VICTORIAN PROTECTIVE DATA SECURITY FRAMEWORK (VPDSF) ROSETTA STONE **CORE**

VPDSS	STANDARDS FOR LAW ENFORCEMENT DATA SECURITY (SLEDS – FORMERLY CLEDS STANDARDS) BY CPDP	WHOLE OF VICTORIAN GOVERNMENT CIO COUNCIL INFORMATION MANAGEMENT AND INFORMATION SECURITY STANDARDS	PROTECTIVE SECURITY POLICY FRAMEWORK (PSPF) BY ATTORNEY GENERALS DEPARTMENT	ISO27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS
GOVERNANCE				
1 **GOVERNANCE** – SECURITY MANAGEMENT FRAMEWORK	1. Information Security Management Structure 2. Security Roles (Security Exec, ASA, ITSA) 40. Identify and document legal requirements	SEC POL 01 Information Security Management Policy SEC STD 01 Information Security Management Framework SEC GUIDE 01 ISMF Implementation Guide	GOV-2 Security Roles (Security Executive, ASA and ITSA) GOV-3 Knowledge/skills of ASA and ITSA INFOSEC 2 (23) Information security framework PHYSEC 7 (36) Implement heightened security levels	4.1 Context of the organisation – Understanding the organisation and its context 4.2 Context of the organisation – Understanding the needs and expectations of interested parties 4.3 Context of the organisation – Determining the scope of the information security management system 4.4 Context of the organisation –Lifecycle of Information security management system 5.1 Leadership – Leadership and commitment 5.3 Leadership – Organisational roles, responsibilities and authorities 6.1.1 Planning – Actions to address risks and opportunities – General 6.2 Information security objectives and planning to achieve them 7.1 Support – Resources 7.2 Support – Competence 7.3 Support – Awareness 7.4 Support – Communication 7.5.1 Support – Documented information – General 7.5.2 Support – Documented information – Creating and updating 7.5.3 Support – Documented information – Control of documented information 8.1 Operation – Operational planning and control 9.1 Performance evaluation – Monitoring, measurement, analysis and evaluation 9.2 Performance evaluation – Internal audit 9.3 Performance evaluation – Management review 10.1 Improvement – Nonconformity and corrective action 10.2 Improvement – Continual improvement

VPDSS	STANDARDS FOR LAW ENFORCEMENT DATA SECURITY (SLEDS – FORMERLY CLEDS STANDARDS) BY CPDP	WHOLE OF VICTORIAN GOVERNMENT CIO COUNCIL INFORMATION MANAGEMENT AND INFORMATION SECURITY STANDARDS	PROTECTIVE SECURITY POLICY FRAMEWORK (PSPF) BY ATTORNEY GENERALS DEPARTMENT	ISO27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS
2 **GOVERNANCE** – SECURITY RISK MANAGEMENT	31. Risk Management Policy	SEC STD 01 Information Security Management Framework	GOV-6 Risk Management approach	6.1.1 Planning – Actions to address risks and opportunities – General 6.1.2 Planning – Actions to address risks and opportunities – Information security risk assessment 6.1.3 Planning – Actions to address risks and opportunities – Information security risk treatment 8.2 Operation – Information security risk assessment 8.3 Operation – Information security risk treatment
3 **GOVERNANCE** – SECURITY POLICIES AND PROCEDURES	3. User Roles and Responsibilities 9. Access Control policy 19. Clear desk and screen policy 24. Cryptographic policy and key management plans 27. Procedures for classifying information 28. Policy and protocols for protection of classified information 38. Formal exchange policies, procedures and controls 40. Identify and document legal requirements	SEC STD 01 Information Security Management Framework	GOV-5 Agency own policies and standards INFOSEC 1 (23) Information security policy and plan PHYSEC 1 (30) Physical security policy and plan	5.1 Leadership – Leadership and commitment 5.2 Leadership – Policy 7.5.1 Support – Documented information – General 7.5.2 Support – Documented information – Creating and updating 7.5.3 Support – Documented information – Control of documented information
4 **GOVERNANCE** – INFORMATION ACCESS	8. Suitable persons (need to know) and security checks 9. Access Control policy 10. Monitoring access 29. Personnel security clearance requirements for access to classified information	SEC STD 01 Information Security Management Framework IDAM POL 01 Identity and Access Management IDAM STD 01 Identity and Access Management IDAM STD 02-1 Strength of registration: staff IDAM STD 03 Strength of authentication mechanism IDAM GUIDE 01 – Identity and access management	INFOSEC 5 (27) Access control rules and measures	

VPDSS	STANDARDS FOR LAW ENFORCEMENT DATA SECURITY (SLEDS – FORMERLY CLEDS STANDARDS) BY CPDP	WHOLE OF VICTORIAN GOVERNMENT CIO COUNCIL INFORMATION MANAGEMENT AND INFORMATION SECURITY STANDARDS	PROTECTIVE SECURITY POLICY FRAMEWORK (PSPF) BY ATTORNEY GENERALS DEPARTMENT	ISO27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS
5 **GOVERNANCE** – SECURITY OBLIGATIONS	3. User Roles and Responsibilities 4. Responsibilities in position descriptions prior to employment 5. Confidentiality agreements and clauses	SEC STD 01 Information Security Management Framework	GOV-3 Knowledge/skills of ASA and ITSA	7.3 Support – Awareness
6 **GOVERNANCE** – SECURITY TRAINING AND AWARENESS	7. Induction and ongoing security training	SEC STD 01 Information Security Management Framework	GOV-1 Security awareness training	7.2 Support – Competence 7.3 Support – Awareness
7 **GOVERNANCE** – SECURITY INCIDENT MANAGEMENT	6. Disciplinary system for breaches 32. Reporting, escalation and response procedures for security incidents 33. Continual monitoring and improvement of incident management	SEC STD 01 Information Security Management Framework	GOV-8 Training of investigators and incident management	

VPDSS	STANDARDS FOR LAW ENFORCEMENT DATA SECURITY (SLEDS – FORMERLY CLEDS STANDARDS) BY CPDP	WHOLE OF VICTORIAN GOVERNMENT CIO COUNCIL INFORMATION MANAGEMENT AND INFORMATION SECURITY STANDARDS	PROTECTIVE SECURITY POLICY FRAMEWORK (PSPF) BY ATTORNEY GENERALS DEPARTMENT	ISO27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS
8 **GOVERNANCE** – BUSINESS CONTINUITY MANAGEMENT	34. Business Continuity Plans 35. Testing and review of BCP	SEC STD 01 Information Security Management Framework	GOV-11 Business Continuity Management Program	

VPDSS	STANDARDS FOR LAW ENFORCEMENT DATA SECURITY (SLEDS – FORMERLY CLEDS STANDARDS) BY CPDP	WHOLE OF VICTORIAN GOVERNMENT CIO COUNCIL INFORMATION MANAGEMENT AND INFORMATION SECURITY STANDARDS	PROTECTIVE SECURITY POLICY FRAMEWORK (PSPF) BY ATTORNEY GENERALS DEPARTMENT	ISO27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS
9 **GOVERNANCE** – CONTRACTED SERVICE PROVIDERS	3. User Roles and Responsibilities 5. Confidentiality agreements and clauses 6. Disciplinary system for breaches 7. Induction and ongoing security training 8. Suitable persons (need to know) and security checks 9. Access Control policy 10. Monitoring access 11. Authorised release of information 13. Authorised and timely disposal 14. Physical controls of facilities 15. Physical transport controls of portable storage devices 16. Physical controls of facilities against service disruptions 17. Protections for ICT infrastructure 18. Physical measures during storage, handling and transportation of information 19. Clear desk and screen policy 20. Controls over radio, remote computers and mobile devices 21. Secure remote access 22. Removal of portable storage devices when not required 23. Cryptographic controls implemented IAW government standards 24. Cryptographic policy and key management plans 25.Implement security controls when systems updated/refreshed/changed 26. Procedures to ensure security during development and maintenance 27. Procedures for classifying information 28. Policy and protocols for protection of classified information 29. Personnel security clearance requirements for access to classified information 30. Use of Government approved products and solutions 31. Risk Management Policy 32. Procedures for security incidents 33. Continual monitoring and improvement of incident management 34. Business Continuity Plans 35. Testing and review of BCP 36. Authorised third party access 37. Establish formal agreements with third parties 38. Formal exchange policies, procedures and controls 39. Monitor compliance of third party agreements		GOV-10 Adherence to security provisions in multilateral or bilateral agreements GOV-12 Compliance of contracted service providers with security requirements	8.1 Operation – Operational planning and control

VPDSS	STANDARDS FOR LAW ENFORCEMENT DATA SECURITY (SLEDS – FORMERLY CLEDS STANDARDS) BY CPDP	WHOLE OF VICTORIAN GOVERNMENT CIO COUNCIL INFORMATION MANAGEMENT AND INFORMATION SECURITY STANDARDS	PROTECTIVE SECURITY POLICY FRAMEWORK (PSPF) BY ATTORNEY GENERALS DEPARTMENT	ISO27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS
10 **GOVERNANCE** – GOVERNMENT SERVICES	3. User Roles and Responsibilities 5. Confidentiality agreements and clauses 6. Disciplinary system for breaches 7. Induction and ongoing security training 8. Suitable persons (need to know) and security checks 9. Access Control policy 10. Monitoring access 11. Authorised release of information 13. Authorised and timely disposal 14. Physical controls of facilities 15. Physical transport controls of portable storage devices 16. Physical controls of facilities against service disruptions 17. Protections for ICT infrastructure 18. Physical measures during storage, handling and transportation of information 19. Clear desk and screen policy 20. Controls over radio, remote computers and mobile devices 21. Secure remote access 22. Removal of portable storage devices when not required 23. Cryptographic controls implemented IAW government standards 24. Cryptographic policy and key management plans 25. Implement security controls when systems updated/refreshed/changed 26. Procedures to ensure security during development and maintenance 27. Procedures for classifying information 28. Policy and protocols for protection of classified information 29. Personnel security clearance requirements for access to classified information 30. Use of Government approved products and solutions 31. Risk Management Policy 32. Procedures for security incidents 33. Continual monitoring and improvement of incident management 34. Business Continuity Plans 35. Testing and review of BCP 36. Authorised third party access 37. Establish formal agreements with third parties 38. Formal exchange policies, procedures and controls 39. Monitor compliance of third party agreements		GOV-10 Adherence to security provisions in multilateral or bilateral agreements	

VPDSS	STANDARDS FOR LAW ENFORCEMENT DATA SECURITY (SLEDS – FORMERLY CLEDS STANDARDS) BY CPDP	WHOLE OF VICTORIAN GOVERNMENT CIO COUNCIL INFORMATION MANAGEMENT AND INFORMATION SECURITY STANDARDS	PROTECTIVE SECURITY POLICY FRAMEWORK (PSPF) BY ATTORNEY GENERALS DEPARTMENT	ISO27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS
11 **GOVERNANCE** – SECURITY PLANS	31. Risk Management Policy	SEC STD 01 Information Security Management Framework	GOV-4 Security Plan GOV-6 Risk Management approach INFOSEC 1 (20) info security policy and plan	6.1.1 Planning – Actions to address risks and opportunities – General 6.1.3 Planning – Actions to address risks and opportunities – Information security risk treatment 6.2 Information security objectives and planning to achieve them 8.1 Operation – Operational planning and control 8.2 Operation – Information security risk assessment 8.3 Operation – Information security risk treatment
12 **GOVERNANCE** – COMPLIANCE	43. System for monitoring and audit for compliance against SLEDS	SEC STD 01 Information Security Management Framework	GOV-7 Annual Reporting	9.1 Performance evaluation – Monitoring, measurement, analysis and evaluation 9.2 Performance evaluation – Internal audit 9.3 Performance evaluation – Management review 10.1 Improvement – Nonconformity and corrective action 10.2 Improvement – Continual improvement
CORE DOMAINS				
INFORMATION SECURITY				
13 **INFORMATION SECURITY** – INFORMATION VALUE	27. Procedures for classifying information 28. Policy and protocols for protection of classified information	SEC STD 01 Information Security Management Framework SEC GUIDE 02 Business Impact Levels and Other Criteria	INFOSEC 3 (25) Security classification policies	

VPDSS	STANDARDS FOR LAW ENFORCEMENT DATA SECURITY (SLEDS – FORMERLY CLEDS STANDARDS) BY CPDP	WHOLE OF VICTORIAN GOVERNMENT CIO COUNCIL INFORMATION MANAGEMENT AND INFORMATION SECURITY STANDARDS	PROTECTIVE SECURITY POLICY FRAMEWORK (PSPF) BY ATTORNEY GENERALS DEPARTMENT	ISO27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS
14 **INFORMATION SECURITY –** INFORMATION MANAGEMENT	13. Authorised and timely disposal 42. Protection of records	WoVG Information Management Principles IM STD 01 WoVG Information Asset Custodianship IM STD 02 Agency Information Management Governance IM GUIDE 01 Information Management Roles and Responsibilities	INFOSEC 5 (27) Access control rules and measures INFOSEC 7 (29) Information security controls adhere to legislative requirements	7.5.3 Support – Documented information – Control of documented information
15 **INFORMATION SECURITY –** INFORMATION SHARING	11. Authorised release of information 12. Appropriate electronic messaging measures 36. Authorised third party access 37. Establish formal agreements with third parties 38. Formal exchange policies, procedures and controls 39. Monitor compliance of third party agreements	SEC STD 01 Information Security Management Framework IM GUIDE 02 Consent-based sharing of personal information between Victorian government agencies	GOV-10 Adherence to security provisions in multilateral or bilateral agreements	
PERSONNEL SECURITY				
16 **PERSONNEL SECURITY –** PERSONNEL LIFECYCLE	4. Responsibilities in position descriptions prior to employment 5. Confidentiality agreements and clauses 6. Disciplinary system for breaches 8. Suitable persons (need to know) and security checks 29. Personnel security clearance requirements for access to classified information	SEC STD 01 Information Security Management Framework IDAM STD 02-1 Strength of registration: staff	PERSEC 1 (14) Eligible and suitable persons PERSEC 2 (15) Manage ongoing suitability of persons PERSEC 3 (16) Identify, record and review positions with security clearance requirements PERSEC 4 (17) Security clearance management and sponsorship PERSEC 5 (18) Security clearance eligibility waivers PERSEC 7 (20) Policies for security clearance maintenance PERSEC 8 (21) Sharing information that may impact on clearance holders suitability PERSEC 9 (22) Separation policies for departing clearance holders	

VPDSS	STANDARDS FOR LAW ENFORCEMENT DATA SECURITY (SLEDS – FORMERLY CLEDS STANDARDS) BY CPDP	WHOLE OF VICTORIAN GOVERNMENT CIO COUNCIL INFORMATION MANAGEMENT AND INFORMATION SECURITY STANDARDS	PROTECTIVE SECURITY POLICY FRAMEWORK (PSPF) BY ATTORNEY GENERALS DEPARTMENT	ISO27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS
ICT SECURITY				
17 **ICT SECURITY** – ICT LIFECYCLE	12. Appropriate electronic messaging measures 15. Physical controls of portable storage devices 17. Protections for ICT infrastructure 19. Clear desk and screen policy 20. Controls over radio, remote computers and mobile devices 21. Secure remote access 22. Removal of portable storage devices when not required 23. Cryptographic controls implemented IAW government standards 24. Cryptographic policy and key management plans 25. Implement security controls when systems updated/refreshed/changed 26. Procedures to ensure security during development and maintenance 30. Use of Government approved products and solutions	SEC STD 01 Information Security Management Framework SEC STD 03 Information Security – Penetration Testing SEC GUIDE 03 Information security penetration testing guideline IDAM STD 03 Strength of authentication mechanism	INFOSEC 4 (26) Implement 'Strategies to mitigate targeted cyber intrusions' in the ISM INFOSEC 6 (28) ICT development security controls INFOSEC 7 (29) Information security controls adhere to legislative requirements	
PHYSICAL SECURITY				
18 **PHYSICAL SECURITY** – PHYSICAL LIFECYCLE	13. Authorised and timely disposal 14. Physical controls of facilities 15. Physical transport controls of portable storage devices 16. Physical controls of facilities against service disruptions 17. Protections for ICT infrastructure 18. Physical measures during storage, handling and transportation of information 19. Clear desk and screen policy 22. Removal of portable storage devices when not required	SEC STD 01 Information Security Management Framework	PHYSEC 1 (30) Physical security policy and plan PHYSEC 3 (32) Early integration of security for facilities PHYSEC 6 (35) Physical controls of information and ICT systems PHYSEC 7 (36) Implement heightened security levels	

VPDSS ✓	STANDARDS FOR LAW ENFORCEMENT DATA SECURITY (SLEDS – FORMERLY CLEDS STANDARDS) BY CPDP	WHOLE OF VICTORIAN GOVERNMENT CIO COUNCIL INFORMATION MANAGEMENT AND INFORMATION SECURITY STANDARDS	PROTECTIVE SECURITY POLICY FRAMEWORK (PSPF) BY ATTORNEY GENERALS DEPARTMENT	ISO27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS
	SLEDS SECTIONS NOT COVERED:	**WOVG SECTIONS NOT COVERED:**	**PSPF SECTIONS NOT COVERED:**	
	41. Controls for legal, regulatory and contractual compliance regarding IP and proprietary software	SEC STD 02 Critical Information Infrastructure Risk Management	GOV-9 Guidance to staff on federal legislation	
		SEC STD 10 Information Security – IP Address Management	GOV-13 Compliance with Public Governance, Performance and Accountability Rule and Fraud Control Policy	
		SEC GUIDE 04 Safeguarding information while travelling guideline	PERSEC 3 (16) – DSAP register	
		SEC GUIDE 06 Information security cloud computing security considerations guideline	PERSEC 6 (19) Use of AGSVA for security clearances	
		IDAM STD 02-2 Strength of registration: citizens	PHYSEC 2 (31) Policies for threats to staff and incident reporting	
		IDAM POL 02 Citizen Identity Management	PHYSEC 4 (33) OHS obligations	
			PHYSEC 5 (34) Physical safety of citizens	

VICTORIAN PROTECTIVE DATA SECURITY FRAMEWORK (VPDSF) ROSETTA STONE **SUPPLEMENTARY**

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
GOVERNANCE				
1 **GOVERNANCE** – SECURITY MANAGEMENT FRAMEWORK	Information Security Governance – Information Security Engagement – Roles and Responsibilities – CISO Information Security Governance – Information Security Engagement – Roles and Responsibilities – ITSA Information Security Governance – Information Security Engagement – Roles and Responsibilities – ITSM Information Security Governance – Information Security Engagement – Roles and Responsibilities – ITSO Information Security Governance – Information Security Engagement – Roles and Responsibilities – System Owners	SG1.1 Security Governance Approach – Security Governance Framework SG1.2 Security Governance Approach – Security Direction SG2.2 Security Governance Components – Stakeholder Value Delivery SM2.1 Information Security Management – Information Security Function SM2.3 Information Security Management – Legal and Regulatory Compliance LC1.1 Local Environments – Local Environment Profile LC1.2 Local Environments – Local Security Coordination	0.2 Information security requirements 5.1 Information security policies – Management direction for information security 6.1 Organisation of information security – Internal organisation 6.1.1 Organisation of information security – Internal organisation – Information security roles and responsibilities 18.1 Compliance – Compliance with legal and contractual requirements 18.1.1 Compliance – Compliance with legal and contractual requirements – Identification of applicable legislation and contractual requirements 18.2 Compliance – Information security reviews 18.2.1 Compliance – Information security reviews – Independent review of information security 18.2.2 Compliance – Information security reviews – Compliance with security policies and standards	Req A3 – Designated Entities Supplemental Validation (DESV) – A3.2 Document and validate PCI DSS scope
2 **GOVERNANCE** – SECURITY RISK MANAGEMENT	Information Security Risk Management	SG2.3 Security Governance Components – Information Security Assurance IR1.1 Information Risk Assessment Framework – Information Risk Assessment – Management Approach IR1.2 Information Risk Assessment Framework – Information Risk Assessment – Methodology IR1.3 Information Risk Assessment Framework – Information Risk Assessment – Supporting Material IR2.1 Information Risk Assessment Process – Risk Assessment Scope IR2.2 Information Risk Assessment Process – Business Impact Assessment IR2.6 Information Risk Assessment Process – Threat Profiling IR2.7 Information Risk Assessment Process – Vulnerability Assessment IR2.8 Information Risk Assessment Process – Risk Evaluation IR2.9 Information Risk Assessment Process – Risk Treatment SI2.2 Security Performance – Information Risk Reporting	0.3 Selecting controls	Req 12 – Maintain a policy that addresses information security for all personnel (particularly 12.2 – Risk assessment process)

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
3 **GOVERNANCE** – SECURITY POLICIES AND PROCEDURES	Information Security Governance – Information Security Documentation – Documentation Fundamentals Information Security Governance – Information Security Documentation – Information Security Policy Information Security Governance – Information Security Documentation – Standard Operating Procedures	SM1.1 Security Policy Management – Information Security Policy SM1.2 Security Policy Management – Acceptable Use Policies	0.4 Developing your own guidelines 0.6 Related standards 5.1.1 Information security policies – Management direction for information security – Policies for information security 5.1.2 Information security policies – Management direction for information security – Review of the policies for information security 6.1.3 Organisation of information security – Internal organisation – Contact with authorities 6.2.1 Organisation of information security – Mobile devices and teleworking – Mobile device policy 6.2.2 Organisation of information security – Mobile devices and teleworking – Teleworking 8.2.3 Asset management – Information classification – Handling of assets 11.2.9 Physical and environmental security – Equipment – Clear desk and clear screen policy 12.1 Operations security – Operational procedures and responsibilities 12.1.1 Operations security – Operational procedures and responsibilities – Documented operating procedures 18.1.4 Compliance – Compliance with legal and contractual requirements – Privacy and protection of personally identifiable information 18.2 Compliance – Information security reviews 18.2.1 Compliance – Information security reviews – Independent review of information security 18.2.2 Compliance – Information security reviews – Compliance with security policies and standards	Req 12 – Maintain a policy that addresses information security for all personnel

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
4 **GOVERNANCE** – INFORMATION ACCESS	Information Technology Security – Access Control – Identification, Authentication and Authorisation Information Technology Security – Access Control – Privileged Access	SA1.1 Access Management – Access Control SA1.2 Access Management – User Authorisation SA1.3 Access Management – Access Control Mechanisms SA1.4 Access Management – Access Control Mechanisms – Password SA1.5 Access Management – Access Control Mechanisms – Token SA1.6 Access Management – Access Control Mechanisms – Biometric SA1.7 Access Management – Sign–on Process TS1.4 Security Solutions – Identity and Access Management	6.1.2 Organisation of information security – Internal organisation – Segregation of duties 9.1 Access control – Business requirements of access control 9.1.1 Access control – Business requirements of access control – Access control policy 9.1.2 Access control – Business requirements of access control – Access to networks and network services 9.2 Access control – User access management 9.2.1 Access control – User access management – User registration and de–registration 9.2.2 Access control – User access management – User access provisioning 9.2.3 Access control – User access management – Management of privileged access rights 9.2.4 Access control – User access management – Management of secret authentication information of users 9.2.5 Access control – User access management – Review of user access rights 9.2.6 Access control – User access management – Removal or adjustment of access rights 9.3 Access control – User responsibilities 9.3.1 Access control – User responsibilities – Use of secret authentication information 9.4 Access control – System and application access control 9.4.1 Access control – System and application access control – Information access restriction 9.4.2 Access control – System and application access control – Secure log–on procedures 9.4.3 Access control – System and application access control – Password management system 9.4.4 Access control – System and application access control – Use of privileged utility programs 9.4.5 Access control – System and application access control – Access control to program source code	Req 7 – Restrict access to cardholder data by business need to know Req 8 – Identify and authenticate access to system components Req 10 – Track and monitor all access to network resources and cardholder data Req A3 – Designated Entities Supplemental Validation (DESV) – A3.4 Control and manage logical access to the cardholder data environment

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
5 **GOVERNANCE** – SECURITY OBLIGATIONS		PM1.2 Human Resource Management – Ownership and Responsibilities PM1.3 Human Resource Security – Remote Working	7.1.2 Human resource security – Prior to employment – Terms and conditions of employment 7.2 Human resource security – During employment 7.2.1 Human resource security – During employment – Management responsibilities 7.3.1 Human resource security – Termination and change of employment – Termination or change of employment responsibilities 8.1.3 Asset management – Responsibility for assets – Acceptable use of assets 8.1.4 Asset management – Responsibility for assets – Return of assets 11.2.8 Physical and environmental security – Equipment – Unattended user equipment	Req 12 – Maintain a policy that addresses information security for all personnel (particularly 12.4 – security responsibilities)
6 **GOVERNANCE** – SECURITY TRAINING AND AWARENESS	Personnel Security – Personnel Security for Systems – Information Security Awareness and Training	PM2.1 Security Awareness / Education – Security Awareness Programme PM2.2 Security Awareness / Education – Security Awareness Messages PM2.3 Security Awareness / Education – Security Education / Training	6.1.4 Organisation of information security – Internal organisation – Contact with special interest groups 7.2.1 Human resource security – During employment – Management responsibilities 7.2.2 Human resource security – During employment – Information security awareness, education and training	Req 12 – Maintain a policy that addresses information security for all personnel (particularly 12.6 – awareness program)

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
7 **GOVERNANCE** – SECURITY INCIDENT MANAGEMENT	Information Security Governance – Information Security Documentation – Incident Response Plan Information Security Governance – Cyber Security Incidents – Detecting Cyber Security Incidents Information Security Governance – Cyber Security Incidents – Reporting Cyber Security Incidents Information Security Governance – Cyber Security Incidents – Managing Cyber Security Incidents	TM2.1 Security Incident Management – Security Incident Management Framework TM2.2 Security Incident Management – Security Incident Management Process TM2.3 Security Incident Management – Emergency Fixes TM2.4 Security Incident Management – Forensic Investigations BC1.4 Business Continuity Framework – Crisis Management	6.1.3 Organisation of information security – Internal organisation – Contact with authorities 16.1 Information security incident management – Management of information security incidents and improvements 16.1.1 Information security incident management – Management of information security incidents and improvements – Responsibilities and procedures 16.1.2 Information security incident management – Management of information security incidents and improvements – Reporting information security events 16.1.3 Information security incident management – Management of information security incidents and improvements – Reporting information security weaknesses 16.1.4 Information security incident management – Management of information security incidents and improvements – Assessment of and decision on information security events 16.1.5 Information security incident management – Management of information security incidents and improvements – Response to information security incidents 16.1.6 Information security incident management – Management of information security incidents and improvements – Learning from information security incidents 16.1.7 Information security incident management – Management of information security incidents and improvements – Collection of evidence	Req 12 – Maintain a policy that addresses information security for all personnel (particularly 12.10 – incident response) Req A3 – Designated Entities Supplemental Validation (DESV) – A3.5 Identify and respond to suspicious events
8 **GOVERNANCE** – BUSINESS CONTINUITY MANAGEMENT	Information Security Governance – Information Security Documentation – Business Continuity and Disaster Recovery Plans	BC1.1 Business Continuity Framework – Business Continuity Strategy BC1.2 Business Continuity Framework – Business Continuity Programme BC2.1 Business Continuity Process – Business Continuity Planning BC2.2 Business Continuity Process – Business Continuity Arrangements BC2.3 Business Continuity Process – Business Continuity Testing	6.1.3 Organisation of information security – Internal organisation – Contact with authorities 17.1 Information security aspects of business continuity management – Information security continuity 17.1.1 Information security aspects of business continuity management – Information security continuity – Planning information security continuity 17.1.2 Information security aspects of business continuity management – Information security continuity – Implementing information security continuity 17.1.3 Information security aspects of business continuity management – Information security continuity – Verify, review and evaluate information security continuity 17.2 Information security aspects of business continuity management – Redundancies 17.2.1 Information security aspects of business continuity management – Redundancies – Availability of information processing facilities	

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
9 **GOVERNANCE** – CONTRACTED SERVICE PROVIDERS	Information Security Governance – Information Security Engagement – Outsourced General Information Technology Services Information Security Governance – Information Security Engagement – Outsourced Cloud Services	SC1.1 External Supplier Management – External Supplier Management Process SC1.2 External Supplier Management – Outsourcing SC2.1 Cloud Computing – Cloud Computing Policy SC2.2 Cloud Computing – Cloud Service Contracts	15.1 Supplier relationships – Information security in supplier relationships 15.1.1 Supplier relationships – Information security in supplier relationships – Information security policy for supplier relationships 15.1.2 Supplier relationships – Information security in supplier relationships – Addressing security within supplier agreements 15.1.3 Supplier relationships – Information security in supplier relationships – Information and communication technology supply chain 15.2 Supplier relationships – Supplier service delivery management 15.2.1 Supplier relationships – Supplier service delivery management – Monitoring and review of supplier services 15.2.2 Supplier relationships – Supplier service delivery management – Managing changes to supplier services	Req A1 – Additional PCI DSS Requirements for Shared Hosting Providers Req 12 – Maintain a policy that addresses information security for all personnel (particularly 12.8 – service provider management)
10 **GOVERNANCE** – GOVERNMENT SERVICES	Information Security Governance – Information Security Engagement – Outsourced General Information Technology Services	SC1.1 External Supplier Management – External Supplier Management Process SC1.2 External Supplier Management – Outsourcing	15.1 Supplier relationships – Information security in supplier relationships 15.1.1 Supplier relationships – Information security in supplier relationships – Information security policy for supplier relationships 15.1.2 Supplier relationships – Information security in supplier relationships – Addressing security within supplier agreements 15.1.3 Supplier relationships – Information security in supplier relationships – Information and communication technology supply chain 15.2 Supplier relationships – Supplier service delivery management 15.2.1 Supplier relationships – Supplier service delivery management – Monitoring and review of supplier services 15.2.2 Supplier relationships – Supplier service delivery management – Managing changes to supplier services	Req A1 – Additional PCI DSS Requirements for Shared Hosting Providers

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
11 **GOVERNANCE** – SECURITY PLANS		SG2.1 Security Governance Components – Information Security Strategy		
12 **GOVERNANCE** – COMPLIANCE	Compliance and Non–compliance	SI1.1 Security Audit – Security Audit Management SI1.2 Security Audit – Security Audit Process – Planning SI1.3 Security Audit – Security Audit Process – Fieldwork SI1.4 Security Audit – Security Audit Process – Reporting SI1.5 Security Audit – Security Audit Process – Monitoring SI2.1 Security Performance – Security Monitoring and Reporting SI2.3 Security Performance – Information Security Compliance Monitoring	18.1 Compliance – Compliance with legal and contractual requirements 18.1.1 Compliance – Compliance with legal and contractual requirements – Identification of applicable legislation and contractual requirements	Req A3 – Designated Entities Supplemental Validation (DESV) – A3.1 Implement a PCI DSS compliance program Req A3 – Designated Entities Supplemental Validation (DESV) – A3.3 Validate PCI DSS is incorporated into business–as–usual (BAU) activities
CORE DOMAINS				
INFORMATION SECURITY				
13 **INFORMATION SECURITY** – INFORMATION VALUE	Information Technology Security – Media Security – Media Handling	IR2.2 Information Risk Assessment Process – Business Impact Assessment IR2.3 Information Risk Assessment Process – Business Impact Assessment – Confidentiality Requirements IR2.4 Information Risk Assessment Process – Business Impact Assessment – Integrity Requirements IR2.5 Information Risk Assessment Process – Business Impact Assessment – Availability Requirements IM1.1 Information Classification and Privacy – Information Classification and Handling	8.1 Asset management – Responsibility for assets 8.1.1 Asset management – Responsibility for assets – Inventory of assets 8.1.2 Asset management – Responsibility for assets – Ownership of assets 8.2 Asset management – Information classification 8.2.1 Asset management – Information classification – Classification of information	

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
14 **INFORMATION SECURITY** – INFORMATION MANAGEMENT	Information Technology Security – Product Security – Product Classifying and Labelling Information Technology Security – Product Security – Product Sanitisation and Disposal Information Technology Security – Media Security – Media Sanitisation Information Technology Security – Media Security – Media Destruction Information Technology Security – Media Security – Media Disposal Information Technology Security – Email Security – Email Protective Markings	IM1.1 Information Classification and Privacy – Information Classification and Handling IM2.1 Information Protection – Document Management	0.5 Lifecycle considerations 8.1 Asset management – Responsibility for assets 8.1.1 Asset management – Responsibility for assets – Inventory of assets 8.1.2 Asset management – Responsibility for assets – Ownership of assets 8.1.3 Asset management – Responsibility for assets – Acceptable use of assets 8.1.4 Asset management – Responsibility for assets – Return of assets 8.2.2 Asset management – Information classification – Labelling of information 8.2.3 Asset management – Information classification – Handling of assets 18.1.3 Compliance – Compliance with legal and contractual requirements – Protection of records	Req 3 – Protect stored cardholder data (particularly 3.1 regarding data retention and disposal policies, procedures and processes)
15 **INFORMATION SECURITY** – INFORMATION SHARING			13.2 Communications security – Information transfer 13.2.1 Communications security – Information transfer – Information transfer policies and procedures 13.2.2 Communications security – Information transfer – Agreements on information transfer	

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
PERSONNEL SECURITY				
16 **PERSONNEL SECURITY** – PERSONNEL LIFECYCLE	Personnel Security – Personnel Security for Systems – Authorisations, Security Clearances and Briefings	PM1.1 Human Resource Security – Employment Life Cycle	6.1.2 Organisation of information security – Internal organisation – Segregation of duties 7.1 Human resource security – Prior to employment 7.1.1 Human resource security – Prior to employment – Screening 7.1.2 Human resource security – Prior to employment – Terms and conditions of employment 7.2 Human resource security – During employment 7.2.1 Human resource security – During employment – Management responsibilities 7.2.3 Human resource security – During employment – Disciplinary process 7.3 Human resource security – Termination and change of employment 7.3.1 Human resource security – Termination and change of employment – Termination or change of employment responsibilities 8.1.4 Asset management – Responsibility for assets – Return of assets 9.2.6 Access control – User access management – Removal or adjustment of access rights 13.2.4 Communications security – Information transfer – Confidentiality or non–disclosure agreements	Req 12 – Maintain a policy that addresses information security for all personnel (particularly 12.7 – personnel screening)

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
ICT SECURITY				
17 **ICT SECURITY** – ICT LIFECYCLE CONTINUED	Information Security Governance – Information Security Documentation – Security Risk Management Plan Information Security Governance – Information Security Documentation – System Security Plan Information Security Governance – Information Security Documentation – Emergency Procedures Information Security Documentation – System Accreditation Information Security Governance – System Accreditation – Accreditation Framework Information Security Governance – System Accreditation – Conducting Accreditations Information Security Governance – System Accreditation – Conducting Certifications Information Security Governance – System Accreditation – Conducting Security Assessments or Audits Information Security Governance – Information Security Monitoring – Vulnerability Management Information Security Governance – Information Security Monitoring – Change Management Personnel Security – Personnel Security for Systems – Authorisations, Security Clearances and Briefings Communications Security – Communications Infrastructure – Cable Management Fundamentals Communications Security – Communications Infrastructure – Cable Management for Non–Shared Government Facilities Communications Security – Communications Infrastructure – Cable Management for Shared Government Facilities Communications Security – Communications Infrastructure – Cable Management for Shared Non–Government Facilities Communications Security – Communications Infrastructure – Cable Labelling and Registration Communications Security – Communications Infrastructure – Cable Patching Communications Security – Communications Infrastructure – Emanation Security Threat Assessments Communications Security – Communications Systems and Devices – Radio Frequency, Infrared and Bluetooth Devices	PA1.1 Equipment Management – Hardware Life Cycle Management PA1.2 Equipment Management – Office Equipment PA1.3 Equipment Management – Industrial Control Systems PA2.1 Mobile Computing – Mobile Device Configuration PA2.2 Mobile Computing – Enterprise Mobility Management PA2.3 Mobile Computing – Mobile Device Connectivity PA2.4 Mobile Computing – Employee–owned Devices PA2.5 Mobile Computing – Portable Storage Devices SD1.1 System Development Management – System Development Methodology SD1.2 System Development Management – System Development Environments SD1.3 System Development Management – Quality Assurance SD2.1 System Development Life Cycle – Specifications of Requirements SD2.2 System Development Life Cycle – System Design SD2.3 System Development Life Cycle – Software Acquisition SD2.4 System Development Life Cycle – System Build SD2.5 System Development Life Cycle – System Testing SD2.6 System Development Life Cycle – Security Testing SD2.7 System Development Life Cycle – System Promotion Criteria SD2.8 System Development Life Cycle – Installation Process SD2.9 System Development Life Cycle – Post–implementation Review SD2.10 System Development Life Cycle – System Decommission BA1.1 Corporate Business Applications – Business Application Register BA1.2 Corporate Business Applications – Business Application Protection	6.2 Organisation of information security – Mobile devices and teleworking 8.3 Asset management – Media handling 8.3.1 Asset management – Media handling – Management of removable media 8.3.2 Asset management – Media handling – Disposal of media 9.1.2 Access control – Business requirements of access control – Access to networks and network services 9.2.3 Access control – User access management – Management of privileged access rights 9.2.4 Access control – User access management – Management of secret authentication information of users 9.3 Access control – User responsibilities 9.3.1 Access control – User responsibilities – Use of secret authentication information 9.4 Access control – System and application access control 9.4.1 Access control – System and application access control – Information access restriction 9.4.2 Access control – System and application access control – Secure log–on procedures 9.4.3 Access control – System and application access control – Password management system 9.4.4 Access control – System and application access control – Use of privileged utility programs 9.4.5 Access control – System and application access control – Access control to program source code 10.1 Cryptographic controls 10.1.1 Cryptographic controls – Policy on the use of cryptographic controls 10.1.2 Cryptographic controls – Key management 11.2.3 Physical and environmental security – Equipment – Cabling security 11.2.5 Physical and environmental security – Equipment – Removal of assets 11.2.6 Physical and environmental security – Equipment – Security of equipment and assets off–premises 11.2.7 Physical and environmental security – Equipment – Secure disposal or re–use of equipment 11.2.8 Physical and environmental security – Equipment – Unattended user equipment	Req 1 – Install and maintain a firewall configuration to protect cardholder data Req 2 – Do not use vendor–supplied defaults for system passwords and other security parameters Req 3 – Protect stored cardholder data Req 4 – Encrypt transmission of cardholder data across open, public networks Req 5 – Protect all systems against malware and regularly update anti–virus software or programs Req 6 – Develop and maintain secure systems and applications Req 10 – Track and monitor all access to network resources and cardholder data Req 11 – Regularly test security systems and processes Req A2 – Additional PCI DSS Requirements for Entities using SSL/early TLS

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
17 **ICT SECURITY** – ICT LIFECYCLE CONTINUED	Communications Security – Communications Systems and Devices – Fax Machines and Multifunction Devices Communications Security – Communications Systems and Devices – Telephones and Telephone Systems Information Technology Security – PSPF Mandatory Requirement INFOSEC 4 explained Information Technology Security – Product Security – Product Selection and Acquisition Information Technology Security – Product Security – Product Installation and Configuration Information Technology Security – Product Security – Product Maintenance and Repairs Information Technology Security – Media Security – Media Usage Information Technology Security – Software Security – Standard Operating Environments Information Technology Security – Software security – Software Patching Information Technology Security – Software Security – Software Development Information Technology Security – Software Security – Web Application Development Information Technology Security – Software Security – Database Systems Information Technology Security – Email Security – Email Policy Information Technology Security – Email Security – Email Infrastructure Information Technology Security – Email Security – Email Content Filtering Information Technology Security – Access Control – Event Logging and Auditing Information Technology Security – Secure Administration Information Technology Security – Network Security – Network Management Information Technology Security – Network Security – Network Design and Configuration Information Technology Security – Cryptography – Cryptographic Fundamentals Information Technology Security – Cryptography – ASD Approved Cryptographic Algorithms Information Technology Security – Cryptography – ASD Approved Cryptographic Protocols	BA1.3 Corporate Business Applications – Browser–based Application Protection BA1.4 Corporate Business Applications – Information Validation BA2.1 End User Developed Applications (EUDA) – EUDA Inventory BA2.2 End User Developed Applications (EUDA) – Protection of Spreadsheets BA2.3 End User Developed Applications (EUDA) – Protection of Databases BA2.4 End User Developed Applications (EUDA) – EUDA Development SY1.1 System Configuration – Computer and Network Installations SY1.2 System Configuration – Server Configuration SY1.3 System Configuration – Virtual Servers SY1.4 System Configuration – Network Storage Systems SY2.1 System Maintenance – Service Level Agreements SY2.2 System Maintenance – Performance and Capacity Management SY2.3 System Maintenance – Backup SY2.4 System Maintenance – Change Management NC1.1 Network Management – Network Device Configuration NC1.2 Network Management – Physical Network Management NC1.3 Network Management – Wireless Access NC1.4 Network Management – External Network Connections NC1.5 Network Management – Firewalls NC1.6 Network Management – Remote Maintenance NC2.1 Electronic Communications – Email NC2.2 Electronic Communications – Instant Messaging NC2.3 Electronic Communications – Voice over IP (VoIP) Networks NC2.4 Electronic Communications – Telephony and Conferencing TS1.1 Security Solutions – Security Architecture TS1.2 Security Solutions – Malware Protection Activities TS1.3 Security Solutions – Malware Protection Software TS1.5 Security Solutions – Intrusion Detection	12.1.4 Operations security – Operational procedures and responsibilities – Separation of development, testing and operational environments 12.2 Operations security – Protection from malware 12.2.1 Operations security – Protection from malware – Controls against malware 12.3 Operations security – Backup 12.3.1 Operations security – Backup – Information backup 12.4 Operations security – Logging and monitoring 12.4.1 Operations security – Logging and monitoring – Event logging 12.4.2 Operations security – Logging and monitoring – Protection of log information 12.4.3 Operations security – Logging and monitoring – Administrator and operator logs 12.4.4 Operations security – Logging and monitoring – Clock synchronisation 12.5 Operations security – Control of operational software 12.5.1 Operations security – Control of operational software – Installation of software on operational systems 12.6 Operations security – Technical vulnerability management 12.6.1 Operations security – Technical vulnerability management – Management of technical vulnerabilities 12.6.2 Operations security – Technical vulnerability management – Restrictions on software installation 12.1 Operations security – Information systems audit considerations 12.7.1 Operations security – Information systems audit considerations – Information systems audit controls 13.1 Communications security – Network security management 13.1.1 Communications security – Network security management – Network controls 13.1.2 Communications security – Network security management – Security of network services 13.1.3 Communications security – Network security management – Segregation in networks 13.2.3 Communications security – Information transfer – Electronic messaging 14.1 System acquisition, development and maintenance – Security requirements of information systems	

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
17 **ICT SECURITY** – ICT LIFECYCLE	Information Technology Security – Cryptography – Transport Layer Security Information Technology Security – Cryptography – Secure Shell Information Technology Security – Cryptography – Secure Multipurpose Internet Mail Extension Information Technology Security – Cryptography – Internet Protocol Security Information Technology Security – Cryptography – Key Management Information Technology Security – Cross Domain Security – Gateways Information Technology Security – Cross Domain Security – Cross Domain Solutions Information Technology Security – Cross Domain Security – Firewalls Information Technology Security – Cross Domain Security – Diodes Information Technology Security – Cross Domain Security – Web Content and Connections Information Technology Security – Cross Domain Security – Peripheral Switches Information Technology Security – Data Transfers and Content Filtering – Data Transfer Policy Information Technology Security – Data Transfers and Content Filtering – Data Transfer Procedures Information Technology Security – Data Transfers and Content Filtering – Content Filtering Information Technology Security – Working Off–Site – Mobile Devices Information Technology Security – Working Off–Site – Working Outside the Office Information Technology Security – Working Off–Site – Working From Home	TS1.6 Security Solutions – Information Leakage Protection TS1.7 Security Solutions – Digital Rights Management TS2.1 Cryptography – Cryptographic Solutions TS2.2 Cryptography – Cryptographic Key Management TS2.3 Cryptography – Public Key Infrastructure TM1.1 Cyber Security Resilience – Technical Vulnerability Management TM1.2 Cyber Security Resilience – Security Event Logging TM1.3 Cyber Security Resilience – Security Event Management TM1.4 Cyber Security Resilience – Threat Intelligence TM1.5 Cyber Security Resilience – Cyber Attack Protection BC1.3 Business Continuity Framework – Resilient Technical Environments	14.1.1 System acquisition, development and maintenance – Security requirements of information systems – Information security requirements analysis and specification 14.1.2 System acquisition, development and maintenance – Security requirements of information systems – Securing application services on public networks 14.2 System acquisition, development and maintenance – Security in development and support processes 14.2.1 System acquisition, development and maintenance – Security in development and support processes – Secure development policy 14.2.2 System acquisition, development and maintenance – Security in development and support processes – System change control procedures 14.2.3 System acquisition, development and maintenance – Security in development and support processes – Technical review of applications after operating platform changes 14.2.4 System acquisition, development and maintenance – Security in development and support processes – Restrictions on changes to software packages 14.2.5 System acquisition, development and maintenance – Security in development and support processes – Secure system engineering principles 14.2.6 System acquisition, development and maintenance – Security in development and support processes – Secure development environment 14.2.7 System acquisition, development and maintenance – Security in development and support processes – Outsourced development 14.2.8 System acquisition, development and maintenance – Security in development and support processes – System security testing 14.2.9 System acquisition, development and maintenance – Security in development and support processes – System acceptance testing 14.3 System acquisition, development and maintenance – Test data 14.3.1 System acquisition, development and maintenance – Test data – Protection of test data 14.3 System acquisition, development and maintenance – Test data 14.3.1 System acquisition, development and maintenance – Test data – Protection of test data 18.2.3 Compliance – Information security reviews – Technical compliance review	

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
PHYSICAL SECURITY				
18 **PHYSICAL SECURITY** – PHYSICAL LIFECYCLE	Physical Security – Physical Security for Systems – Facilities and Network Infrastructure Physical Security – Physical Security for Systems – Servers and Network Devices Physical Security – Physical Security for Systems – ICT Equipment and Media	IM2.2 Information Protection – Sensitive Physical Information LC2.1 Physical and Environmental Security – Physical Protection LC2.2 Physical and Environmental Security – Power Supplies LC2.3 Physical and Environmental Security – Hazard Protection	6.2 Organisation of information security – Mobile devices and teleworking 8.3.3 Asset management – Media handling – Physical media transfer 11.1 Physical and environmental security – Secure areas 11.1.1 Physical and environmental security – Secure areas – Physical security perimeter 11.1.2 Physical and environmental security – Secure areas – Physical entry controls 11.1.3 Physical and environmental security – Secure areas – Securing offices, rooms and facilities 11.1.4 Physical and environmental security – Secure areas – Protecting against external and environmental threats 11.1.5 Physical and environmental security – Secure areas – Working in secure areas 11.1.6 Physical and environmental security – Secure areas – Delivery and loading areas 11.2 Physical and environmental security – Equipment 11.2.1 Physical and environmental security – Equipment – Equipment siting and protection 11.2.3 Physical and environmental security – Equipment – Cabling security 11.2.4 Physical and environmental security – Equipment – Equipment maintenance 11.2.5 Physical and environmental security – Equipment – Removal of assets 11.2.6 Physical and environmental security – Equipment – Security of equipment and assets off–premises 11.2.7 Physical and environmental security – Equipment – Secure disposal or re–use of equipment	Req 9 – Restrict physical access to cardholder data

VPDSS	AUSTRALIAN SIGNALS DIRECTORATE (ASD) – INFORMATION SECURITY MANUAL (ISM) 2016	INFORMATION SECURITY FORUM (ISF) – GOOD PRACTICE STANDARD FOR INFORMATION SECURITY 2016	ISO27002:2015 – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI – DSS)
	ISM SECTIONS NOT COVERED:	**ISF SECTIONS NOT COVERED:**	**ISO27002 SECTIONS NOT COVERED:**	
	Information Security Governance – Information Security Engagement – Government Engagement	SM2.2 Information Security Management – Information Security Projects	6.1.5 Organisation of information security – Internal organisation – Information security in project management	
	Personnel Security – Personnel Security for Systems – Using the Internet	IM1.2 Information Classification and Privacy – Information Privacy	11.2.2 Physical and environmental security – Equipment – Supporting utilities	
		SA2.1 Customer Access – Customer Access Arrangements	12.1.2 Operations security – Operational procedures and responsibilities – Change management	
		SA2.2 Customer Access – Customer Contracts	12.1.3 Operations security – Operational procedures and responsibilities – Capacity management	
		SA2.3 Customer Access – Customer Connections	14.1.3 System acquisition, development and maintenance – Security requirements of information systems – Protecting application services transactions	
			18.1.2 Compliance – Compliance with legal and contractual requirements – Intellectual property rights	
			18.1.5 Compliance – Compliance with legal and contractual requirements – Regulation of cryptographic controls	