BRITISH COLUMBIA

Office of the Chief
Information Officer

Information Security Policy v3.0

2016 Revision Summary

The Information Security Policy (ISP) v3.0 2016 replaces ISP v2.2 2012. The new version has undergone revision based on the updated ISO 27002:2013 standard, new and updated government policies and standards, and the overall government IM/IT strategic objectives.

Version 3.0 of the Information Security Policy represents significant updates from ISP v 2.2, in both the organization of the document and specific policy changes driven by a variety of factors.

Policy Content Changes

Information Management, Technology and Security are in a constant state of growth and fluctuation. Government must respond appropriately to ensure that the information security foundation supports these changes and provides employees, including service providers and contractors with the tools necessary to perform their responsibilities. ISP v3.0 contains a number of such updates:

- references to the new Privacy Management and Accountability Policy
- references to new or revised policies and standards in support of mobile work and teleworking;
- the protection of test data, including the use of production data for testing;
- the appropriate use of information resources;
- the payment card industry data security standard; and
- cloud computing.

Revisions have been made to provide more clarity, specifically for terms and definitions, and the requirement for conducting Security Threat and Risk Assessments. Broken web links have been corrected and new links added. Obsolete references have been updated or deleted.

Organization of the document

References – a master list of references is included at the front of the document that ISP users can refer to. This eliminates the need of overcrowding the policies with repeating reference sections. The ISP document focusses on the policy content and a hyperlink change can be done only once.

Numbering – Anyone familiar with the Information Security Policy will immediately see that there are more chapters and the ordering of the individual policies has changed in many instances. Feedback received from Ministry Information Security Officers and other ISP users was that the numbering of ISP policies was different than the policies in the ISO Standard 27002:2013. In response to this request, Version 3.0 has been re-ordered as needed to match the ISO Standard table of contents. A comparison document between ISP v2.2 and the new ISP v3.0 highlights the high-level changes and is available together with the policy. The following is a brief overview of the major changes:

- Chapter 3 is on Human Resource Security (previously Chapter 4);
- Chapter 4 is on Asset Management (previously Chapter 3);
- Previous Chapter 6, Communications and Operations Management, is split into two chapters:
    - Chapter 8 – Operations Security, and
    - Chapter 9 – Communications Security;

- Current Chapter 6 – Cryptography is a new chapter (previously policies existed in other sections).
- Mobile computing policies have moved from Chapter 7 – Access Control to Chapter 2 – Organization of Information Security.
- Chapter 11 – Supplier Relationships is a new chapter, which also includes policies on the use of cloud computing services.

Annual Information Security Review – As required under Chapter 12 of the Core Policies and Procedures Manual, the Information Security Branch works with ministries on annually reviewing their compliance with the Information Security Policy using the iSMART tool and the ISO Standard. Throughout the ISP v3.0, the policies are following by the statement *"ISP # is reported on as part of the annual information security review as CO.#"*. *CO* refers to the *Control Objectives* statements in iSMART. This addition is provided to facilitate ease of use.

Metrics and Enforcement statements – In the ISP v2.2, *Metrics and Enforcement* statements were suggested for each policy as a tool for users to self-evaluate the application of the policy. In ISP v3.0, the term *Recommended Tests* is used instead, to better reflect the intent.