INFORMATION SECURITY GUIDELINE

Appropriate Notification Services

Introduction

1. Guidelines are issued by the Chief Information Officer to provide supplementary instructions or procedures on how to comply with the Information Security Standards. Compliance with guidelines is recommended but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.
2. As part of the vulnerability management process it is important to be notified of any new security issues around the products being used that could increase the probability of systems becoming compromised; the following resources are not meant to provide an exhaustive list but should provide assistance in keeping University IT Support Staff up-to-date on new vulnerabilities, so that appropriate steps can be taken to reduce risks to the affected systems.

Resources

US-CERT – United States Computer Emergency Readiness

- Current Activity - https://www.us-cert.gov/ncas/current-activity
- Alerts - http://www.us-cert.gov/ncas/alerts
- RSS Feed - http://www.us-cert.gov/ncas/alerts.xml

SANS

- NewsBites - http://www.sans.org/newsletters/#newsbites

Canadian Cyber Incident Response Centre (CCIRC)

- Cyber Security Bulletins (RSS Feed) - http://www.publicsafety.gc.ca/cnt/_xml/cybr-ctr-eng.xml

Public Safety Canada – Cyber Security Bulletins

- Alerts - http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/index-eng.aspx#al

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Vulnerability Management standard