PUBLIC SAFETY NETWORK
TE KUPENGA MARUTAU

Public Safety Network
Appendix 5.5
Functional Guidelines Security and Risk Mitigation

Contents

1. Introduction

The Public Safety Network (PSN) programme is an Emergency Services initiative of behalf of Fire and Emergency New Zealand (Fire and Emergency), New Zealand Police (Police), St John New Zealand (St John), and Wellington Free Ambulance (WFA). The PSN programme is tasked with delivering Mission Critical communication services to the Emergency Services sector.

This document should be read in conjunction with the *Appendix 1. Service Requirements* and *Appendices 4.1 to 4.5 Services Guidelines* documents.

2. Document Purpose

This document identifies security risks associated with operational PSN services and potential mitigating controls. It is intended to provide agencies, potential service providers, and other stakeholders with a high-level view of the risks and potential controls associated the use of PSN services.

It is not intended to fully define the PSN security and risk mitigation requirements but is rather a guide as to assist service providers with their design and planning ahead of detailed service design.

3. Approach

The risks and recommended mitigations described in this document represent an aggregated view of risks associated with the adoption of PSN services following a series of workshops with business representatives and subject matter experts from Police, Fire and Emergency, St John and WFA.

Controls identified in these workshops have been separated into two groups based on agency or supplier applicability. In the context of this document an agency refers to the four independent agencies Fire and Emergency, Police, St John and WFA and supplier refers to potential PSN service suppliers.

4. Security Governance

The PSN programme will provide security governance and assurance activities associated with procurement and establishment of the proposed services in the *Schedule 12. Service Catalogue* documents.

The PSN programme (and ongoing the NGCC Lead Entity) will perform the role of Certification Authority (as defined in the NZ Information Security Manual) for all services in the PSN Service Catalogue on behalf of the agencies. The agencies will endorse the scope of the certification activities to ensure they will be sufficient to allow them to accredit the services for their own use as part of secondary procurement and on-boarding.

Note that specialist security requirements for specific functions may require additional security testing and/or controls to allow the use of PSN services for these specialist functions. This is expected to be minor in the overall volumes of service consumption.

5. Security Requirements

Services provided through PSN to Emergency Services agencies will need to provide certain levels of confidentiality, integrity and availability.

Confidentiality Requirements

The PSN services will be used to collect, store, process and/or transmit information that will include personal, health and classified information that must be protected from unauthorised access and disclosure.

Integrity Requirements

The accuracy and completeness of the information within the PSN services is important as the Emergency Services will use this information to make critical decisions. Accidental or deliberate modification or deletion of this information may result in agency staff members making incorrect decisions.

Availability Requirements

PSN services are deemed to be Mission Critical as they may be used in operations relating to urgent, time-critical incidents, or when their performance is a significant contributing factor to the success or failure of work carried out by Emergency Services.

5.1 Information Classification

Based on the New Zealand Government Classification System, the information that will be stored, processed and transmitted by PSN services has been classified as RESTRICTED.

5.2 Legislation, Policy, Standards and Guidelines

Suppliers of PSN services may need to demonstrate compliance with the following acts, policies and standards:

- Civil Defence Emergency Management Act 2002;
- National Civil Defence Emergency Management Plan Order 2015;
- Building Act 2004;
- Privacy Act 1993;
- Health Information Privacy Code 1994;
- Telecommunications Act 2001;
- Telecommunications (Interception Capability & Security) Act 2013;
- Official Information Act 1982; and
- Official Information Act 1982.

PSN is also guided by the following standards, manuals and policies:

- New Zealand Protective Security Requirements;
- New Zealand Information Security Manual (NZISM);
- HISO 10029:2015 Health Information Security Framework;
- ISO/IEC 27002:2007 Code of Practice for IT Security Management;
- Building Regulations; Building Code; and
- NZ/AS Standard 1170:2002 Part 0 General Principles.

6. Detailed Service Risks

This section provides the details on the information security risk scenarios for PSN services. Controls applicable to agencies have been included for informational purposes.

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
R01	An unauthorised party gains access to communications or information on one or more PSN network services or devices using an authorised users' credentials. This results in a complete or partial service outage and/or communications: • Being intercepted; • Being manipulated or swapped; or • Being corrupted or lost. **Affects:** Confidentiality, Integrity, Availability.	• Phishing attacks for user credentials are common. • PSN services may be an attractive target for attackers. • User access management is decentralised with each agency managing their own users. • User access management processes may be inadequate or may not be followed. • Role-based access control may not be well defined or implemented. • Multiple suppliers may have administrative access. • Mobile devices may be lost or stolen.	• Personal information is accessed by unauthorised parties. • Sensitive information regarding operations is accessed by unauthorised parties. • Ongoing operational activities are compromised due to information being released. • Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost or changed. • The personal security of individuals being protected by an agency could be compromised.	SR-01 Contractual Agreements and SLAs CP-02 Architecture and Design Review IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning IS-01 Information Security Policies IS-03 Mobile Device Policy AC-01 Access Controls AC-02 User and Device Access Management AC-03 Privileged Access Management AC-04 Secure Authentication	IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning IS-01 Information Security Policies IS-04 Mobile Device Management (MDM) AC-01 Access Controls AC-02 User and Device Access Management AC-03 Privileged Access Management AC-04 Secure Authentication OP-01 Standard Operating Procedures OP-06 Back-up and Restore OP-08 Event Logging, Alerting and Auditing OP-09 Security Information and Event Management (SIEM)

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
		• PSN equipment is spread across a large geographical area. • Physical security at PSN equipment locations may be inadequate. • Users may share credentials. • Back-ups may not be in place or effective.	• Agency resources may be taken up responding to incorrect information. • Agencies may need to use alternate means of communication which could cause delays in service. • The organisations public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work.	OP-01 Standard Operating Procedures HR-01 Human Resource Security HR-04 Security Awareness	CS-02 Intrusion Detection and Prevention CS-07 Message Integrity SR-04 Security Tests and Controls Audit PE-01 Physical Security Perimeter HR-01 Human Resource Security HR-04 Security Awareness CP-01 Independent Review of Information Security
R02	An unauthorised party gains access to agency communications or information by exploiting a vulnerability in one or more network service components. This results in communications: • Being intercepted; • Being manipulated or swapped; or	• Some networks will carry both PSN and Public communications over the same communication channels. • PSN services may be an attractive target for attackers. • Encryption of communications may not be in place or may be inadequate.	• Personal information is accessed by unauthorised parties. • Sensitive information regarding operations is accessed by unauthorised parties. • Ongoing operational activities are compromised due to information being released. • Communications are interrupted at a critical time	CP-02 Architecture and Design Review CY-04 Cryptographic Key Management SA-02 Secure Application Development IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning	CY-02 Encryption of Data in Transit CY-03 Encryption of Data at Rest CY-04 Cryptographic Key Management OP-05 Malware Detection OP-06 Back-up and Restore OP-08 Event Logging, Alerting and Auditing OP-09 Security Information and Event Management (SIEM)

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
	• Being corrupted or lost. **Affects:** Confidentiality, Integrity, Availability	• Private encryption keys may not be adequately protected and managed. • Communication transit devices may have firmware vulnerabilities. • PSN endpoint communications devices may have software vulnerabilities. • Suppliers may not be following secure coding practices when developing PSN services. • Agencies may not follow secure coding practices when developing services integrated to PSN services. • Agency services integrated to PSN may include software vulnerabilities. • Back-ups may not be in place or effective.	resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost or changed. • The personal security of individuals being protected by an agency could be compromised. • Agency resources may be taken up responding to incorrect information. • Agencies may need to use alternate means of communication which could cause delays in service • The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work. • Potentially sensitive information is made publicly available without	OP-15 Security Tests and Reviews CS-01 Security of Network Services CS-04 Firewalls CP-03 Defence in Depth	OP-11 Configuration Management OP-13 Patch and Vulnerability Management OP-14 Hardening of Systems, Network Devices and Applications OP-15 Security Tests and Reviews CS-01 Security of Network Services CS-02 Intrusion Detection and Prevention CS-04 Firewalls CS-07 Message Integrity PE-01 Physical Security Perimeter SA-02 Secure Application Development SR-04 Security Tests and Controls Audit IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning CP-01 Independent Review of Information Security CP-03 Defence in Depth

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
		• PSN equipment is spread across a large geographical area. • Physical security at PSN equipment locations may be inadequate.	agency consent (internet rebroadcasting of radio communications) • Legal action may be taken against an agency for releasing sensitive information.		
R03	An unauthorised party gains access to agency communications or information by exploiting a vulnerability on one or more PSN devices. This results in communications: • Being intercepted; • Being manipulated or swapped; or • Being corrupted or lost. **Affects:** Confidentiality, Integrity, Availability	• Mobile devices may be lost or stolen. • Devices may have inadequate access controls. • Device storage may not be protected. • Vulnerabilities may exist in device operating systems. • Devices may not be owned or managed by PSN. • Devices may not be patched or updated. • Devices may have vulnerable applications installed alongside those used by PSN services.	• Personal information is accessed by unauthorised parties. • Sensitive information regarding operations is accessed by unauthorised parties. • Ongoing operational activities are compromised due to information being released. • Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost or changed.	CP-01 Independent Review of Information Security CP-02 Architecture and Design Review CY-04 Cryptographic Key Management AC-01 Access Controls AC-02 User and Device Access Management AC-04 Secure Authentication OP-11 Configuration Management OP-13 Patch and Vulnerability Management PE-01 Physical Security Perimeter	CY-02 Encryption of Data in Transit CY-03 Encryption of Data at Rest CY-04 Cryptographic Key Management OP-05 Malware Detection IS-04 Mobile Device Management (MDM) AC-01 Access Controls AC-02 User and Device Access Management AC-03 Privileged Access Management AC-04 Secure Authentication AM-04 Media Sanitation OP-06 Back-up and Restore OP-08 Event Logging, Alerting and Auditing

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
		• PSN equipment is spread across a large geographical area. • Physical security at PSN equipment locations may be inadequate. • Physical security at agency locations may be inadequate. • Suppliers may not following secure coding practices when developing PSN device services. • Back-ups may not be in place or effective.	• The personal security of individuals being protected by an agency could be compromised. • Agency resources may be taken up responding to incorrect information. • Agencies may need to use alternate means of communication which could cause delays in service • The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work.	SA-02 Secure Application Development IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning OP-15 Security Tests and Reviews	OP-09 Security Information and Event Management (SIEM) OP-11 Configuration Management OP-13 Patch and Vulnerability Management OP-14 Hardening of Systems, Network Devices and Applications OP-15 Security Tests and Reviews CS-02 Intrusion Detection and Prevention CS-07 Message Integrity SA-02 Secure Application Development SR-04 Security Tests and Controls Audit IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning CP-01 Independent Review of Information Security
R04	An agency staff member or external party contractor accidently	• User access management is decentralised with each	• Personal information is accessed by unauthorised parties.	SR-01 Contractual Agreements and SLAs	AC-01 Access Controls OP-04 Separation of Pre-Production Environments

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
	accesses, encrypts or deletes information communicated via PSN services. This results in information being: • Viewed or heard by unauthorised persons; or • Information or communications being lost or inaccessible. **Affects:** Confidentiality, Integrity, Availability	agency managing their own users. • User access management processes may be inadequate or may not be followed. • Role-based access control may not be well defined or implemented. • User training may be inadequate. • Back-ups may not be in place or effective.	• Sensitive information regarding operations is accessed by unauthorised parties. • Ongoing operational activities are compromised due to information being released. • Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost or changed. • The personal security of individuals being protected by an agency could be compromised. • Agency resources may be taken up responding to incorrect information. • Agency may not deploy resources to an incident impacting Service Delivery.	IS-01 Information Security Policies HR-03 Role-Based Training HR-04 Security Awareness AC-01 Access Controls AC-02 User and Device Access Management AC-03 Privileged Access Management OP-01 Standard Operating Procedures OP-08 Event Logging, Alerting and Auditing OP-16 Automation and Orchestration CS-03Tenant Segregation CS-06 Non-Disclosure and Confidentiality Agreements CY-01 Cryptographic Policy	OP-06 Backup and Restore OP-08 Event Logging, Alerting and Auditing OP-09 Security Information and Event Management (SIEM) IM-01 Information Security Incident Management CP-01 Independent Review of Information Security

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
			• The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work. • Patient treatment data is lost so cannot be provided to joint organisations (detrimental to patient care). • Data re-entry causing time delays for agency staff to respond to incidents • Revenue loss, through reduced ability to charge for provided services (ambulance charge). • Loss in confidence of agencies' security measures for access to third-party services (NHI, DHB). • The organisation may be in breach of contractual agreements with third parties (e.g. DHBs).	CY-04 Cryptographic Key Management CY-05 System and Information Integrity Verification IM-01 Information Security Incident Management CP-02 Architecture and Design Review	

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
R05	An agency staff member or external contractor (e.g. Air Ambulance) purposely accesses, encrypts or deletes information communicated via PSN services. This results in information being: • Viewed or heard by unauthorised persons; or • Information or communications being lost or inaccessible. **Affects:** Confidentiality, Integrity, Availability	• User access management is decentralised with each agency managing their own users. • User access management processes may be inadequate or may not be followed. • Role-based access control may not be well defined or implemented. • The vetting process in place at an agency may be inadequate. • Users may share credentials. • Back-ups may not be in place or effective.	• Personal information is accessed by unauthorised parties. • Sensitive information regarding operations is accessed by unauthorised parties. • Ongoing operational activities are compromised due to information being released. • Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost or changed. • The personal security of individuals being protected by an agency could be compromised. • Agency resources may be taken up responding to incorrect information.	SR-01 Contractual Agreements and SLAs IS-01 Information Security Policies HR-01 Human Resource Security HR-02 Screening AC-01 Access Controls AC-02 User and Device Access Management AC-03 Privileged Access Management OP-01 Standard Operating Procedures OP-08 Event Logging, Alerting and Auditing CS-03 Tenant Segregation CS-06 Non-Disclosure and Confidentiality Agreements CY-01 Cryptographic Policy	OP-06 Backup and Restore OP-08 Event Logging, Alerting and Auditing OP-09 Security Information and Event Management (SIEM) IM-01 Information Security Incident Management CP-01 Independent Review of Information Security

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
			• The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work. • Patient treatment data is lost so cannot be provided to joint organisations (detrimental to patient care). • Data re-entry causing time delays for agency staff to respond to incidents. • Revenue loss, through reduced ability to charge for provided services (ambulance charge). • Loss in confidence of agencies security measures for access to third-party services (NHI, DHB). • The organisation may be in breach of contractual agreements with third parties (e.g. DHBs).	CY-04 Cryptographic Key Management CY-05 System and Information Integrity Verification IM-01 Information Security Incident Management	

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
R06	A supplier staff member accidently accesses encrypts or deletes information communicated via PSN services. This results in information being: • Viewed or heard by unauthorised person; or • Information or communications being lost or inaccessible **Affects:** Confidentiality, Integrity, Availability	• User access management processes may be inadequate or may not be followed. • Role-based access control may not be well defined or implemented. • User training may be inadequate. • Back-ups may not be in place or effective.	• Personal information is accessed by unauthorised parties. • Sensitive information regarding operations is accessed by unauthorised parties. • Ongoing operational activities are compromised due to information being released. • Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost or changed. • The personal security of individuals being protected by an agency could be compromised. • Agency resources may be taken up responding to incorrect information.	CY-01 Cryptographic Policy CY-02 Encryption of Data in Transit CY-04 Cryptographic Key Management CY-05 System and Information Integrity Verification SR-01 Contractual Agreements and SLAs IM-01 Information Security Incident Management CP-02 Architecture and Design Review	IS-01 Information Security Policies HR-03 Role-Based Training AC-01 Access Controls AC-02 User and Device Access Management AC-03 Privileged Access Management CY-01 Cryptographic Policy CY-02 Encryption of Data in Transit CY-03 Encryption of Data at Rest CY-04 Cryptographic Key Management OP-01 Standard Operating Procedures OP-04 Separation of Pre-Production Environments OP-06 Backup and Restore OP-08 Event Logging, Alerting and Auditing OP-09 Security Information and Event Management (SIEM) OP-16 Automation and Orchestration

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
			• The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work. • Patient treatment data is lost so cannot be provided to joint organisations (detrimental to patient care). • Data re-entry causing time delays for agency staff to respond to incidents. • Revenue loss, through reduced ability to charge for provided services (ambulance charge). • Loss in confidence of agencies' security measures for access to third-party services (NHI, DHB). • The organisation may be in breach of contractual agreements with third parties (e.g. DHBs).		CS-03 Tenant Segregation CS-06 Non-Disclosure and Confidentiality Agreements SR-04 Security Tests and Controls Audit IM-01 Information Security Incident Management CP-01 Independent Review of Information Security

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
R07	A supplier staff member purposely accesses encrypts or deletes information communicated via PSN services. This results in information being: • Viewed or heard by unauthorised persons; or • Information or communications being lost or inaccessible. **Affects:** Confidentiality, Integrity, Availability	• User access management processes may be inadequate or may not be followed. • Role-based access control may not be well defined or implemented. • Multiple suppliers may have administrative access. • The vetting process in place at a supplier may be inadequate. • Users may share credentials. • Back-ups may not be in place or effective.	• Personal information is accessed by unauthorised parties. • Sensitive information regarding operations is accessed by unauthorised parties. • Ongoing operational activities are compromised due to information being released. • Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost or changed. • The personal security of individuals being protected by an agency could be compromised. • Agency resources may be taken up responding to incorrect information.	CY-05 System and Information Integrity Verification OP-08 Event Logging, Alerting and Auditing SR-01 Contractual Agreements and SLAs IM-01 Information Security Incident Management CP-02 Architecture and Design Review	HR-01 Human Resource Security HR-02 Screening AC-01 Access Controls AC-02 User and Device Access Management AC-03 Privileged Access Management CY-04 Cryptographic Key Management OP-06 Backup and Restore OP-08 Event Logging, Alerting and Auditing OP-09 Security Information and Event Management (SIEM) SR-03 ICT Supply Chain Management SR-04 Security Tests and Controls Audit IM-01 Information Security Incident Management CP-01 Independent Review of Information Security

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
			• The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work. • Patient treatment data is lost so cannot be provided to joint organisations (detrimental to patient care). • Data re-entry causing time delays for agency staff to respond to incidents. • Revenue loss, through reduced ability to charge for provided services (ambulance charge). • Loss in confidence of agencies' security measures for access to third-party services (NHI, DHB). • The organisation may be in breach of contractual agreements with third parties (e.g. DHBs).		

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
R08	One or more PSN services is unavailable due to a Denial of Service (DoS) attack, significant spike in usage, or resource limitations. This results in: • Communications channels being unavailable; • Information or communications being lost or inaccessible; or • Delays to incident response. **Affects:** Availability	• PSN services may be shared with other supplier customers. • PSN services may be an attractive target for attackers. • Large amounts of traffic could be needed at network edges that may not have the required capacity. • Effective load balancing may not be in place. • Services may not have been load tested. • Public use of communications infrastructure may impact agency use. • Atmospheric conditions may limit network throughput (wireless/satellite). • The supplier may reprioritise traffic for larger customers.	• Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost. • The personal security of individuals being protected by an agency could be compromised. • Delays may be experienced in agencies' response to emergencies. • Staff safety may be compromised through lack of communication. • Extended outage would have a detrimental impact on patient outcomes. • Inability to route traffic via diverse networks (e.g. Spark, Vodafone). • The organisation's public reputation could be adversely affected.	SR-01 Contractual Agreements and SLAs SR-04 Security Tests and Controls Audit IM-01 Information Security Incident Management CP-02 Architecture and Design Review IS-04 Mobile Device Management (MDM) IM-04 High Availability and Fault Tolerance	OP-03 Performance and Capacity Management CS-02 Intrusion Detection and Prevention CS-04 Firewalls CS-05 DoS Protection SR-04 Security Tests and Controls Audit IM-04 High Availability and Fault Tolerance OP-08 Event Logging, Alerting and Auditing CP-01 Independent Review of Information Security SA-02 Secure Application

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
			• Agencies that rely on donations could suffer financially due to loss of trust in their work.		
R09	PSN Services are disrupted or unavailable due to a man-made event, outage or natural disaster. This results in: • Communications channels being unavailable; or • Information or communications being lost or inaccessible. **Affects:** Availability	• PSN equipment is spread across a large geographical area. • PSN equipment is exposed to extreme weather events. • PSN equipment is affected by atmospheric conditions (e.g. solar activity). • New Zealand has many active earthquake faults. • Networks may not have capacity to deal with increased load during a disaster.	• Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost. • The personal security of individuals being protected by an agency could be compromised. • Delays may be experienced in agencies' response to emergencies. • Staff safety may be compromised through lack of communication. • An agency's ability to respond to a natural disaster may be diminished.	PE-02 Facility and Equipment Protection SA-03 Due Diligence SR-01 Contractual Agreements and SLAs SR-03 ICT Supply Chain Management IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning OP-01 Standard Operating Procedures CP-02 Architecture and Design Review IM-04 High Availability and Fault Tolerance	PE-02 Facility and Equipment Protection IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning IM-04 High Availability and Fault Tolerance OP-03 Performance and Capacity Management OP-06 Back-up and Restore CS-03 Tenant Segregation SR-03 ICT Supply Chain Management SR-04 Security Tests and Controls Audit CP-01 Independent Review of Information Security

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
			• Extended outage would have a detrimental impact on patient outcomes. • Inability to route traffic via diverse networks (e.g. Spark, Vodafone). • The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work.		
R10	PSN service suffers a hardware (e.g. server, communications tower) or software failure. This results in: • Some or all communications channels being unavailable; • Information or communications being lost or inaccessible; or • Delays to incident response.	• PSN equipment is exposed to extreme weather events. • Change management processes may be inadequate. • Release management processes may be inadequate. • Asset lifecycles may not be sufficiently managed.	• Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost. • The personal security of individuals being protected by an agency could be compromised.	SR-01 Contractual Agreements and SLAs SA-03 Due Diligence IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning CP-02 Architecture and Design Review	AM-01 Asset Lifecycle Management PE-02 Facility and Equipment Protection OP-02 Change Management OP-06 Backup and Restore OP-07 Data Resiliency OP-08 Event Logging, Alerting and Auditing OP-12 Release Management SR-04 Security Tests and Controls Audit

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
	Affects: Availability		• Delays may be experienced in agencies' response to emergencies. • Staff safety may be compromised through lack of communication. • The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work.		IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning IM-04 High Availability and Fault Tolerance CP-01 Independent Review of Information Security
R11	A supplier administrator accidently misconfigures PSN services. This results in information being: • Viewed or heard by unauthorised persons; or • Information or communications being lost or inaccessible. **Affects:**	• User access management processes may be inadequate or may not be followed. • Supplier administrator training may be inadequate. • Change management processes may be inadequate. • Release management processes may be inadequate.	• Personal information is accessed by unauthorised parties. • Sensitive information regarding operations is accessed by unauthorised parties. • Ongoing operational activities are compromised due to information being released. • Communications are interrupted at a critical time resulting in death or injury	SR-01 Contractual Agreements and SLAs SA-03 Due Diligence IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning CP-02 Architecture and Design Review	OP-02 Change Management OP-06 Backup and Restore OP-08 Event Logging, Alerting and Auditing OP-12 Release Management IM-01 Information Security Incident Management IM-04 High Availability and Fault Tolerance HR-03 Role-Based Training OP-01 Standard Operating Procedures

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
	Confidentiality, Integrity, Availability	• Multiple suppliers may have administrative access to a service. • Back-ups may not be in place or effective.	to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost or changed. • The personal security of individuals being protected by an agency could be compromised. • The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work.		OP-04 Separation of Pre-Production Environments OP-16 Automation and Orchestration SA-01 Documentation SR-04 Security Tests and Controls Audit CP-01 Independent Review of Information Security
R12	If a key person responsible (supplier and/or agency) for system development or support is unavailable at a critical time, the security and operation of the system may be detrimentally impacted. This may result in:	• Key personnel succession plans may be undefined or not in place. • The familiarity with the PSN services may be difficult to obtain should the need arise. • The system support documentation may be inadequate.	• Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost. • The personal security of individuals being protected	HR-03 Role-Based Training OP-01 Standard Operating Procedures IM-03 Business Continuity and Disaster Recovery Planning SA-01 Documentation	HR-03 Role-Based Training OP-01 Standard Operating Procedures IM-03 Business Continuity and Disaster Recovery Planning SA-01 Documentation SR-01 Contractual Agreements and SLAs

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
	• An inability to manage and maintain the PSN services; • Diminished capability to operate the PSN services; or • Inability to restore the PSN services following an outage or incident. **Affects:** Integrity, Availability	• Some PSN services will require higher vetting levels which can take time to clear.	by an agency could be compromised. • Delays may be experienced in agencies' response to emergencies. • Staff safety may be compromised through lack of communication. • The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work.	SR-01 Contractual Agreements and SLAs SR-05 Vendor Management	CP-01 Independent Review of Information Security
R13	Suppliers of PSN services suffer a significant supply chain interruption. This may result in: • An inability to manage and replace PSN devices; • Diminished capability to operate the PSN services; or • Inability to restore the PSN services following an outage or incident.	• Key components or devices sourced from foreign countries become unavailable. • Cost of components or devices has significantly increased due to reduced supply. • Replacement stock prioritised to other customers. • Asset lifecycles may not be sufficiently managed.	• Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Delays may be experienced in agencies' response to emergencies. • Delays may be experienced in replacing critical components or devices.	SR-01 Contractual Agreements and SLAs SA-03 Due Diligence IM-03 Business Continuity and Disaster Recovery Planning	OP-01 Standard Operating Procedures OP-06 Back-up and Restore IM-03 Business Continuity and Disaster Recovery Planning IM-04 High Availability and Fault Tolerance AM-01 Asset Lifecycle Management SR-01 Contractual Agreements and SLAs

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
	Affects: Availability	• Spare components and parts are not kept locally.	• Staff safety may be compromised through lack of communication. • The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work.		SR-03 ICT Supply Chain Management SA-03 Due Diligence CP-01 Independent Review of Information Security CP-04 Standards-based hardware and software
R14	PSN software or hardware is supplied by a company based in a foreign jurisdiction which is subject to laws forcing the implementation of backdoor access. Backdoors may be accessed by foreign state actors or other unauthorised parties resulting in communications: • Being intercepted; • Being manipulated or swapped; or • Being corrupted or lost.	• End-to-end supply chains may not be well known. • Components may be built in foreign jurisdictions not subject to New Zealand law. • Software or firmware updates may contain backdoors after purchase and installation of equipment. • Foreign jurisdiction governments or laws may change over the life of the contract.	• Personal information is accessed by unauthorised parties. • Sensitive information regarding operations is accessed by unauthorised parties. • Ongoing operational activities are compromised due to information being released. • Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of	SR-01 Contractual Agreements and SLAs SA-03 Due Diligence SA-04 Data Location and Sovereignty IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning CP-01 Independent Review of Information Security CP-02 Architecture and Design Review SR-02 Exit Strategy	CY-02 Encryption of Data in Transit CY-03 Encryption of Data at Rest CY-04 Cryptographic Key Management OP-02 Change Management OP-06 Backup and Restore OP-08 Event Logging, Alerting and Auditing OP-12 Release Management IM-01 Information Security Incident Management SR-01 Contractual Agreements and SLAs SA-03 Due Diligence

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
	Affects: Confidentiality, Integrity, Availability	• Equipment from 'safer' jurisdictions may incur significant additional cost.	staff or the public may be lost or changed. • The personal security of individuals being protected by an agency could be compromised. • The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work. • Loss in confidence of agencies' security measures for access to third-party services (NHI, DHB).		SA-04 Data Location and Sovereignty SR-04 Security Tests and Controls Audit CP-01 Independent Review of Information Security
R15	PSN data or communications traffic may be stored in or transmitted through a foreign jurisdiction. This may mean that stored data or transmissions are subject to foreign jurisdiction intercept and seizure laws resulting in a	• PSN may use cloud services operated outside of New Zealand. • Network traffic may be routed outside of New Zealand. • Foreign state data and communication laws may change over time.	• Personal information is accessed by unauthorised parties. • Sensitive information regarding operations is accessed by unauthorised parties. • Ongoing operational activities are compromised	SR-01 Contractual Agreements and SLAs SA-03 Due Diligence SA-04 Data Location and Sovereignty IM-01 Information Security Incident Management IM-03 Business Continuity and	AC-02 User and Device Access Management CY-02 Encryption of Data in Transit CY-03 Encryption of Data at Rest OP-06 Back-up and Restore IM-03 Business Continuity and Disaster Recovery Planning

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
	foreign state gaining access PSN data and transmissions. Foreign states may requisition available capacity for internal needs removing capacity from PSN. **Affects:** Confidentiality, Integrity, Availability	• Geological allegiances may change over time. • Communications traffic may not be easily rerouted to avoid foreign state interference.	due to information being released. • Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost or changed. • The personal security of individuals being protected by an agency could be compromised. • The organisation's public reputation could be adversely affected. • Agencies that rely on donations could suffer financially due to loss of trust in their work. • Loss in confidence of agencies' security measures for access to third-party services (NHI, DHB).	Disaster Recovery Planning CP-02 Architecture and Design Review SR-02 Exit Strategy SR-05 Vendor Management	IM-04 High Availability and Fault Tolerance SR-01 Contractual Agreements and SLAs SA-03 Due Diligence SA-04 Data Location and Sovereignty SR-02 Exit Strategy CP-01 Independent Review of Information Security

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
R16	One or more PSN supplier is forced out of business or is sold to another entity. This may result in: • Services no longer being supported; • Issues with service continuity during any business transition; or • Services being taken over by an untrusted entity. **Affects:** Confidentiality, Integrity, Availability	• PSN suppliers may be publicly traded entities. • PSN suppliers may experience financial difficulties. • PSN subject to government regulatory action that forces business change.	• Personal information is accessed by unauthorised parties. • Sensitive information regarding operations is accessed by unauthorised parties. • Ongoing operational activities are compromised due to information being released. • Communications are interrupted at a critical time resulting in death or injury to agency staff or the public. • Critical information related to the health and safety of staff or the public may be lost or changed. • The personal security of individuals being protected by an agency could be compromised. • The organisation's public reputation could be adversely affected.	SR-01 Contractual Agreements and SLAs SA-03 Due Diligence IM-01 Information Security Incident Management IM-03 Business Continuity and Disaster Recovery Planning IM-05 Code Escrow SR-02 Exit Strategy SR-03 ICT Supply Chain Management SR-05 Vendor Management	OP-02 Change Management OP-06 Backup and Restore OP-08 Event Logging, Alerting and Auditing OP-01 Standard Operating Procedures SR-01 Contractual Agreements and SLAs SA-01 Documentation CP-01 Independent Review of Information Security CP-04 Standards-based hardware and software

	Description	Drivers	Consequences	Recommended Controls	
				Agency	Supplier
			• Agencies that rely on donations could suffer financially due to loss of trust in their work. • Loss in confidence of agencies' security measures for access to third-party services (NHI, DHB).		

7. Control Recommendations

This section provides details of the 57 recommended security controls for the proposed PSN services.

7.1 Control to Risk Mapping

Identifier	Title	Number of Associated Risks	Applicable to	
			Agency	Supplier
IS-01	Information Security Policies	2	Y	Y
IS-04	Mobile Device Management (MDM)	2	Y	
HR-01	Human Resource Security	2	Y	Y
HR-02	Screening	1	Y	Y
HR-03	Role-Based Training	3	Y	Y
HR-04	Security Awareness	1	Y	Y
AM-01	Asset Lifecycle Management	2		Y
AM-04	Media Sanitisation and Disposal	1		Y
AC-01	Access Controls	4	Y	Y
AC-02	User and Device Access Management	4	Y	Y
AC-03	Privileged Access Management	3	Y	Y
AC-04	Secure Authentication	2	Y	Y
CY-01	Cryptographic Policy	3	Y	Y
CY-02	Encryption of Data in Transit	3		Y
CY-03	Encryption of Data at Rest	3		Y
CY-04	Cryptographic Key Management	4	Y	Y
CY-05	System and Information Integrity Verification	4	Y	
PE-01	Physical Security Perimeter	3	Y	Y
PE-02	Facility and Equipment Protection	2	Y	Y
OP-01	Standard Operating Procedures	8	Y	Y
OP-02	Change Management	4		Y
OP-03	Performance and Capacity Management	2		Y
OP-04	Separation of Pre-Production Environments	3		Y
OP-05	Malware Protection	2		Y
OP-06	Back-up and Restore	14		Y

OP-07	Data Resiliency	1		Y
OP-08	Event Logging, Alerting and Auditing	12	Y	Y
OP-09	Security Information and Event Management (SIEM)	7		Y
OP-11	Configuration Management	3	Y	Y
OP-12	Release Management	3		Y
OP-13	Patch and Vulnerability Management	2	Y	Y
OP-14	Hardening of Systems, Network Devices and Applications	2		Y
OP-15	Security Tests and Reviews	2	Y	Y
OP-16	Automation and Orchestration	3	Y	Y
CS-01	Security of Network Services	1	Y	Y
CS-02	Intrusion Detection and Prevention	4		Y
CS-03	Tenant Segregation	4	Y	Y
CS-04	Firewalls	2	Y	Y
CS-05	DoS Protection	1		Y
CS-06	Non-Disclosure and Confidentiality Agreements	3	Y	Y
CS-07	Message Integrity	3		Y
SA-01	Documentation	2	Y	Y
SA-02	Secure Application Development	4	Y	Y
SA-03	Due Diligence	7	Y	Y
SA-04	Data Location and Sovereignty	2	Y	Y
SR-01	Contractual Agreements and SLAs	14	Y	Y
SR-02	Exit Strategy	3	Y	Y
SR-03	ICT Supply Chain Management	4	Y	Y
SR-04	Security Tests and Controls Audit	12	Y	Y
IM-01	Information Security Incident Management	14	Y	Y
IM-03	Business Continuity and Disaster Recovery Planning	11	Y	Y
IM-04	High Availability and Fault Tolerance	4	Y	Y
IM-05	Code Escrow	1	Y	

CP-01	Independent Review of Information Security	16	Y	Y
CP-02	Architecture and Design Review	11	Y	
CP-03	Defence in Depth	1	Y	Y
CP-04	Standards based hardware and software	2		Y

7.2 Control Definitions

The table below provides detailed descriptions of the recommended controls to reduce the likelihood and/or impact of the risks identified.

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
Information Security Governance and Policies	IS-01	Information Security Policies	Information Security Policies form part of an information security framework that establishes the baseline set of policies, standards and guidelines that are required for the organisation to effectively manage its security risks, in line with its business requirements. The framework is designed to be flexible and extensible to: • Enable development of new policy artefacts whilst minimising the need to revise or redevelop the security policy. • Establish a structured, consistent and robust approach to the development, implementation and review of the policy artefacts. • Ensure that staff are provided with access to information that is relevant to their roles.	5.1.7 5.2
Information Security Governance and Policies	IS-04	Mobile Device Management (MDM)	Defining, documenting and managing secure mobile device configurations ensures that all devices used to access the service are hardened to a consistent baseline. Mobile Device Management also provides the ability to remotely control devices (including remote device wiping) and apply an agency's mobile device policies.	N/A
Human Resource Security	HR-01	Human Resource Security	Documented Human Resource Security processes ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are employed. Some of the processes to be considered may include: • Background checks to validate an individual's job experience, training and qualifications, and that they are of good character. • Screening through an appropriate service (e.g. Ministry of Justice check) to identify any history of criminal behaviour.	3.5.4 9 12.7.15 12.7.16 19.1.18

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			• A new staff induction process that covers their responsibilities for information security. • Ensuring that all staff, authorised third parties read and understand policies relevant to their position. • Knowledge of the Code of Conduct, Acceptable Use and/or the information security policy. • The employee's Terms and Conditions of Employment. • Processes to include monitoring and management of changes in employee circumstances and behaviour. • Ensuring that skill shortages or dependence on individual staff members are managed and minimised. • Ensuring that the organisation and third-party staff who are users or administrators receive formal training on how to perform the tasks that are relevant to their role. • Disciplinary processes to act against staff and contractors who have breached information security policy. • Termination and change of employment processes.	
Human Resource Security	HR-02	Screening	Security vetting and background verification checks on all candidates for employment (including contractors and Service Provider staff) will provide the organisation with the assurance that any prospective employee or third-party is of good character. Access to higher classification of information will require more formal security clearance through the New Zealand Security Intelligence Service (NZSIS). The use of an aftercare system will ensure that there is an ongoing process for determining an individual's suitability for their role.	9.2

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
Human Resource Security	HR-03	Role-Based Training	Ensure that organisation and third-party staff who are users or administrators receive formal training on how to perform the tasks that are relevant to their role before they are granted access to the information services and systems.	9.1.7
Human Resource Security	HR-04	Security Awareness	Providing all organisation employees and contractors with regular security awareness will ensure they are conversant with organisational policies and procedures. It will also allow for current and emerging threats to be articulated to these staff on a regular basis.	3.2.18 3.3.13 5.2.3 8.2.7 9.1 11.5.14 11.6.71 18.4.7 19.5.29 22.1.27
Asset Management	AM-01	Asset Lifecycle Management	A defined and implemented Asset Lifecycle Management process will ensure that all software and hardware components are upgraded or replaced in a timely manner, when the cessation of support is announced, extended support options would incur excessive costs or the vendor no longer intends to support the product. This may incorporate an inventory of assets and cover ownership, reissue, return, recycling, decommissioning and the destruction of organisation-owned hardware, software, mobile devices and any other removable media.	8.4.8 12.3 12.4.7 12.5 12.6 13.1 13.4 13.5 13.6

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
Asset Management	AM-04	Media Sanitisation and Disposal	A defined and implemented Media Sanitisation and Disposal process will ensure that all media and endpoint devices are sanitised prior to disposal or reuse. It will also outline the procedures to be followed if media cannot be adequately sanitised (e.g. using cryptographic erasure techniques when using cloud services). An audit trail of media undergoing sanitisation and disposal will provide the required assurance.	12.6 13.4 13.5 13.6
Access Control	AC-01	Access Controls	Establish a documented access control policy, which documents the business requirements for access, the principles for access (e.g. need-to-know, attribute based, role-based), the protection requirements for information and data, and the access control rules that will ensure these requirements are met. Specific rules may be based on business functions, processes, or user roles and responsibilities. They may also be implemented as physical or logical means. Typical access control policies need to be documented, and should cover: • Type of access control (role-based, attribute-based, condition-based). • Where and when a person can access. • What information a user or device can access. • What actions a user or device can perform. • The access rights of users or devices (e.g. read, write, delete). • The access rights of service accounts, applications, and privileged utility programmes.	8 16

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
Access Control	AC-02	User and Device Access Management	User and Device Access Management ensures information, services and systems are only accessed by users and devices who are explicitly authorised. User and Device Access Management reduces the likelihood of unauthorised access to information, services and systems through formalised and controlled procedures including: • The registering of users and devices (so that they are uniquely identifiable, accountable for their actions, and can be assigned access rights). • Provisioning of access rights for users and devices, in line with the access control policy. • Restricting and controlling of privileged access rights, in line with the access control policy. • Securely allocating user and device credential information (e.g. unique identifiers, secret authentication information). • Reviewing user and device access rights on a regular basis. • Removing or adjusting access rights of users and devices (e.g. change of a user's role or responsibilities). • De-registering or removing access rights of users and devices (e.g. upon termination or a change of their responsibilities or relationship).	9.2.6 9.2.7 16
Access Control	AC-03	Privileged Access Management	Controlling the allocation, maintenance and removal of privileged access rights will ensure that the use of administrative privileges is restricted to only those activities that require them, and not for business as usual or day-to-day activities. Privileged access rights need to be controlled through formal authorisation processes and implemented in accordance with an access control policy. Ensure that areas of conflicting duties or responsibilities are segregated. This will reduce the opportunity for unauthorised or unintentional modification, or misuse, of the organisation's information and data. In addition, appropriate segregation of	9.2.6 9.2.12 16.3 16.4.11

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			duties for administrative activities will prevent an individual compromising the security of the environment.	
Access Control	AC-04	Secure Authentication	Secure authentication is the identification and authentication mechanisms that verify the identity of a user or device. Secure authentication mechanisms need to consider the following: • Enforcing the use of unique identifiers and passwords (or passphrases) to maintain accountability. • Securely distributing authentication information or credentials. • Strong passwords managed in line with a defined access control policy. • Support for multi-factor authentication mechanisms (e.g. soft-tokens, digital certificates, and biometrics). • Enabling users to self-manage their own credentials; including first log-in, password resets, and account lock-out. • Ensure that secret authentication information (e.g. passwords, secret keys, API keys) are securely protected (e.g. use password safes, do not hardcode). At a minimum, users and devices should be authenticated with a password. Multi-factor authentication should be used where possible as it provides the strongest level of authentication. Multi-factor authentication requires a combination of at least two of the following forms of identification: • Something you know (e.g. username and password). • Something you have (e.g. hardware, software token, digital certificate). • Something you are (e.g. biometric fingerprint, a geo-location).	16.1 16.4.10 17.5.6 17.5.7 19.1
Cryptography	CY-01	Cryptographic Policy	The development and implementation of Cryptographic Policies will maximise the benefits and minimise the risks of using cryptographic techniques and help avoid inappropriate or incorrect use. These policies may include topics such as:	17

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			• Roles and responsibilities for cryptographic practices. • Approved cryptographic algorithms, protocols and key lengths. • Information on when and how to apply cryptographic controls (e.g. encrypting data at rest, hashing data in transit). • Impact of the use of cryptographic controls (content inspection, e.g. for malware detection). • Key management processes and procedures. • Secure cryptographic erasure requirements.	
Cryptography	CY-02	Encryption of Data in Transit	Ensuring business sensitive, private, or otherwise classified information that flows over the public or untrusted network such as the internet or internal networks is protected using approved cryptographic protocols, reduces the likelihood of information being disclosed to, or captured by, an unauthorised person.	8.3.5 16.1.21 17.1.36 17.2 17.3 17.4 22.1.24
Cryptography	CY-03	Encryption of Data at Rest	Ensuring business sensitive, private, or otherwise classified information stored on media is encrypted using approved encryption algorithms and protocols, and reduces the likelihood of unauthorised disclosure.	8.4.10 8.4.11 8.4.12 8.4.13 16.1.20 17.1.34 17.1.35

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
				17.1.37
Cryptography	CY-04	Cryptographic Key Management	The development, documentation and implementation of key management processes ensure that cryptographic keys are controlled throughout their lifecycle and are fit for purpose. A cryptographic key lifecycle includes: • Creation. • Storage and protection. • Distribution. • Use. • Renewal. • Recovery. • Revocation. • Destruction.	17.1.39 17.9
Cryptography	CY-05	System and Information Integrity Verification	Implementing solutions to monitor, detect, and alert on possible compromise of system and/or information integrity ensures that the integrity of the service and information is intact. System integrity verification can be achieved using tools such as File Integrity Monitoring (FIM). Information integrity can be achieved using techniques such as digital signatures, hash comparison etc.	5.5.4 7.1.5 12.1 12.4 13.1.11 16.5.12 18.2.16 20.3.13 22.2.15
Physical and Environmental Security	PE-01	Physical Security Perimeter	The use of security perimeters defines the boundary of restricted areas that contain sensitive information and/or information processing facilities. Physical protection can be achieved by creating one or more sound physical barriers.	8

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			The use of multiple barriers gives additional protection, and appropriate entry controls ensure that only authorised personnel are allowed access. Using a separate party to manage the physical access control (as opposed to the party managing logical access controls) ensures proper separation of duties.	
Physical and Environmental Security	PE-02	Facility and Equipment Protection	Ensure that locations for critical business processes and/or information processing facilities are evaluated for external threats, either natural or man-made, prior to selection. This includes evaluating against earthquakes, flooding, fire, extreme weather, civil unrest and explosions. Siting and protecting equipment reduces the risks from environmental threats and hazards, and opportunities for unauthorised access. Considerations for equipment security may include: • Locating equipment in a dedicated room. • Monitoring the environmental conditions (temperature, humidity, smoke, fire, etc.). • Restricting access to the equipment room to specific individuals. • Securing cabling and networking equipment. By ensuring environmental factors and supporting utilities are factored into equipment security considerations will provide a holistic approach to security. Some of these considerations may include: • Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. • Emergency lighting and communications should be provided. • Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms.	8.1 8.4

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			• Climate controls capable of maintaining the temperature and humidity of the environment within the hardware manufacturers' operating limits.	
Operations Security	OP-01	Standard Operating Procedures	Standard Operating Procedures provide step-by-step instructions for completing tasks and processes, so that there is assurance the processes are consistent and repeatable. They help ensure that staff using the system are provided with clear, unambiguous steps on how to carry out a function of the service. This helps reduce the opportunity for staff making mistakes when using or maintaining the service. Standard Operating Procedures also provide ICT staff with clear, unambiguous procedures that may include: • Installation and configuration of system components. • Scheduling requirements. • Instructions for handling errors and other exceptional conditions. • Special output and media handling instructions. • Tools available and their use. • Restart and recovery procedures for specific components. • Support and escalation contact, including external parties.	5.1.11 5.5 10.5.7
Operations Security	OP-02	Change Management	A documented formal Change Management process ensures all changes to system configurations (including emergency changes) are approved through a defined Change Management process. The risk of implementing any change is formally assessed as part of the approval process for all changes that could impact the security posture of the service as part of the approval process. In addition, the updating of all relevant system documentation will reflect any configuration changes (i.e. configuration changes inform the Configuration Management process).	6.3
Operations Security	OP-03	Performance and Capacity Management	A performance and capacity plan ensures that the service has adequate resources available to meet the agreed Service Level Agreements (SLAs). It includes monitoring of the service and defining and implementing expected thresholds with	12.7.19

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			automated alerts being generated when they are exceeded. Performance and capacity monitoring may also include periodic reports to ensure that SLAs and contractual agreements are being met. In addition, monitoring the performance and capacity of services and systems can provide early warning for potential security threats, as well as triggers when additional resources should be allocated to meet increased demands.	
Operations Security	OP-04	Separation of Pre-Production Environments	To prevent unauthorised access or changes to the operational environment, non-operational environments such as development, test and training environments must be separated from operational ones. Consider the following to ensure effective separation of environments: • All changes must be tested in a non-operational environment before being transferred into the operational environment. • Testing must not be done in operational environments. • Rules for the transfer or installation of software into operational environments from non-operational environments. • Users must have different accounts for operational and non-operational environments. • Operational or production data must not be used in non-operational environments, unless the same security controls are in place in the non-operational environment.	14.4.4 14.4.6 22.2.14
Operations Security	OP-05	Malware Protection	The installation of malware protection software on all endpoints and devices will reduce the likelihood of malicious code infecting the service. Configuring the protection to perform real-time checks for malware, automatically update its definition database, quarantine any infected files and automatically alert System Administrator(s) will ensure any infection is managed. Additional controls that detect and/or prevent the use of known malicious websites may also be considered.	7.1.5 7.3.8 12.7.20 14.1.8 14.1.9

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
				14.2.4 14.2.5 14.3.10 18.4.10 21.4.10 21.4.11
Operations Security	OP-06	Back-up and Restore	Defining and implementing a back-up process will ensure that all business-critical information, configurations, logs, etc. are recoverable to assist in meeting the business owner's requirements, including the Recovery Point Objective (RPO). The process may include appropriate controls required to protect the highest classification of information included in the back-up as well as regular restoration tests to confirm its effectiveness. An offline encrypted copy of all back-up may be required and maintained in a location that meets the physical and environmental security requirements for back-up media. Consideration should be given to ensuring a local copy of back-up data is held to support business continuity in case of failure of the service.	5.5.5 6.4 21.1.26
Operations Security	OP-07	Data Resiliency	Design and configure the solution to provide data resiliency (also seen as back-up). Data resiliency needs to ensure that organisation data (e.g. documents, code, configuration, logs) is prevented from being lost, corrupted or unavailable. Also define and capture processes to restore lost or corrupted data within the solution. Data resiliency considerations include: • Versioning. • Recovery and restoration (individual files, bulk files and folders). • Retention of deleted or removed data (aka soft-delete, recycle bins).	N/A

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
Operations Security	OP-08	Event Logging, Alerting and Auditing	Organisations are able to investigate and respond better to security incidents by developing and documenting their logging, alerting and reporting requirements, and also ensuring that the service can provide an adequate level of logging and reporting. Logging and reporting considerations include: • Log security and availability requirements, including retention and archiving. • The secure and reliable delivery of log information between logging components. • Any log auditing requirements (e.g. who did what and when). • The list of events associated with a system or software component to be logged.	4.4.5 7.1 8.2.7 9.4.8 9.4.9 9.4.10 12.4.5 14.1.8 14.2.7 14.3.6 16.4.11 16.5 18.3.19 18.5.8 19.1.12 19.1.13 20.4.5 21.4.11
Operations Security	OP-09	Security Information and Event Management (SIEM)	Implementing a Security Information and Event Management (SIEM) solution that is capable of log aggregation and correlation that can automatically detect and alert on selected events in real-time will provide the organisation with additional security. Many SIEM solutions are capable of detecting abnormal behaviour patterns (e.g. identification of numerous user accounts being locked out, indicating a user account enumeration and/or a brute force password attack is underway). Additionally, a	16.5

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			SIEM solution can be implemented to reflect normal business processes and alert on security logs that do not conform with business-as-usual.	
Operations Security	OP-11	Configuration Management	Configuration management is a process that establishes and maintains the consistent configuration of a solution throughout its life. It provides assurance that all solution components are configured in accordance with approved security policies, settings and standards. It also enables misconfigurations or deviations to be detected and appropriately managed. Configuration Management should cover four activities: • Configuration Identification – identifying the software and hardware assets and setting and maintaining secure configuration baselines. These may be managed in approved configuration documentation (e.g. Standard Operating Environment, As-builts) or a tool such as a Configuration Management database (CMDB). • Configuration Control – managing the configuration of each item following change requests and making updates to affected systems and documentation. • Configuration Status Accounting – being able to account for and report on the organisation's systems and components, and the current configuration of them at any time. • Configuration Verification and Audit – review the hardware and software configuration against the defined configuration item baselines, as part of security testing or formal audits.	3.3.6 5.2.3 5.5.4 5.5.5 12.2 14.1 14.2.7 18.1.10 19.1.22 19.5.26 21.1.16 22.2.15 22.3.10
Operations Security	OP-12	Release Management	A defined and implemented Release Management process will ensure software and firmware updates (including new releases) and configuration changes are deployed in a non-operational (e.g. development or test) environment prior to being deployed into production. It will also ensure that use cases, regression testing and user acceptance testing is performed in line with the scope of the changes to the system.	14.4.4 14.4.6

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
Operations Security	OP-13	Patch and Vulnerability Management	A comprehensive Patch Management strategy must be defined and implemented for services including all system components (e.g. operating systems, databases, applications and network device firmware). The strategy includes a process for monitoring appropriate sources for vulnerability alerts as well as vendors, Common Vulnerabilities and Exposures (CVE) databases and the National Cyber Security Centre (NCSC). Automated tools could provide an effective means of determining the patch and vulnerability requirements and status. The strategy also includes defining scheduled maintenance windows, the process for handling out-of-band patch releases and the evaluation of the patches in a non-operational environment before they are installed into production.	5.5.4 6.2 12.4 14.1.9 19.4.9
Operations Security	OP-14	Hardening of Systems, Network Devices and Applications	By ensuring operating systems, applications, virtual hosts and network devices are hardened in line with an appropriate hardening standard (e.g. vendor guidelines or Centre for Internet Security [CIS] benchmark) limits the opportunity for a vulnerability in the service to be exploited.	5.5.4 14.1 22.2.14
Operations Security	OP-15	Security Tests and Reviews	Security tests and reviews assess the effectiveness of security controls for a solution. These are typically conducted as internal, external or independent reviews or audit activities. Test and review activities should be conducted periodically, to provide through-life assurance that security controls are effective. • Security Testing – Security tests such as vulnerability scans, assessments or penetration tests should be performed to provide assurance that technical controls are securely implemented, and that no significant vulnerabilities exist for the solution. • Security Reviews and Audits – Reviews and audits are formal activities that review the security architecture, design, implementation and/or management of an organisation or system.	6.1

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			• Any issues or deficiencies identified during these activities need to be appropriately managed (e.g. through a defect register, remediation plan) until they are addressed.	
Operations Security	OP-16	Automation and Orchestration	Automate and Orchestrate operational tasks and processes to increase the speed and accuracy of the deployment and maintenance of information services and systems. Examples of Automation and Orchestration include: • Automated tasks (scripts, workflows, processes) • Orchestrated deployments (deployment scripts, build images, application packages).	6.2.4 7.1.5 18.1.10
Communications Security	CS-01	Security of Network Services	Ensure that network services (including those outsourced) are protected against malicious and accidental compromise by identifying and implementing appropriate security mechanisms and management processes. Means of securing network services include: • Using structured internet and network addressing and naming schemas (e.g. IPv4/6, DNS). • Identifying and creating network trust domains based on business security requirements (e.g. guest networks, user networks, etc). • Limiting access to network services and security domains (e.g. management zones). • Protecting network records using secure protocols and cryptographic technologies (e.g. DNSSEC, secure routing).	18
Communications Security	CS-02	Intrusion Detection and Prevention	Intrusion Detection and Prevention monitors network and/or system activities for malicious activity. The main functions are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. They can be deployed in four ways:	7.1.5 11.7.30 18.4

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			• Network-Based Intrusion Prevention System (NIPS): monitors the entire network for suspicious traffic by analysing protocol activity. • Wireless Intrusion Prevention Systems (WIPS): monitor a wireless network for suspicious traffic by analysing wireless networking protocols. • Network Behaviour Analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations. • Host-Based Intrusion Prevention System (HIPS): an installed software package which monitors a single host for suspicious activity by analysing events occurring within that host.	21.4.11
Communications Security	CS-03	Tenant Segregation	Tenant Segregation is achieved through the implementation of the appropriate multi-layered controls that considers the deployment (e.g. private, hybrid, public, etc.) and service model (SaaS, PaaS, IaaS). Segregation (separation) between tenants' domains ensures that tenant information and services are isolated within enforced boundaries. Proper segregation also provides assurance that incidents are contained and only impact the affected tenant and do not extend to co-tenants. Effective tenant segregation ensures that one tenant cannot deliberately or inadvertently interfere with the security of the other tenants.	22.2.14
Communications Security	CS-04	Firewalls	Firewalls are deployed to monitor and control connections and information flows between security domains. Consider the use of host-based firewalls, network-based firewalls, and web-application firewalls (WAFs) as a holistic group of firewall services. Define, document, and configure a firewall rule-base to only permit the inbound and outbound (ingress and egress) connections, protocols and ports required to support the solution. Ensure that the firewall is configured to protect against web-based	14.1.8 18.3.8 18.3.16 19.1.13 19.3 19.5.26

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			attacks, including DoS/DDoS (e.g. SYN Flooding, Smurf, ICMP Ping Flood, Fraggle attacks), SQL Injection and Cross Site Scripting (XSS).	21.4.10
Communications Security	CS-05	DoS Protection	Implement a solution to detect and prevent Denial of Service (DoS) and distributed denial of service (DDoS) attacks. These solutions need to work in conjunction with upstream network providers to be truly effective. Services must be designed to protect against non-technical Denial of Service attacks that target business processes (e.g. submitting a large number of false contact requests).	18.3.18 18.3.19
Communications Security	CS-06	Non-Disclosure and Confidentiality Agreements	Identifying, articulating and regularly reviewing the organisation's requirements for confidentiality or non-disclosure agreements reflects the organisation's needs for the protection of its information. Ensuring contracts with Service Providers, Vendors and authorised third parties incorporate appropriate non-disclosure and confidentiality agreement provides the organisation with the assurance that its information will be safe from disclosure.	2.2 4.4.8 12.7.16
Communications Security	CS-07	Message Integrity	Message Integrity is used to provide recipients with a method of authenticating the source of a message, the ability to verify the integrity of a message and non-repudiation by the sender or recipient (i.e. the sender cannot claim that they did not send the message, or, the sender can gain assurance that the recipient has received the message). Message Integrity can be implemented as formal transfer policies, procedures and/or technical controls to ensure the integrity of information when being transferred.	17.4 18.2.16
System Acquisition, Development and Maintenance	SA-01	Documentation	Documentation is the process of capturing the necessary information about the people, processes and technologies of an information service or system, to ensure the secure development, operation, management, maintenance and recovery of the information service or system.	5 6.4.7 6.4.8

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			Information service and system security documentation needs to be appropriately created, managed and maintained to ensure that it is up to date and available to those who need it.	
System Acquisition, Development and Maintenance	SA-02	Secure Application Development	Establishing rules for the development of software and systems will ensure that the developers use secure development practices such as those defined and documented by Microsoft and the Open Web Application Security Project (OWASP). Functional testing is primarily used to verify that a service or a piece of software is providing the functionality required by the business. Typically, functional testing involves evaluating and comparing each service or software function with the business requirements (including security).	14.4 14.5
System Acquisition, Development and Maintenance	SA-03	Due Diligence	Due diligence must be undertaken for the provision of the service. The organisation must: • Define and document its business requirements for information security for a specified service based on the information classification, sensitivity and value of the data. • Assess whether the documented business requirements for information security are met by the service. • Assess the long-term financial viability of the Service Provider and the sustainability of their business model. • Identify and assess any third-party dependencies the Service Provider has in the delivery of their service. • Identify in which countries the data could be processed, transmitted and/or stored in. • Seek expert legal advice on the implications of data being processed, transmitted and/or stored in those foreign jurisdictions.	2.2.5 4.4.8 12.7

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			• Clearly define the legal jurisdiction for contractual disputes relating to the use and function of the service. • Perform a limited pilot of the service to identify any issues with its adoption. • Formally plan and design service integration and data migration.	
System Acquisition, Development and Maintenance	SA-04	Data Location and Sovereignty	The use of services located outside of New Zealand's jurisdiction, or owned by foreign companies, introduces data sovereignty risk. Data stored, processed or transmitted by the service may be subject to legislation and regulation in those countries through which data is stored, processed and transmitted. Similarly, a foreign-owned service provider operating a service within New Zealand may be subject to the laws of the country where its registered head offices are located. Organisations must: • Identify in which countries the data could be processed, transmitted and/or stored in. • Seek expert legal advice on the implications of data being processed, transmitted and/or stored in those foreign jurisdictions. • Clearly define the legal jurisdiction for contractual disputes relating to the use and function of the service.	2.2.5 4.4.8 12.7
Supplier Relationships	SR-01	Contractual Agreements and SLAs	Contractual and SLAs are the only mechanisms that an organisation can use to ensure and enforce that a cloud-based and/or managed service will meet its requirements. Where a Service Provider retains direct control over ICT system operations, organisations need to ensure that contracts and associated SLAs: • Clearly define the legal jurisdiction for contractual disputes relating to the use and function of the service. • Clearly define the ownership of the data stored, processed and/or transmitted by the service.	2.3.22 2.3.23 3.3.7 4.4.8 12.7.15 12.7.16 13.1.11 22.1.22

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			• Define in which jurisdiction official information can and will be stored, processed and/or transmitted by the service. • Ensure that official and/or private information is appropriately protected to accepted information security standards in the Service Provider's environment, including back-ups and other environmental copies. • Ensure that the time to return to full service after a failure or outage, including data restoration, meets the organisation's business continuity requirements. • Require that all access to the organisation's information and systems be monitored. • Require and specify means to notify the organisation of any actual or possible unauthorised access. • Require engagement with the organisation in resolution of any information access incidents or issues. • Require regular reports be delivered from the Service Provider on their performance against the SLA's. • Require the organisation to be allowed to carry out regular audits to ensure compliance with its requirements or provide a full copy of all relevant independent third-party audit reports. • Require sufficient resiliency from the Service Provider in its own and its network provider's infrastructures to minimise the impact of infrastructure failures, denial of service and other Internet based attacks. • Ensure the contract with the Service Provider outlines clearly the services in scope and that the organisation is alerted when requiring services that are not within the scope. • Ensure that appropriate communication paths are defined, to manage the provider’s performance against the contract and SLAs. This channel is	

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			necessary for effective change management, resolving security incidents, technical issues, and breaches of SLAs.	
Supplier Relationships	SR-02	Exit Strategy	An exit strategy outlines the processes for leaving a current situation, either after a predetermined objective has been achieved or as a strategy to mitigate failure. At worst, an exit strategy will save face. At best, an exit strategy will peg a withdrawal to the achievement of an objective worth more than the cost of continued involvement. Exit strategies typically include the means to extract the organisation's settings, configurations and information from the Service Provider in a format that can be used by the organisation, to stand up the service or use the information in a different set-up.	N/A
Supplier Relationships	SR-03	ICT Supply Chain Management	Being aware of any reliance the Service Provider has on any third-party, will allow the organisation to ensure these are identified and addressed in the contracts between them and the Service Provider. This ensures that the Service Provider can provide assurance and be held accountable that these third parties meet the organisation's security requirements.	12.7
Supplier Relationships	SR-04	Security Tests and Controls Audit	Controls Auditing assesses the effectiveness of the processes and controls in place for the service. This could be done through internal or external audit. Audits are usually performed periodically to ensure that the security of the environment holding information is managed and maintained as agreed and documented. Should the Service Provider not allow customers to perform their own audits, a full copy of any independent third-party audit reports (e.g. SAS70, SSAE16 and ISO 27001), plus a statement of applicability, can provide assurance that appropriate controls are in place and that they are effectively managed and maintained. Penetration tests (when allowed), also provide assurance that controls are configured and enforced to protect against real-world attack scenarios.	4 5.8 19.5.24
Information Security Incident	IM-01	Information Security	An Information Security Incident Management process will ensure preparedness to respond to information security incidents and allows any information security	5.1.12

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
Management and Continuity		Incident Management	incidents to be responded to, contained, and dealt with in a controlled manner to minimise the impact of an event. Incident management typically includes records of previous incidents for analysis and learning purposes to help avoid future incidents. It will contain broad guidelines on what constitutes an information security incident, communication channels, the authority responsible for initiating an incident response, the steps necessary to ensure the integrity of any evidence, and the recovery process. In addition, incident management and response includes a public relations and communications plan to ensure that reputational damage is minimised. Regularly testing and validating incident management and response plans by running simulations, such as the incident response table-top exercises, helps improve readiness and provide assurance of the effectiveness of the process and the communications channels. Reviewing the Service Provider's Information Security Incident Management process with that of the organisation will allow for complementary and streamlined organisation response procedure and communications to occur.	5.6 7 11.6.69 11.7.34 14.1.12
Information Security Incident Management and Continuity	IM-03	Business Continuity and Disaster Recovery Planning	Define Business Continuity Plans (BCP) to outline how the organisation will continue to operate during and following a disruptive event. This plan needs to assess the potential impact to the essential business functions (e.g. Business Impact Assessment) and identify all dependent ICT systems that are critical for that function. The BCP should also define the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for the business function. To support the business continuity plan, a Disaster Recovery Plan needs to be defined and implemented that addresses each identified ICT service or system. This plan needs to outline the ICT response and recovery procedures, in accordance with the requirements of the overarching BCP. Develop and test these plans periodically to confirm that appropriate measures to ensure the continuity of critical business services, and the supporting ICT systems, are effective.	3.2.17 3.3.12 6.4

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
Information Security Incident Management and Continuity	IM-04	High Availability and Fault Tolerance	The implementation of High Availability and fault tolerant solutions ensures that services continue operating effectively in the event of high demand or failure some components. This involves designing and implementing components to provide a sufficient level of availability and reduce single points of failure. High Availability and fault tolerant designs may include: • Load balancing. • Component clustering. • Automated failover. • Passive and active redundancies (i.e. service, system, network).	18.3.19 19.5.24 19.5.26
Compliance	CP-01	Independent Review of Information Security	Conducting planned, regular, independent reviews of the organisation's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security), ensures that effective controls are implemented and managed. This may include undergoing a formal certification and accreditation process, to confirm that effective controls have been implemented to effectively reduce the identified risks to an acceptable level for the organisation.	4 5.8 6.1
Compliance	CP-02	Architecture and Design Review	Reviewing the architecture and design of the service ensures that it meets the functional and non-functional business requirements including adequate controls to protect the confidentiality, integrity and availability of information stored, processed or transmitted by the service. An Architecture and Design review will also assess the organisation's adoption of, and integration with, the service to ensure that the organisation's own security controls will meet the businesses requirements.	4.3 5.1.8 5.1.15 6.1.9
Compliance	CP-03	Defence in Depth	The application of defence-in-depth to the protection of systems and infrastructure is enhanced through the use of successive layers of security controls. All layers are	10.7

Group	Identifier	Title	Description	NZISM Reference V3.2, 18/07/2019
			designed to control and limit access to those with the appropriate authorisation for the site, infrastructure and system. Additionally, the use of different brands or technologies to achieve the same control objective (e.g. use different firewall vendors for internet and backend firewalls), reduces the possibility of an attacker circumventing all controls by circumventing one vendor or type of technology.	
Compliance	CP-04	Standards-based hardware and software	Adopting hardware and/or software solutions approved by the Government Communications Security Bureau (GCSB) reduces the risk of state actor interference by using devices that have been approved as meeting national security standards.	N/A