ISO 27001:2013 Controls			Control Included	Reasons for selection				Means of implementation
Controls	Section	Control Objective / Control		Legal requirements	Contractual obligations	Business requirements / adopted best practises	Risk assessment	
A.5 Information Security Policies	5.1	Management direction for information security						
	5.1.1	Policies for information security	Yes				x	Information Security Policy
	5.1.2	Review of the policies for information security	Yes				x	Information Security Policy
A.6 Organisation of information security	6.1	Internal organisation						
	6.1.1	Information security roles and responsibilities	Yes			x		OS Security Framework
	6.1.2	Segregation of duties	Yes				x	OS Security Framework RSSG Terms of Reference
	6.1.3	Contact with authorities	Yes				x	OS Security Framework Incident Management Framework
	6.1.4	Contact with special interest groups	Yes				x	OS Security Framework
	6.1.5	Information security in project management	Yes		x			Security NFR
	6.2	Mobile devices and teleworking						
	6.2.1	Mobile devices policy	Yes				x	Remote Access Policy
	6.2.2	Teleworking	Yes				x	Remote Access Policy
	7.1	Prior to employment						

ISO 27001:2013 Controls			Control Included	Reasons for selection				Means of implementation
Controls	Section	Control Objective / Control		Legal requirements	Contractual obligations	Business requirements / adopted best practises	Risk assessment	
A.7 Human resource security	7.1.1	Screening	Yes		x			Personal Security Vetting Policy
	7.1.2	Terms and conditions of employment	Yes		x			Personal Security Vetting Policy Employment Policies
	7.2	During employment						
	7.2.1	Management responsibilities	Yes				x	Essential Policies in Workday Information Security Policy in Workday
	7.2.2	Information security, education and training	Yes				x	Security September: Information Security Article Security September: Virtual Private Network article Security September: Your Digital Footprint article Mandatory e-learning packages
	7.2.3	Disciplinary process	Yes			x		Disciplinary Policy
	7.3	Termination and change of employment						
	7.3.1	Termination or change of employment responsibilities	Yes			x		Access Control Policy Disciplinary Policy Improving Performance Sickness Absence Policy
	8.1	Responsibility for assets						

ISO 27001:2013 Controls			Control Included	Reasons for selection				Means of implementation
Controls	Section	Control Objective / Control		Legal requirements	Contractual obligations	Business requirements / adopted best practises	Risk assessment	
A.8 Asset management	8.1.1	Inventory of assets	Yes				x	Software Asset Management Policy Information Asset Lists
	8.1.2	Ownership of assets	Yes				x	Software Asset Management Policy
	8.1.3	Acceptable use of assets	Yes				x	Acceptable use of electronic communications and social media policy Acceptable use terms for non-OS staff using Office 365 platform
	8.1.4	Return of assets	Yes				x	Software Asset Management Policy
	8.2	Information classification						
	8.2.1	Classification of information	Yes		x			Protective Marking Policy
	8.2.2	Labelling of information	Yes		x			Protective Marking Policy
	8.2.3	Handling of assets	Yes				x	Protective Marking Policy
	8.3	Media handling						
	8.3.1	Management of removable media	Yes				x	Removable Media Policy
	8.3.2	Disposal of media	Yes				x	Removable Media Policy Data Retention and Destruction Policy
	8.3.3	Physical media transfer	Yes				x	Removable Media Policy
A.9 Access control	9.1	Business requirements of access control						
	9.1.1	Access control policy	Yes				x	Access Control Policy

ISO 27001:2013 Controls			Control Included	Reasons for selection				Means of implementation
Controls	Section	Control Objective / Control		Legal requirements	Contractual obligations	Business requirements / adopted best practises	Risk assessment	
	9.1.2	Access to networks and network services	Yes				x	Access Control Policy
	9.2	User access management						
	9.2.1	User registration and de-registration	Yes				x	Access Control Policy
	9.2.2	User access provisioning	Yes				x	Access Control Policy
	9.2.3	Management of privileged access rights	Yes				x	Access Control Policy
	9.2.4	Management of secret authentication information of users	Yes				x	Access Control Policy
	9.2.5	Review of user access rights	Yes				x	Access Control Policy
	9.2.6	Removal or adjustment of access rights	Yes				x	Access Control Policy
	9.3	User responsibilities						
	9.3.1	User of secret authentication information	Yes				x	Password Policy How to be secure SharePoint page with advice about protecting data
	9.4	System and application access control						
	9.4.1	Information access restriction	Yes				x	Access Control Policy
	9.4.2	Secure log-on procedures	Yes			x		Password Policy Bitlocker password advice
	9.4.3	Password management system	Yes			x		Password Policy Bitlocker password advice
	9.4.4	Use of privileged utility programs	Yes				x	Acceptable use of electronic communications and social media policy

ISO 27001:2013 Controls			Control Included	Reasons for selection				Means of implementation
Controls	Section	Control Objective / Control		Legal requirements	Contractual obligations	Business requirements / adopted best practises	Risk assessment	
	9.4.5	Access control to programme source code	Yes				x	Access Control Policy
A.10 Cryptography	10.1	Cryptographic controls						
	10.1.1	Policy on the use of cryptographic controls	Yes				x	Cryptography and Encryption Policy
	10.1.2	Key management	Yes				x	Cryptography and Encryption Policy
A.11 Physical and environmental security	11.1	Secure areas						
	11.1.1	Physical security perimeter	Yes			x		Physical Security Policy
	11.1.2	Physical entry controls	Yes			x		Physical Security Policy
	11.1.3	Securing offices, rooms and facilities	Yes			x		Physical Security Policy
	11.1.4	Protecting against external and environmental threats	Yes			x		Physical Security Policy
	11.1.5	Working in secure areas	Yes				x	Physical Security Policy
	11.1.6	Delivery and loading areas	Yes				x	Physical Security Policy
	11.2	Equipment						
	11.2.1	Equipment siting and protection	Yes			x		Business Continuity Plans
	11.2.2	Supporting utilities	Yes				x	Business Continuity Plans
	11.2.3	Cabling security	Yes				x	Physical Security Policy
	11.2.4	Equipment maintenance	Yes				x	Physical Security Policy
	11.2.5	Removal of assets	Yes				x	Acceptable use of electronic communications and social media policy

ISO 27001:2013 Controls			Control Included	Reasons for selection				Means of implementation
Controls	Section	Control Objective / Control		Legal requirements	Contractual obligations	Business requirements / adopted best practises	Risk assessment	
	11.2.6	Security of equipment and assets off-premises	Yes				x	Acceptable use of electronic communications and social media policy
	11.2.7	Secure disposal or re-use of equipment	Yes				x	Data Retention and Destruction Policy
	11.2.8	Unattended user equipment	Yes				x	Acceptable use of electronic communications and social media policy
	11.2.9	Clear desk and clear screen policy	Yes			x		OS Security Framework Information Security Policy Protective Marking Policy
A.12 Operations security	12.1	Operational procedures and responsibilities						
	12.1.1	Documented operating procedures	Yes			x		Technology & Design Change Management Principles, Process and Governance Incident Management Framework Physical Security Policy
	12.1.2	Change management	Yes				x	Change Management Policy
	12.1.3	Capacity management	Yes				x	Azure Cost Optimization SharePoint SAN Port Capacity SAN Capacity (VPN needed to access)

ISO 27001:2013 Controls			Control Included	Reasons for selection				Means of implementation
Controls	Section	Control Objective / Control		Legal requirements	Contractual obligations	Business requirements / adopted best practises	Risk assessment	
	12.1.4	Separation of development, testing and operational environments	Yes				x	Network Security Policy
	12.2	Protection from malware						
	12.2.1	Controls against malware	Yes			x		Endpoint Security Policy
	12.3	Backup						
	12.3.1	Information backup	Yes		x			Backup and Recovery Policy
	12.4	Logging and monitoring						
	12.4.1	Event logging	Yes				x	Security Monitoring Policy
	12.4.2	Protection of log information	Yes				x	Security Monitoring Policy
	12.4.3	Administrator and operator logs	Yes				x	Security Monitoring Policy
	12.4.4	Clock synchronisation	Yes				x	Security Monitoring Policy
	12.5	Control of operational software						
	12.5.1	Installation of software on operational systems	Yes				x	Acceptable use of electronic communications and social media policy
	12.6	Technical Vulnerability Management						
	12.6.1	Management of technical vulnerabilities	Yes				x	Vulnerability Management Policy
	12.6.2	Restrictions on software installation	Yes				x	Acceptable use of electronic communications and social media policy
	12.7	Information systems audit considerations						
	12.7.1	Information systems audit controls	Yes				x	Information Security Policy

ISO 27001:2013 Controls			Control Included	Reasons for selection				Means of implementation
Controls	Section	Control Objective / Control		Legal requirements	Contractual obligations	Business requirements / adopted best practises	Risk assessment	
A.13 Communications security	13.1	Network security management						
	13.1.1	Network controls	Yes				x	Network Security Policy
	13.1.2	Security of network services	Yes		x			Network Security Policy
	13.1.3	Segregation of networks	Yes				x	Network Security Policy
	13.2	Information transfer						
	13.2.1	Information transfer policies and procedures	Yes		x			Data Protection Policy
	13.2.2	Agreements on information transfer	Yes		x			Data Protection Policy International Data Transfers - Supplementary Measures
	13.2.3	Electronic messaging	Yes				x	Acceptable use of electronic communications and social media policy
	13.2.4	Confidentiality or non-disclosure agreements	Yes				x	Non-Disclosure Agreements
A.14 System acquisition, development and maintenance	14.1	Security requirements of information systems						
	14.1.1	Information security requirements analysis and specification	Yes				x	Security NFR
	14.1.2	Securing application services on public networks	Yes		x			Security NFR
	14.1.3	Protecting application services transactions	Yes				x	Security NFR
	14.2	Security in development and support process						

ISO 27001:2013 Controls			Control Included	Reasons for selection				Means of implementation
Controls	Section	Control Objective / Control		Legal requirements	Contractual obligations	Business requirements / adopted best practises	Risk assessment	
	14.2.1	Secure development policy	Yes				x	Security NFR
	14.2.2	System change control procedures	Yes				x	Change Management Policy
	14.2.3	Technical review of applications after operating platform changes	Yes				x	Change Management Policy
	14.2.4	Restrictions on changes to software	Yes				x	Change Management Policy
	14.2.5	Secure system engineering principles	Yes				x	Security NFR
	14.2.6	Secure development environment	Yes				x	Security NFR
	14.2.7	Outsourced development	Yes				x	Security NFR
	14.2.8	System security testing	Yes				x	Security NFR
	14.2.9	System acceptance testing	Yes				x	Security NFR
	14.3	Test data						
	14.3.1	Protection of test data	Yes				x	Security NFR
A.15 Supplier relationships	15.1	Information security in supplier relationships						
	15.1.1	Information security policy for supplier relationships	Yes		x			Procurement Policy
	15.1.2	Addressing security within supplier agreements	Yes		x			Non-Disclosure Agreements
	15.1.3	Information and communication technology supply chain	Yes		x			Non-Disclosure Agreements
	15.2	Supplier service delivery management						
	15.2.1	Monitoring and review of supplier services	Yes				x	Procurement Policy
	15.2.2	Managing changes to supplier services	Yes				x	Procurement Policy

ISO 27001:2013 Controls				Reasons for selection				
Controls	**Section**	**Control Objective / Control**	**Control Included**	**Legal requirements**	**Contractual obligations**	**Business requirements / adopted best practises**	**Risk assessment**	**Means of implementation**
A.16 Information security incident management	16.1	Management of information security incidents and improvements						
	16.1.1	Responsibilities and procedures	Yes			x		Incident Management Framework
	16.1.2	Reporting information security events	Yes			x		Incident Management Framework
	16.1.3	Reporting information security weaknesses	Yes			x		Security and Data Protection
	16.1.4	Assessment of decision on information security events	Yes				x	Incident Management Framework
	16.1.5	Response to information security incidents	Yes			x		Incident Management Framework
	16.1.6	Learning from information security incidents	Yes			x		Incident Management Framework
	16.1.7	Collection of evidence	Yes				x	Ransomware playbook (Confidential)
A.17 Information security aspects of business continuity management	17.1	Information security continuity						
	17.1.1	Planning information security continuity	Yes		x			Business Continuity Management Framework
	17.1.2	Implementing information security continuity	Yes				x	Business Continuity Management Framework
	17.1.3	Verify, review and evaluate information security continuity	Yes				x	Business Continuity Management Framework
	17.2	Redundancies						
	17.2.1	Availability of information processing facilities	Yes				x	Business Continuity Management Framework

ISO 27001:2013 Controls			Control Included	Reasons for selection				Means of implementation
Controls	Section	Control Objective / Control		Legal requirements	Contractual obligations	Business requirements / adopted best practises	Risk assessment	
A.18 Compliance	18.1	Compliance with legal and contractual requirements						
	18.1.1	Identification of applicable legislation and contractual requirements	Yes	x				Data and Information Sharing Policy
	18.1.2	Intellectual property rights	Yes	x				Intellectual Property
	18.1.3	Protection of records	Yes	x				Data Protection Policy
	18.1.4	Privacy and protection of personally identifiable information	Yes	x				Data Protection Policy Data and Information Sharing Policy
	18.1.5	Regulation of cryptographic controls	Yes				x	Cryptography and Encryption Policy
	18.2	Information security reviews						
	18.2.1	Independent review of information security	Yes			x		Information Security Internal Audit Policy
	18.2.2	Compliance with security policies and standards	Yes			x		RSSG Terms of Reference
	18.2.3	Technical compliance review	Yes			x		RSSG Terms of Reference

1. Further Information

1.1 Document Approval

Definitive versions of this document must be approved by the Chief Information Security Officer and/or the Chief Technology Officer.

Minor versions of this document must be approved by the Governance Risk and Compliance Consultant, Information Security, Technology.

1.2 Responsibility for this document

Governance Risk and Compliance Consultant, Information Security, Technology is responsible for the content of this document.

1.3 Change History

Table 1: Change history

Issue	Date	Description	Reviewed By	Approved By
1.0	Feb 2023	First definitive version	Governance Risk and Compliance Consultant, Information Security, Technology	Chief Information Security Officer
2.0	July 2023	Second definitive version – Implementation of changes recommended by Audit 0323	Governance Risk and Compliance Consultant, Information Security, Technology	Chief Information Security Officer
2.1	Aug 2023	Minor version – Replace ISMS Scope with OS Security Framework.	Governance Risk and Compliance Consultant, Information Security, Technology	Governance Risk and Compliance Consultant, Information Security, Technology
2.2	Sept 2023	Minor version – Update links to updated documents.	Governance Risk and Compliance Consultant, Information Security, Technology	Governance Risk and Compliance Consultant, Information Security, Technology