a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #21
Requesting Variances from Information Security Standards

Introduction

1. In order to protect University information assets, the Chief Information Officer (CIO) has issued binding Information Security Standards. Academic and administrative units that wish to deviate from these Information Security Standards are required to request a variance from the CIO.
2. This document establishes the procedure for Administrative Heads of Unit to request such a variance.
3. The CIO has issued this document under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

Variance Request Procedure

4. Initial Request - the Administrative Head of Unit must submit the following information to information.security@ubc.ca:
    a. contact information;
    b. description of the requested variance and expected duration;
    c. explanation of why the variance is warranted;
    d. analysis of risk associated with granting the variance, and what controls will be in place to manage this risk; and
    e. analysis of cost and resource implications of granting the variance.
5. When considering the request for a variance, the CIO may seek the input of the Information Security Governance Committee (which is the Advisory Committee defined in Policy SC14) if he or she considers this appropriate.
6. The CIO may authorize a variance from the Information Security Standards in any of the following circumstances:
    a. the Administrative Head of Unit is temporarily unable to meet the compliance standard;
    b. compliance is not achievable for technical or financial reasons;
    c. an alternate method of compliance is available that offers equivalent or better security; or
    d. the variance is otherwise reasonable and is consistent with the Information Security Standards.
7. If the CIO approves a deviation, he or she will set out the terms of the variance, including any applicable mitigation requirements or other conditions.
8. If the CIO denies the requested deviation, he or she will provide an explanation and, if possible, a suggestion of alternatives.

Resolution of Disagreements

9. If a disagreement arises and cannot be resolved in a timely manner between the CIO and the Administrative Head of Unit with respect to the requested deviation, then either party may refer the disagreement to the Responsible Executive specified under Policy SC14, who will decide the matter. This Responsible Executive may consult with the Information Security Governance Committee and/or the other Responsible Executive if he or she determines it would be appropriate to do so.
10. The Responsible Executive's decision is final.

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems