | |
| 1 | 2 | 3 | 4 | 5 |
| 5 | Medium | High | High | Extreme | Extreme |
| 4 | Low | Medium | High | High | Extreme |
| 3 | Low | Medium | Medium | High | High |
| 2 | Low | Low | Medium | Medium | High |
| 1 | Low | Low | Low | Low | Medium |

# Appendix B – Supplemental Scan and Review Details

[[Add to individual appendices any relevant diagrams, lists, logs, etc, as deemed relevant and necessary.]]

1. The consequences of a successful cyber-attack is most likely to be felt in impact to reputation (information breach), mandate/objectives (Denial of Service), and stakeholders (information breach). Impact on staff and financials is likely to be moderate or less and most likely attributed to costs and morale from having to respond to an information breach or an attack that causes widespread data integrity disruption. [↑](#footnote-ref-1)