

## 3.01 Statement of Applicability (Version 5.0)

A.5.1   Policies for information security	Contro Ref'ce		Control description	Appl- ied?	Justification for exclusion or reference Document
As 1.1 Provisions for information security An information security policy occurrent shall be approved by management, published and communicated to all employees and be estimate, approved by management, published and communicated to the service of the policies for information security and published and communicated to the period of the policies for information security. The policies for information security is settled to the policies of the policies for information security. The policies for information security shall be reviewed at planmed as the policies for information security. As 1. Internal organisation of information security roles and settlement of the policies of the policies of the policies shall be defined and allocated.  As 1. Internal organisation of information security roles and settlement of the policies shall be defined and allocated.  As 1. Internal organisation of information security represents the segregation of dulies segregation of dulies.  Conflict with special interest groups and produce opportunities for unsubstitutes shall be defined and allocated.  As 1. Conflict with authorities.  As 2. Management of the special interest groups are contracted or uninterdioral modification or information security in proyect information security shall be addressed in project management.  As 2. Management in the special interest groups are contracted properties of the policy document or information security in proyect information security in proyect information security in the project management.  As 2. Management in the project groups are contracted to the project management.  As 2. Management in project groups are contracted to the project management.  As 2. Management in project groups are contracted to the project management.  As 3. The project group of the project groups are contracted to the project groups and the project groups and the project groups are project groups and the projec	A.5	Information security policies			
management, and published and communicated to all employees and towards and towards and control and country accounts accountly and towards and control and and communicated to an employees and relevant electrical parties.  As 1.1 Review of the policies for information security.  As 3.1 Information security.  As 3.1 Information accounts are all information accounts and an employees and relevant changes occur to ensure their continuing all security.  As 3.1 Information accounts are accounts and an employees and relevant changes occur to ensure their continuing an employees.  As 3.1 Information accounts are accounts and accounts are accounted as a continuing an employee and an employees and account and accounts and accounts and accounts are accounted as a continuing and accounts and accounts and accounts and accounts and accounts are accounted and accounts account	A.5.1	Management direction for information	on security		
security intervals or f significant changes occur to narse their ocintinuing substitutions of information security.  4.6.1 Internal organisation  4.1.1 Information security roles and All information security responsibilities shall be defined and allocated.  4.1.1 Information security roles and All information security responsibilities shall be defined and allocated.  5.1.1 Information security roles and accomplishing shall be appropried to produce opportunities for unauthorized or unintentical modification or produce of the produce of th	A.5.1.1	,	management, and published and communicated to all employees and relevant external parties. A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.		
A.6.1 Information security responsibilities shall be defined and allocated. A.6.1.2 Segregation of duties Conflicting duties and areas of responsibility shall be segregated to responsibilities shall be defined and allocated. A.6.1.3 Contact with authorities Appropriate contacts with sunderstoord modification or misuse of the organization's assets. A.6.1.4 Contact with special interest groups or other specialists. A.6.1.5 Information security in project Information security information security in project Information	A.5.1.2		intervals or if significant changes occur to ensure their continuing	Y	ISMS1.00, 1.09
A 6.1.1 Contact with special interest groups of the organizations accurately in project information security in project information in project information in the security in security in project information in the security information in the security in security in project information in the security in security in security in security in project information in the security in securit					
A. 1.2 Segregation of duties of conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized curintentional modification or vival contact with authorities of contact with authorities of unauthorized curintentional modification or vival contact with authorities or unauthorized contacts with squared authorized or unintentional modification or vival contact with squared authorized or unintentional modification or vival contact with squared authorized or unintentional modification or vival contact with squared authorized or unintentional modification or vival contact with squared authorized or unintentional modification or vival contact with squared authorized or unintentional modification or vival contact with squared the project.  A. 6.1.5.1 Information security in project information security shall be addressed in project menagement, regardless of the type of the project.  A. 6.2.2 Notice device policy the project information security was security or vival or			All information and the second		101404 00 4 00
reduce opportunities for manufactors of uniformation or misuse of the organization's assets.  A 5.1.3. Contact with authorities of the comparization of the		responsibilities	, ·		<u> </u>
A 6.1.4 Contact with special interest groups is surprised to mortise with special interest groups or other specialist security from an understanded. A 6.1.5 Mobile devices and televorking information security in project information security measures shall be adopted to manage in the risks introduced by using mobile devices.  A 6.2.1 Mobile device policy			reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.		policy documents
security forums and professional associations shall be maintained.  Information security in project Immanagement Information security shall be addressed in project management, Ingardiss of the type of the project.  A compared to the project of th					
A 6.2 I Mobile devices and teleworking agreement regardless of the type of the project.  A 6.2 Mobile devices and teleworking and the security shall be addressed in project management, and the security and the security management and the security and the security management and the security management and the security management and the security management and the security of the security and the security and the security of the security of the security and the security of the security of the security and the security of	A.6.1.4	Contact with special interest groups		Υ	ISMS2.12
A 6.2   Mobile devices and teleworking   Apolicy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.  A 6.2   Teleworking   Apolicy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.  A 7.1   Prior to employment   Y   ISMS2.18    A.7.1   Prior to employment   Screening   Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and with the properties of the properties requirements, the classification of and the propionical to the business requirements, the classification of and the propionical to the business requirements, the classification of and the propionical to the business requirements, the classification of and the propionical to the business requirements and the classification of the propionical properties of the organization of the propionical state of the propionical propion	A.6.1.5		Information security shall be addressed in project management,	Υ	ISMS2.08
A 5.2.1 Mobile device policy A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices. A 7.2.1 Prior to employment A.7.1.1 Prior to employment A.7.1.1 Screening Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the preporterior than the proportional to the business requirements, the classification of the information to be accessed and the preporterior than the preporterior to the preporterior than the preporterior to the preporterior than	A 6 2		regardless of the type of the project.		
A 5.2.2 Teleworking A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites. Y ISMS2.18  A.7.1 Prior to employment  A.7.1.1 Screening Background verification checks on all candidates for employment shall be carried out in accordance with retent lews, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.  A.7.2 During employment  A.7.2.1 The contractual agreements with employees and contractors shall state the rand the organization responsibilities for information security.  A.7.2.2 Unring employment  A.7.2.1 Information labelling and handling information security in accordance with the established policies and procedures, as relevant for the result of the accessed and procedures, as relevant for the state of the organization and vision and training and regular process in place to take action against employees who have committed an information security in accordance with the established policies and procedures, as relevant for the state of the communication and change of employment  A.7.3.1 Termination and change of employment responsibilities  A.7.3.1 Termination and change of employment responsibilities  A.8.1.1 Expensibilities  A.8.1.1 Expensibility for assets  A.8.1.1 Inventory of assets  A.8.1.1 Inventory of assets  A.8.1.2 Ownership of assets  A.8.2.3 Asset management  A.8.3.4 Capital or assets  A.8.3.5 Asset management  A.8.5.1 Termination or change of employment information and communication processing facilities shall be identified and an inventory of these assets shall be identified. A will be communicated to the employment or change in employment in the even of the employment or change in employment in the even of the employment or change in employment in the even of the employment or change in employment in the even of the employment or change in employment in the even of the employment or change in employment in the ev	A.6.2.1			Υ	ISMS2.17
A.7.1 Prior to employment Sorening    Background verification checks on all candidates for employment shall be carried out in accordance with nelevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.   A.7.1.2   Terms and conditions of employment   The contractual agreements with employees and contractors shall state the rand the organization in to be accessed and the perceived risks.   A.7.2.1   Terms and conditions of employment   The contractual agreements with employees and contractors shall state the rand the organization in the same state of the organization and the perceived risks.   A.7.2.2   During employment   The contractual agreement with employees and contractors to apply information security in accordance with the established policies and procedures of the organization and training information security avareness, education and training electron and training information security avareness, education and training electron and training process in the organization and characteristic and training process in the process of the organization and policies and procedures, as relevant for their politic manufaction and characteristic and training and training and training electron and training and training and training and training and training and training electron and training and tr	A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to	Y	ISMS2.18
A.7.1.1 Screening Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethnic and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.  The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.  A.7.2 During employment  A.7.2.1 Management responsibilities  Management shall require all employees and contractors shall state their and the organization's responsibilities for information security in accordance with the established policies and procedures of the organization and under their organization.  A.7.2.1 Information labelling and handling information security awareness, education and training organization and, where relevant, contractors shall receive appropriate awareness education and training and training obtained training of training organization and communicated disciplinary process in place to take action against employees who have committed an information security breach.  A.7.2.3 Termination and change of employment information security responsibilities and duties that remain valid after termination or change of employment information security responsibilities and duties that remain valid after termination or change of employment and the employee or contractor and enforced.  A.8.1 Responsibility for assets  A.8.1.1 Inventory of assets  A.8.1.2 Ownership of assets  A.8.1.3 Acceptable use of assets  Rules for the acceptable use of information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.  A.8.2.1 Information classification  A.8.2.2 Labelling of information  A.8.2.3 Handling of assets  Procedures of the acceptable use of information of their employment in information in their processing facilities shall be identified.  A.8.3.1 Handling of assets  Procedures of the acceptable use of information of their	A.7	Human resource security			
be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.  A.7.1.2 Terms and conditions of employment The contractions here proportional to the business requirements, the classification of the information to be accessed and the perceived risks.  A.7.2.2 During employment  A.7.2.1 Management responsibilities  Management shall require all employees and contractors to apply information security in accordance with the established policies and proceedures of the organization.  A.7.2.2 Information labelling and handling information security in accordance with the established policies and proceedures of the organization and maining succession of the organization and where relevant, contractors shall receive appropriate awareness education and training and regular violet of the organization and proceedures of the organization and information and regular violet of the propriate awareness education and training and regular violet of the propriate awareness education and training and regular violet of the propriate awareness education and training and regular violet of the propriate awareness education and training and regular violet of the propriate awareness education and training and regular violet of the propriate awareness education and training and regular violet of the propriate awareness education and training and regular violet of the propriate awareness education and training and regular violet of the propriate awareness education and training and regular violets and violets and violets and proceedings and	A.7.1	Prior to employment			
A.7.1.2 Terms and conditions of employment their and the organization's responsibilities for information security.  A.7.2.1 Management responsibilities in Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.  A.7.2.2 Information labelling and handling information abelling and handling information security in accordance with the established policies and procedures of the organization.  A.7.2.3 Disciplinary process  There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.  A.7.3.1 Termination and change of employment responsibilities of change of the employee or contractor and enforced.  A.7.3.1 Termination or change of employment responsibilities and fulfiles that remain valid after termination or change of employment responsibilities in or change of employment termination or change of employment shall be defined, communicated to the employee or contractor and enforced.  A.8.1.1 Inventory of assets  A.8.1.2 Ownership of assets  Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.  A.8.1.2 Ownership of assets  Alse of the capacity of these assets shall be drawn up and maintained.  A.8.3.4 Return of assets  All employees and external party users shall require all the inventory shall be identified. documented and implemented.  A.8.2.1 Classification of information  Information shall be desirable in terms of legal requirements, value, critically and sensitivity to unauthorised disclosure or modification.  A.8.2.2 Labelling of information  Information shall be desirable in accordance with the information is abeliang shall be developed and implemented in accordance with the information classification	A.7.1.1	Screening	be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification	Y	ISMS2.01, 4.2.2
A.7.2.1 Management responsibilities	A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state	Υ	ISMS2.01, 4.2.3
information security in accordance with the established policies and procedures of the organization.  A.7.2.2 Information labelling and handling information security awareness, education and training and procedures of the organization and training and replair updates in organizational policies and procedures, as relevant, contractors shall receive appropriate awareness education and training and repular updates in organizational policies and procedures, as relevant for their job function.  A.7.2.3 Disciplinary process  There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.  A.7.3.1 Termination and change of employment responsibilities and duties that remain valid after termination or change of employment information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.  A.8.1 Responsibility for assets  A.8.1.1 Inventory of assets  A.8.1.2 Ownership of assets  A.8.1.3 Acceptable use of assets  Rules for the acceptable use of information and information processing facilities shall be identified, and an inventory shall be owned.  A.8.1.4 Return of assets  A.8.1.5 Return of assets  A.8.1.6 Return of assets  A.8.1.7 Classification of information  A.8.2.1 Information classification  A.8.2.1 Classification of information  A.8.2.2 Labelling of information  Information shall be classified in terms of legal requirements, value, critically and sensitivity to unauthorised discosure or modification.  A.8.2.2 Labelling of information  A.8.2.3 Handling of assets  Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.  A.8.3.2 Disposal of media  Media shall be disposed of securely when no longer required, using  Y ISMS2.02, 4.5.5	A.7.2	During employment			
A.7.2.2 Information labelling and handling incomplete in the properties of the organization and, where relevant, contractors shall regular updates in organizational policies and procedures, as relevant for their job function.  A.7.2.3 Disciplinary process  There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.  A.7.3.1 Termination and change of employment responsibilities are security breach.  A.7.3.1 Termination or change of employment responsibilities are security presponsibilities and duties that remain valid after termination or change of employment the employee or contractor and enforced.  A.8.1 Responsibility for assets  A.8.1.1 Inventory of assets  A.8.1.2 Ownership of assets  A.8.1.3 Acceptable use of assets  A.8.1.3 Acceptable use of assets  Rules for the acceptable use of information and information and of assets associated with information and information processing facilities shall be identified, documented and implemented.  A.8.1.1 Return of assets  A.8.1.2 Return of assets  A.8.1.3 Acceptable use of information information and information processing facilities shall be identified, documented and implemented.  A.8.1.1 Classification of information  Information shall be classified in terms of legal requirements, value, critically and sensitivity to unauthorised disclosure or modification.  A.8.2.1 Classification of information  Information shall be classified in terms of legal requirements, value, critically and sensitivity to unauthorised disclosure or modification.  A.8.2.2 Labelling of information  Information shall be classified in terms of legal requirements, value, critically and sensitivity to unauthorised disclosure or modification.  A.8.2.3 Handling of assets  Proc	A.7.2.1	Management responsibilities	information security in accordance with the established policies and	Y	ISMS1.00, 1.07
A.7.2.3 Disciplinary process	A.7.2.2	Information security awareness,	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their	Y	ISMS1.00, 1.12
A.7.3 Termination and change of employment responsibilities and duties that remain valid after responsibilities are duties that remain valid after termination or change of employment shall be defined, communicated to the employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove of termination or change in employment, not before remove the employment or the information of a sasets associated with information and information processing facilities shall be identified, documented and implemented.  A.8.1.1 Return of assets Rules for the acceptable use of information and of assets associated with information processing facilities shall be identified, documented and implemented.  A.8.2.2 Information classification  A.8.3.4 Return of assets Assets associated with information processing facilities shall be identified, documented and implemented in accordance with the information classification scheme adopted by the organization.  A.8.3.4 Handling of assets Procedures for information classification scheme adopted by the organization.  A.8.3.5 Proce	A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information	Y	ISMS2.01, 4.3.2
A.S. 1 Termination or change of employment responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.  A.B. 1 Asset management  A.B. 1 Responsibility for assets  A.B. 1.1 Inventory of assets  A.B. 1.2 Ownership of assets  A.B. 1.3 Acceptable use of assets  A.B. 1.3 Acceptable use of assets  A.B. 1.4 Return of assets  A.B. 1.4 Return of assets  A.B. 1.5 Information classification  A.B. 2.1 Classification Classification  A.B. 2.1 Classification of information  A.B. 2.1 Labelling of information  A.B. 2.2 Labelling of information  A.B. 2.3 Handling of assets  A.B. 3.3 Media handling  A.B. 3.4 Management of removable media  A.B. 3.5 Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.  A.B. 3.1 Management of removable media  Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.  A.B. 3.2 Disposal of media  A.B. 3.3 Disposal of media  A.B. 3.4 Disposal of media  A.B. 3.5 Disposal of media  A.B. 3.6 Disposal of media  A.B. 3.7 Labelling of infedia  A.B. 3.8 Disposal of media  A.B. 3.9 Disposal of media  A.B. 3.0 Disposal of media  A.B. 3.1 Management of removable media in the information ball deciration of the information classification scheme adopted by the organization.  A.B. 3.1 Management of removable media in accordance with the classification scheme adopted by the organization.  A.B. 3.1 Disposal of media  A.B. 3.2 Disposal of media	A.7.3	Termination and change of employm			
A.8.1 Responsibility for assets  A.8.1.1 Inventory of assets  A.8.1.2 Ownership of assets  A.8.1.2 Ownership of assets  A.8.1.3 Acceptable use of assets  A.8.1.3 Acceptable use of assets  Rules for the acceptable use of information and of assets associated with information and information and of assets associated with information and information and of assets associated with information and information processing facilities shall be identified, documented and implemented.  A.8.1.4 Return of assets  All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.  A.8.2 Information classification  A.8.2.1 Classification of information  Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.  A.8.2.2 Labelling of information  A.8.2.3 Handling of assets  Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.  Procedures for handling assets shall be developed and implemented in accordance with the information scheme adopted by the organization.  A.8.3.1 Management of removable media  Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.  Media shall be disposed of securely when no longer required, using  Y ISMS2.02, 4.5.5	A.7.3.1	Termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to	Y	Will be communicated in the event of termination or change in
A.8.1.1 Inventory of assets  Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.  A.8.1.2 Ownership of assets  Assets maintained in the inventory shall be owned.  Y ISMS2.11 ISMS3.03  A.8.1.3 Acceptable use of assets  Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.  A.8.1.4 Return of assets  All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.  A.8.2 Information classification  A.8.2.1 Classification of information  Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.  A.8.2.2 Labelling of information  An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.  A.8.2.3 Handling of assets  Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.  A.8.3 Media handling  A.8.3.1 Management of removable media  Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.  Media shall be disposed of securely when no longer required, using  Y ISMS2.02, 4.5.5					
shall be identified and an inventory of these assets shall be drawn up and maintained.  A.8.1.2 Ownership of assets		1 3	T		Links in
A.8.1.2 Ownership of assets	A.8.1.1	Inventory of assets	shall be identified and an inventory of these assets shall be drawn up	Y	
A.8.1.3 Acceptable use of assets  Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.  A.8.1.4 Return of assets  All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.  A.8.2 Information classification  A.8.2.1 Classification of information  Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.  A.8.2.2 Labelling of information  A.8.2.3 Handling of assets  Procedures for handling assets shall be developed and implemented in accordance with the information classification.  A.8.2.3 Media handling  A.8.3.1 Management of removable media  Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.  Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.  A.8.3.2 Disposal of media  Return of assets  Return of assets  Return of assets  All employees and external party users shall return all of the organization.  Y ISMS2.02, 4.4  ISMS2.02, 4.5  ISMS2.02, 4.5  ISMS2.09, 4.4  ISMS2.09, 4.4  ISMS2.09, 4.4  ISMS2.09, 4.4	A.8.1.2	Ownership of assets	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Y	
A.8.1.4 Return of assets All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.  A.8.2 Information classification  A.8.2.1 Classification of information Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.  A.8.2.2 Labelling of information An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.  A.8.2.3 Handling of assets Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.  A.8.3 Media handling  A.8.3.1 Management of removable media Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.  A.8.3.2 Disposal of media Media shall be disposed of securely when no longer required, using Y ISMS2.02, 4.5.5	A.8.1.3	Acceptable use of assets	with information and information processing facilities shall be identified,	Y	
A.8.2 Information classification  A.8.2.1 Classification of information Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.  A.8.2.2 Labelling of information An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.  A.8.2.3 Handling of assets Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.  A.8.3 Media handling  A.8.3.1 Management of removable media Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.  A.8.3.2 Disposal of media Media shall be disposed of securely when no longer required, using Y ISMS2.02, 4.5.5	A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their	Y	ISMS2.01, 4.4.4
A.8.2.2 Labelling of information	A.8.2	Information classification			·
developed and implemented in accordance with the information classification scheme adopted by the organization.  A.8.2.3 Handling of assets Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.  A.8.3 Media handling  A.8.3.1 Management of removable media Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.  A.8.3.2 Disposal of media Media shall be disposed of securely when no longer required, using Y ISMS2.02, 4.5.5	A.8.2.1		criticality and sensitivity to unauthorised disclosure or modification.		
A.8.2.3 Handling of assets Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.  A.8.3 Media handling  A.8.3.1 Management of removable media Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.  A.8.3.2 Disposal of media Media shall be disposed of securely when no longer required, using  Y ISMS2.02, 4.5  ISMS2.09, 4.4  ISMS2.09, 4.4	A.8.2.2		developed and implemented in accordance with the information classification scheme adopted by the organization.		
A.8.3 Media handling  A.8.3.1 Management of removable media Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.  A.8.3.2 Disposal of media Media shall be disposed of securely when no longer required, using Y ISMS2.02, 4.5.5	A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the	Υ	ISMS2.02, 4.5
A.8.3.1 Management of removable media Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.  A.8.3.2 Disposal of media Media shall be disposed of securely when no longer required, using Y ISMS2.02, 4.5.5	A.8.3	Media handling	ο ι γωτικ 2010 11.		
A.8.3.2 Disposal of media Media shall be disposed of securely when no longer required, using Y ISMS2.02, 4.5.5	A.8.3.1		media in accordance with the classification scheme adopted by the	Y	ISMS2.09, 4.4
	A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using	Y	ISMS2.02, 4.5.5

A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Υ	ISMS2.09
	Access control			
A.9.1 B	Business requirements of access cor	itrol		
A.9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Y	ISMS2.06
A.9.1.2 A.9.2 U	Access to networks and network services  Jser access management	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Y	ISMS2.06, 4.1 to 4.3
A.9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be	Y	ISMS2.06, 4.1
A.9.2.1	User access provisioning	implemented to enable assignment of access rights.  A formal user access provisioning process shall be implemented to	' Y	ISMS2.06, 4.1
		assign or revoke access rights for all user types to all systems and services.		
A.9.2.3	Management of privileged access rights	controlled.	Y	ISMS2.06, 4.2
A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	Υ	ISMS2.15
A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Y	Rather than Asset Owners this review forms part of Lexer's internal
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Y	audit process. ISMS2.01, 4.4.5
A.9.3 U	Jser responsibilities	, apper consider		
A.9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	Y	ISMS2.15
	System and application access control			
A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Y	ISMS2.06
A.9.4.2 A.9.4.3	Secure log-on procedures  Password management system	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.  Password management systems shall be interactive and shall ensure	Y Y	ISMS2.02, 4.5.2
A.9.4.4	Use of privileged utility programs	quality passwords.   The use of utility programs that might be capable of overriding system	Ү	ISMS2.05, 4.3
A.9.4.5	Access control to program source code	and application controls shall be restricted and tightly controlled.  Access to program source code shall be restricted.	Υ	ISMS2.05, 4.3
A.10	Cryptology			•
A.10.1	Cryptographic controls	<del></del> -		
A.10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Y	ISMS2.09
A.10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Y	ISMS2.09, 4.4
	Physical and environment security			
	Secure areas	Convite maximum about he defined and wood to make a specifical	Y	ICMC2 02
A.11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Ť	ISMS2.03
A.11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Y	ISMS2.03
A.11.1.3 A.11.1.4	Securing offices, rooms and facilities  Protecting against external and	Physical security for offices, rooms and facilities shall be designed and applied.  Physical protection against natural disasters, malicious attack or	Y	ISMS2.03
	environmental threats	accidents shall be designed and applied.		
A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	Y	ISMS2.03, 4.4.2
A.11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	N	None exist
	Equipment	Equipment shall be alted and and anti-stade and 10 11 5	.,	May and mark and a second seco
A.11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Y	Key equipment used in the handling of RESTRICTED information is operated by AWS. This control is outsourced and controlled by contract. No requirement for internal policy.
A.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Y	Key equipment used in the handling of RESTRICTED information is operated by AWS. This control is outsourced and controlled by contract. No requirement for internal policy.
A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Y	Key equipment used in the handling of RESTRICTED information is operated by AWS. This control is outsourced and controlled by contract. No requirement for internal policy.
A.11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Y	Key equipment used in the handling of RESTRICTED information is operated by AWS. This control is outsourced and controlled by
				contract. No requirement for internal policy.

A.11.2.6	Security of equipment and assets off- premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Y	Key equipment used in the handling of RESTRICTED information is operated by AWS. This control is outsourced and controlled by contract. No requirement for internal policy.
A.11.2.7	Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Y	ISMS2.11, 4.2.1
A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Υ	ISMS2.13, 4.1 ISMS2.17 ISMS2.09, 4.1
A.11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Υ	ISMS2.13
	perations security			
	perational procedures and respon-	, , , , , , , , , , , , , , , , , , , ,		
A.12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	Υ	ISMS2.04
A.12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Y	ISMS2.08, 4.10.1 ISMS2.21, 4.8
A.12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Y	ISMS2.08, 4.9
A.12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Y	ISMS2.08, 4.5
A.12.2 P	rotection from malware			
A.12.2.1 A.12.3 B	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Y	Lexer operates ClamAV and AWS Guard Duty on all in-scope servers
A.12.3.1	Information backup	Backup copies of information, software and system images shall be	Υ	ISMS2.16
	ogging and monitoring	taken and tested regularly in accordance with an agreed backup policy.		
A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information	Υ	ISMS2.20, 4.2
A.12.4.2	Protection of log information	security events shall be produced, kept and regularly reviewed.  Logging facilities and log information shall be protected against	Y	ISMS2.20, 4.2
A.12.4.3	Administrator and operator logs	tampering and unauthorized access.  System administrator and system operator activities shall be logged and	Y	ISMS2.08, 4.2
		the logs protected and regularly reviewed.		·
A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Y	ISMS2.08, 4.6
	control of operational software			
A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Υ	ISMS2.08, 4.3, 4.4, 4.5
A.12.6 To A.12.6.1	echnical vulnerability management Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Y	ISMS2.08, 4.3, 4.4
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	Υ	ISMS2.08, 4.3, 4.4, 4.5 ISMS2.10, 4.3.1
	formation systems audit considera			
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Y	ISMS2.20
	communications security			
	letwork security management	Note and a school by a second and a school by the school b		LIOMAGO OF
A.13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Y	ISMS2.05
A.13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Y	ISMS2.05 ISMS2.07
A.13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	Υ	ISMS2.05, 4.1.3 ISMS2.08, 4.5
A.13.2.1	Information transfer policies and	Formal transfer policies, procedures and controls shall be in place to	Y	ISMS2.02, 4.4
	procedures	protect the transfer of information through the use of all types of communication facilities.		ISMS2.09, 4.3
A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	Y	ISMS2.07, 4.3 A policy on customer agreements is not considered necessary as the needs and requirements of each customer are different.
A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Y	ISMS2.10, 4.3.2 ISMS2.09, 4.3
A.13.2.4	Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Y	ISMS2.09, 4.3 ISMS2.01, 4.2.3 ISMS2.07, 4.3 All customer agreements also include a confidentiality clause but not included in a policy
A.14 S	ystem acquisition, development ar	id maintenance		mot moladed in a policy
	ecurity requirements of information			
A.14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Y	ISMS2.08
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Y	ISMS2.09, 4.3

A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message	Υ	ISMS2.09, 4.3
A 14 0 0	ourity in doublement and an	duplication or replay.		1
	ecurity in development and suppor			
A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established	Υ	ISMS2.08 ISMS2.21
A.14.2.2	System change control procedures	and applied to developments within the organization.  Changes to systems within the development lifecycle shall be controlled	Y	ISMS2.21
		by the use of formal change control procedures.		101100 00 10
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on	Υ	ISMS2.08, 4.3 ISMS2.21, 4.6
A.14.2.4	Restrictions on changes to software	organizational operations or security.  Modifications to software packages shall be discouraged, limited to	Y	ISMS2.08, 4.5
4405	packages	necessary changes and all changes shall be strictly controlled.	Υ	101400 00
.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Ť	ISMS2.08
.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration	Y	ISMS2.08, 4.5
.14.2.7	Outsourced development	efforts that cover the entire system development lifecycle.  The organization shall supervise and monitor the activity of outsourced	N	Lexer does not outsource system
	Catoda de velopment	system development.	.,	development.
.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	Y	ISMS2.08, 4.6
.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for	Y	ISMS2.21, 4.6
.14.3 Te	l est data	new information systems, upgrades and new versions.		
.14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	Y	ISMS2.08, 4.5, 4.6
	upplier relationships			1
	formation security in supplier relat	ionships		
.15.1.1	Information security in supplier relationships and information security policy for supplier	Information security requirements for mitigating the risks associated with	Y	ISMS2.07, 4.3
10. 1. 1	relationships	supplier's access to the organization's assets shall be agreed with the supplier and documented.	T	10/10/2.07, 4.3
A.15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	Y	ISMS2.07, 4.3
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Y	ISMS2.07
.15.2 S	upplier service delivery manageme			
.15.2.1	Monitoring and review of supplier	Organizations shall regularly monitor, review and audit supplier service	Υ	ISMS2.07, 4.4
	services	delivery.		
A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Y	ISMS2.07, 4.4
4.16 In	formation security incident manag			
	anagement of information security			
.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security	Υ	ISMS2.19, 4.2
.16.1.2	Reporting information security events	incidents. Information security events shall be reported through appropriate	Υ	ISMS2.19, 4.2
1.16.1.3	Reporting information security	management channels as quickly as possible.  Employees and contractors using the organization's information systems	Υ	ISMS2.19, 4.2
	weaknesses	and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.		
.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Υ	ISMS2.19, 4.1
.16.1.5	Response to information security	Information security incidents shall be responded to in accordance with	Υ	ISMS2.19, 4.1, 4.2
	incidents	the documented procedures.		
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future	Υ	ISMS2.19, 4.2
.16.1.7	Collection of evidence	Incidents.  The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Y	ISMS2.19, 4.3
.17 In	formaiton security aspects of busing			
	formation security continuity	-		
.17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Y	ISMS3.09
A.17.1.2	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Y	ISMS3.09
A.17.1.3	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Y	ISMS2.20, 4.5
1.17.2 R	edundancies	, and the same and		1
.17.2.1	Availability of information processing	Information processing facilities shall be implemented with redundancy	Y	ISMS2.03, 4.2.2
	facilities	sufficient to meet availability requirements.		
	ompliance			
1.18.1 C	ompliance with legal and contractu	ual requirements		
A.18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be	Y	ISMS2.12 Records register.
	and contractual requirements	explicitly identified, documented and kept up to date for each information system and the organization.		1. COOLGO TOGISTOIL
A.18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Y	ISMS2.12 ISMS2.10, 4.3.1
	<del>,                                      </del>			

A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification,	Υ	ISMS2.03
		unauthorized access and unauthorized release, in accordance with		ISMS2.09
		legislatory, regulatory, contractual and business requirements.		ISMS2.15
A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Υ	ISMS2.12
A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Υ	ISMS2.09, 4.9
A.18.2	Information security reviews			
A.18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Y	Refer periodic independent audit reports (including SOC 2 and penetarion tests).
A.18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Y	ISMS2.01, 4.3.1 ISMS2.20, 4.5
A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	Υ	ISMS2.20, 4.4



## This is to certify that: LEXER PTY LTD

86 Inkerman Street St. Kilda VIC 3182 AUSTRALIA

operates an

## INFORMATION SECURITY MANAGEMENT SYSTEM

which complies with the requirements of

ISO/IEC 27001:2013

for the following scope

Information security for customer data platform software as a service as per the Statement of Applicability version 5.0

Certificate No: ITGOV40074

Issued: 15 December 2021 Originally Certified: 28 January 2016 Expires: 27 January 2025 Current Certification: 14 December 2021

Frank Camasta Global Head of Technical Services SAI Global Assurance







WWW.JAS-ANZ.ORG/REGISTER



