

UCIT INFORMATION SECURITY STANDARDS

Vulnerability Assessment Standard

Classification IT Infrastructure Security	Table of Contents
Standard # ISS-011	Rationale 1 Scope 2 Definitions 3
Approval Authority Chief Information Officer	Standard 4 Exceptions 5
Implementation Authority Information Security Officer	Parent Policy 6 Related Policies & Standards 7
Effective Date May 11, 2009	History 8
Latest Revision Aug 25, 2009	

Rationale 1 To enable timely identification and mitigation of vulnerabilities and security flaws affecting computing devices within UofC's computing environment.

Scope 2 2.1 This standard applies to all UofC owned or managed servers and network devices connected to the UofC computing environment.

2.2 Subsequent releases of this standard will address:

- a. UofC owned or managed desktops, laptops and other mobile computing devices.
- b. Non-UofC owned or managed computing devices attempting to connect with the UofC computing environment.

Definitions 3 3.1 *Vulnerability*: a bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to the loss of confidentiality, integrity, or availability.

3.2 *Vulnerability Assessment Program (VAP)*: is a program to identify and address vulnerabilities, configuration issues and weakness in web applications, databases, networks, operating systems, and other software and hardware on the University of Calgary campus network. Further details can be found at www.ucalgary.ca/it/infosecurity

Standard	<p>4 4.1 Vulnerability Assessment Frequency</p> <p>a. In accordance with the Vulnerability Assessment program, all servers and network devices are subject to scanning on a monthly basis.</p> <p>b. New UofC owned or managed servers and devices are subject to a Vulnerability Scan prior to introduction to the UofC computing environment.</p> <p>4.2 Remediation</p> <p>All identified vulnerabilities must be remediated. Acceptable remediation activities include:</p> <ul style="list-style-type: none"> • Applying appropriate fixes and patches • Removing (or permanently disabling) the affected services, servers, or devices from the UofC computing environment. • Applying appropriate workarounds or alternate solutions <p>4.3 Remediation Timelines</p> <p>a. Vulnerabilities rated (in accordance with the VAP) as Critical must be addressed within 2 weeks after the initial discovery.</p> <p>b. Vulnerabilities rated a Severe and Moderate must be addressed within 30 days after the initial discovery.</p>																
Exceptions	<p>5 The CIO can approve exceptions to the above standard. Exception requests shall include detailed descriptions of:</p> <p>a. Why the proposed solution is being requested rather than following the standard.</p> <p>b. How the proposed solution varies from the standard.</p> <p>c. What are the implications for long term management of the variation.</p>																
Parent Policy	<p>6 Information Asset Security Monitoring Policy</p>																
Related Policies & Standards	<p>7 Information Asset Protection Policy</p>																
History	<table border="0"> <tr> <td>8</td> <td>Mar 10, 2009</td> <td>Patrick Jungles</td> <td>Initial Draft</td> </tr> <tr> <td></td> <td>May 11, 2009</td> <td>Dennis Tracz</td> <td>Revise content and format</td> </tr> <tr> <td></td> <td>Aug 25, 2009</td> <td>Patrick Jungles</td> <td>Minor revision</td> </tr> <tr> <td></td> <td>Nov 12, 2009</td> <td>Crystal Bourgeault</td> <td>CIO Approval</td> </tr> </table>	8	Mar 10, 2009	Patrick Jungles	Initial Draft		May 11, 2009	Dennis Tracz	Revise content and format		Aug 25, 2009	Patrick Jungles	Minor revision		Nov 12, 2009	Crystal Bourgeault	CIO Approval
8	Mar 10, 2009	Patrick Jungles	Initial Draft														
	May 11, 2009	Dennis Tracz	Revise content and format														
	Aug 25, 2009	Patrick Jungles	Minor revision														
	Nov 12, 2009	Crystal Bourgeault	CIO Approval														

