BRITISH COLUMBIA | Office of the Chief Information Officer

Information Security Policy

Comparison between v2.2 2012 and v3.0 2016

Information Security Policy v2.2 2012	Information Security Policy v3.0 2016
Introduction	**I. Introduction**
	II. Scope
	III. Revisions from ISP v2.2 (2012) to ISP v3.0 (2016)
	IV. Terms and definitions
	V. List of commonly used references
Chapter 1 – Security Policy	**1. Information Security Policies**
1.1 Information security policy	1.1 Information security policy
Chapter 2 – Organizing Information Security	**2. Organization of Information Security**
2.1 Internal organization	2.1 Internal organization
2.2 External parties *(moved to **Supplier Relationships** policies)*	
	2.2 Mobile computing and teleworking
Chapter 4 – Human Resources Security	**3. Human Resource Security**
4.1 Prior to employment	3.1 Prior to employment
4.2 During employment	3.2 During employment
4.3 Termination or change of employment	3.3. Termination or change of employment
Chapter 3 – Asset Management	**4. Asset Management**
3.1 Responsibility for assets	4.1 Responsibility for assets
3.2 Information classification	4.2 Information classification
	4.3 Removable media
Chapter 7 – Access Control	**5. Access Control**
7.1 Business requirement for access control	5.1 Business requirements of access control
7.2 User access management	5.2 Employee access management
7.3 User responsibilities	5.3 Employee responsibilities
7.4 Network access control *(moved to **Communications Security** policies)*	
7.5 Operating system access control *(moved to **Operations Security** policies)*	

Information Security Policy v2.2 2012	Information Security Policy v3.0 2016
7.6 Application and information access control	5.4 System application access control
7.7 Mobile computing and teleworking *(moved to **Organization of Information Security** policies)*	
	6. Cryptography
	6.1 Cryptographic controls
Chapter 5 – Physical and Environmental Security	**7. Physical and Environmental Security**
5.1 Secure areas	7.1 Secure areas
5.2 Equipment security	7.2 Equipment Security
Chapter 6 – Communications and Operations Management	**8. Operations Security**
6.1 Operational procedures and responsibilities	8.1 Operational Procedures and Responsibilities
6.2 Third party service delivery management *(moved to **Supplier Relationships** policies)*	
6.3 System planning and acceptance *(moved to **System Acquisition, Development and Maintenance** policies)*	
6.4 Protection against malicious and mobile code	8.2 Protection from malware
6.5 Backup	8.3 Backup
6.6 Network security management *(moved to **Communication Security** policies)*	
6.7 Media handling *(moved to **Asset Management** policies)*	
6.8 Exchanges of information *(moved to **Communications Security** policies)*	
6.9 Electronic commerce activities *(moved to **System Acquisition, Development and Maintenance** policies)*	
6.10 Monitoring	8.4 Logging and monitoring
	8.5 Control of operational software
	8.6 Technical vulnerability management
	8.7 Information systems audit considerations
	9. Communications Security
	9.1 Network security management
	9.2 Information transfer
Chapter 8 – Information Systems Acquisition, Development and Maintenance	**10. System Acquisition, Development and Maintenance**
8.1 Security requirements of information systems	10.1 Security requirements of information systems

Information Security Policy v2.2 2012	Information Security Policy v3.0 2016
8.2 Correct processing in applications	10.3 Correct processing in applications
8.3 Cryptographic controls *(moved to **Cryptography** policies)*	
8.4 Security of system files *(moved to **Operations Security** policies)*	
8.5 Security in development and support processes	10.2 Security in development and support process
8.6 Vulnerability management *(moved to **Operations Security** policies)*	
	10.4 Test data
	11. Supplier Relationships
	11.1 Information security in supplier relationships
	11.2 Supplier service delivery management
	11.3 Cloud Computing
Chapter 9 – Information Security Incident Management	**12. Information Security Incident Management**
9.1 Reporting information security events and weaknesses *(consolidated with the section below)*	
9.2 Management of information security incidents and improvements	12.1 Management of information security incidents and improvements
Chapter 10 – Business Continuity Management	**13. Information Security Aspects of Business Continuity Management**
10.1 Information security aspects of business continuity management	13.1 Information security continuity
	13.2 Redundancies
Chapter 11 – Compliance	**14. Compliance**
11.1 Compliance with legal requirements	14.1 Compliance with legal and contractual requirements
11.2 Compliance with security policies and standards *(consolidated with the section above)*	
11.3 Information systems audit considerations *(moved to **Operations Security** policies)*	
	14.2 Information security reviews
Appendix A – Glossary	**Appendix A - Glossary**