Présentation				
Company	Shipfix Technologies SAS			
Document Version	2			
	Statement of Applicability			
Valid from	13-Sep-21			
Classification	Public			

	Classification				Publi	c				
	Stateme	nt of Applicability  Applicable ?	Setup status	Risk Assessment Output	Legal and Regulatory	Contractual Obligation	Business solutions Requirement	Best Practices	Justification	Proof
	ISO27001:2017 Statement of Applicability									
A.5 A.5.1	Information security policies Management direction for information security									
A.5.1.1	Policies for information security	•	,		,	,			To ensure our employee and relevant parties understand management direction and support for information security in accordance with business requirements and	Master List of Documents
A.5.1.2	Review of the Policies for information security	,	,				,	,	relevant laws and regulations. To ensure the continuing suitability, adequacy and effectiveness of our policies.	Check Plan
A.6 A.6.1	Organization of information security Internal organization								and checken and checken and an appropriate	
A.6.1.1	Information Security roles & responsibilities	,	,			-		,	To ensure that everyone at Shipfix understand their roles and responsibilities	* Job Description available in Notion * Security and Privacy roles available for all in Security &
A.6.1.2	Segregation of duties	,	,						and avoid possible doubt.  To reduce a) conflict of interests, b)  opportunities for unauthorised or  unintentional modification or misuse of the  organization's assets.	Privacy Homepage  *Shipfis has an org. chart (see Vanta)  *Job des defined in @Our People  *Roles available for all @Security & Privacy Homepage
A.6.1.3	Contact with authorities	,	,		,			,	organization's assets.  To be able to able to be reactive in case of crisis and to receive potential updates from the authorities related to security and privacy.	* DPO registered as such with the CNIL
A.6.1.4	Contact with special interest groups		•					,	To be able to able to be reactive in case of crisis and to receive potential updates from the special interest groups related to security and privacy	* CFO Connect (HR / Finance / Legal)
A.6.1.5	Information security in project management	•	J	v			·	,	To ensure that Shipfix addresses Information Security and Privacy in project management, regardless of the type of the project.	Information Security Policy - Chapter 21. Security in Projects
A.6.2 A.6.2.1	Mobile devices and teleworking  Mobile device policy	,					,	,	To manage the risks introduced by using	Information Security Policy
A.6.2.2	Teleworking	·	v	,			,	,	mobile devices such as Laptops To protect information accessed, processed or stored all all time and from any location given that the majority of our employees are teleworking	Information Security Policy
A.7.1	Human resource security Prior to employment									
A.7.1.1	Screening	•	,	v			,		To ensure that employees are suitable for the roles for which they are considered.	Human Resource Security Policy
A.7.1.2 A.7.2	Terms and conditions of employment  During employment	,	,				v	~	To ensure that employees and contractors understand their responsibilities.	Human Resource Security Policy
A.7.2 A.7.2.1	During employment  Management responsibilities	v	,			v		,	To ensure management's involvement in Security and Privacy matters	Human Resource Security Policy
A.7.2.2	Information security awareness, education and training	v	·	v		,		,	To ensure our employees and other relevant third parties are aware of the security risks and understand how to avoid them To ensure employee understand that	Human Resource Security Policy
A.7.2.3 A.7.3	Disciplinary process  Termination and change of employment	•	,	,	-			•	disciplinary process in place to take action against those who commit an information security and privacy breaches.	Human Resource Security Policy
A.7.3.1	Termination or change of employment responsibilities	·	v	ĭ			v	•	To ensure that information security and privacy responsibilities and duties remain valid after termination or change of employment.	Human Resource Security Policy
A.8.1	Asset management Responsibility for assets								To identify clearly all our assets are be able to	
A.8.1.1	Inventory of assets	· ·						~	prioritise in case of security or privacy incident	Asset Management Policy
A.8.1.2	Ownership of assets	v	v					,	To identify organisational assets and define appropriate protection responsibilities.	Asset Management Policy
A.8.1.3	Acceptable use of assets	v	v	~				~	To ensure appropriate use of assets by our employees or any other relevant third party	Asset Management Policy
A.8.1.4	Return of assets	·	v	٠ ا				•	To ensure that we get back the assets upon departure of employees or relevant third parties to ensure privacy and security	Asset Management Policy
A.8.2 A.8.2.1	Information classification  Classification of information			v				,	To ensure that information receives an appropriate level of protection in accordance with its importance to Shipfix.	Asset Management Policy
A.8.2.2	Labeling of information	•	•	,				•	To make sure that anyone with access to informations understands easily its level of confidentiality  To ensure that our employees and relevant	Asset Management Policy
A.8.2.3 A.8.3	Handling of assets  Media handling	•	,	,				~	third parties understands what are the security requirements relevant to each confidentiality classification	Asset Management Policy
A.8.3.1	Management of removable media	,	,	~				,	Because we do not restrict the use of removable media Because we do not restrict the use of	Asset Management Policy
A.8.3.2	Disposal of media	•	,	~				~	removable media  Because we do not restrict the use of	Asset Management Policy
A.8.3.3 A.9	Physical media transfer  Access control	v	,	,				,	removable media	Asset Management Policy
A.9.1 A.9.1.1	Business requirements of access control  Access control policy	,	,	,			,	,	To limit access to our assets and informations	Access Control Policy
A.9.1.2	Access to networks and network services	v	v	~			,	,	To prevent misuse of our networks and related services (willingly or inadvertently)	Access Control Policy
A.9.2 A.9.2.1	User access management User registration and de-registration User access provision	,	,	~			,	~	To monitor access rights To manage access rights	Access Control Policy Access Control Policy
A.9.2.2 A.9.2.3	Management of privileged access rights	Ž	ž	Ž			-	,	To prevent misuse of our systems (willingly or inadvertently)	Access Control Policy
A.9.2.4	Management of secret authentication information of users	,	,	,			,	~	To prevent unauthorised access to our systems	Access Control Policy
A.9.2.5 A.9.2.6	Review of user access rights  Removal or adjustment of access rights	,		Ž			,	,	To ensure access are al ways up to date To prevent unauthorised access to our systems upon departure or change of	Access Control Policy Access Control Policy
A.9.3	User responsibilities								responsibilities	
A.9.3.1	Use of secret authentication information	,	v	,				,	To ensure understand the importance of strong authentication	Access Control Policy
A.9.4 A.9.4.1	System and application access control Information access restriction	v	,	,				~	To limit access to our systems To prevent unauthorized access to systems	Access Control Policy
A.9.4.2 A.9.4.3	Secure log-on procedures  Password management system	v		,	L	L-	L-	, ,	and applications. To ensure the use of strong password	Access Control Policy Access Control Policy
A.9.4.4	Use of privileged utility programs	,	,	v				,	To restrict access to systems capable of overriding our informations and assets	Access Control Policy
A.9.4.5 A.10	Access control to programme source code  Crystography	v	,	v				,	To ensure we stay in control of our source code	Access Control Policy
A.10.1 A.10.1.1	Cryptographic controls (Policy is for all) Policy on the use of cryptography controls		,	v	J	J	Ţ		To ensure proper and effective use of	Cryptoography Policy
A.10.1.1	Folicy on the use or cryptography controls  Key management	,	,	,	,	,	,	,	Cryptography To ensure proper and effective use of	Cryptoography Policy
A.11 A.11.1	Physical and environmental security  Secure areas								cryptography	
A.11.1.1	Physical security perimeter	,	v	~	,			~	To give define the area with different types of restriction	Physical and Environment Security
A.11.1.2 A.11.1.3	Physical entry controls Securing offices, rooms and facilities	ž	,	,	,			,	To restrict access to our assets To ensure the respective areas are secured appropriately	Physical and Environment Security  Physical and Environment Security
A.11.1.4 A.11.1.5	Protecting against internal and environmental threats Working in secure areas	ž		J.	·			,	To ensure continuity in case of threats To ensure the security of working areas	Physical and Environment Security Physical and Environment Security Physical and Environment Security
A.11.1.6 A.11.2	Delivery and loading areas Equipment	·	Ť	Ť	_			,	To restrict access to restricted areas  To reduce the risks from environmental	Physical and Environment Security
A.11.2.1 A.11.2.2	Equipment siting and protection  Supporting utilities	,	*	,	-			•	threats and hazards, and opportunities for unauthorised access To ensure business continuity	Physical and Environment Security  Physical and Environment Security
A.11.2.3	Cabling security	Ž	ž	~	-			,	To prevent interception, interference or damage of our assets	Physical and Environment Security
A.11.2.4 A.11.2.5	Equipment maintenance Removal of assets	ÿ	,	ž	·			,	To ensure business continuity To restrict the movements of assets	Physical and Environment Security Physical and Environment Security
A.11.2.6	Security of equipment and assets off-premises	·	v	٠	-			~	To ensure security of assets including off- premise (including when working from home)	Physical and Environment Security
A.11.2.7 A.11.2.8	Secure disposal or re-use of equipment Unattended user equipment	ž	ÿ	ž	ž			,	To prevent a data leak To prevent a data leak	Physical and Environment Security Physical and Environment Security
A.11.2.9	Clear desk and clear screen policy	į	· ·	~	-			~	To prevent a data leak	Clean Desk Policy

				_		_				
A.12 A.12.1	Operations security Operational procedures and responsibilities									
A.12.1.1 A.12.1.2	Documented operating procedures  Change management	Ü	- i	v			v	,	To ensure secure operating activities To control changes to the organisation	Information Security Policy Information Security Policy
1.12.1.3	Capacity management	•	~	~			,	,	To ensure we have sufficient capacity at all time	Information Security Policy
.12.1.4	Separation of development, testing and operational environments	,		<b>.</b>			,	,	We work in separate environment to ensure unauthorised access to secure the	To add Security in Development Policy
12.2	Protection from malware								operational environment	
12.2.1	Controls against malware Backup	v	,	v			v	~	To protect our IT environment	Information Security Policy
12.3.1 12.4	Information back up Logging and monitoring	,	-	-			v	v	To be able to restore the system at any point	Backup and recovery policy
12.4.1	Event logging	,	,	,	,		,	,	To track events in order to ensure traceability	Information Security Policy
.12.4.2	Protection of log information	v		,	,		,	~	To ensure the integrity of our log data	Information Security Policy
.12.4.3	Administrator and operator logs	v	•	~	~		~	~	To track event safeguard the integrity of changes	Information Security Policy
.12.4.4	Clock synchronisation	•	~					,	to ensure we have a single reference time to maintain a traceability of our events	Information Security Policy
.12.5	Control of operational software								Control software installation to	
.12.5.1	Installation of software on operational systems	,	-					~	ensure security of our system	Information Security Policy
.12.6	Technical vulnerability management								and enhanced traceability	
.12.6.1	Management of technical vulnerabilities	,	-	-				~	To reinforces our systems and enhance availability	Information Security Policy
12.6.2	Restrictions on software installation	,		-				,	To manage the traceability of software installation	Information Security Policy
12.7	Information systems audit considerations Information systems audit controls	,	,					,	To reinforce integrity via audit controls	Audit Policy
13	Communications security Network security management	·								
13.1.1	Network controls	,	,					,	Networks managements and controls will help to protect our information in systems	Information Security Policy
10.1.1	Network controls	, ,						Ý	and applications (availability)	information security Policy
.13.1.2	Security of network controls			٦					To reinforce the security, ensure consistent service levels of all network services (mostly	Information Security Policy
		·		Ľ				Ţ	outsourced) to enhanced security and availability	
13.1.3	Segregation in networks	v		$L^{T}$	╚╻┨		L	,	To ensure the protection of information in networks	Information Security Policy
13.2 13.2.1	Information transfer Information transfer policies and procedures	,	,					,	To protect the transfer of information.	Information Security Policy
13.2.2	Agreements on information transfer	,	,					,	To secure transfer of business information between Shipfix and third-parties	Information Security Policy
13.2.3	Electronic messaging	,	~					~	To protect our emails	Information Security Policy
13.2.4	Confidentiality or non-disclosure agreements	Į ,		l				ļ	To protect our trade and ensure confidentiality of our employees and third	Information Security Policy
	,								parties during and after their relationship with Shipfix	
14 14.1	System acquisition, development and maintenance Security requirements of information systems									
14.1.1	Information security requirements analysis and specification	,		~			,	,	So InfoSec requirements are included in the requirements for information systems	Secure Development Policy
14.1.2	Securing application services on public networks	·	,	~			,	~	To be protected from fraudulent activity To preserve the integrity of our data, systems and any other	Secure Development Policy
14.1.3	Protecting application services transactions  Security in development and support processes	,	,	,			•	,	assets	Secure Development Policy
14.2.1	Secure development policy	~	~	~			v	,	To explain clearly to everyone the security measure for secure development	Secure Development Policy
14.2.2	System change control procedures	v	~	~			~	,	To secure and control the lifecycle of our development	Secure Development Policy
14.2.3	Technical review of applications after operating platform	,	-	-			~	~	To ensure availability when operating platforms are changed	Secure Development Policy
14.2.4	Restrictions on changes to software	,	,	Ţ			,	,	To ensure integrity and traceability by limiting modifications to software packages	Secure Development Policy
.14.2.5	Secure system engineering principles			,			,	,	to necessary changes	Secure Development Policy
.14.2.6	Secure development environment	ÿ		-			,	Ţ	to reinforce the overall integrity of the platform. To ensure that linfoSec is designed and implemented within the development lifecycle of information systems.	Secure Development Policy
.14.2.7	Outsourced development	0	MANNE						Shipfix does all development "in-house"  Testing is necessary for the integrity of the	Secure Development Policy
.14.2.8	System security testing	·	*	,			~	~	platform Testing is necessary for the integrity of the	Secure Development Policy
.14.2.9	System acceptance testing Test data	·	·	~			~	~	platform	Secure Development Policy
.14.3.1	Protection of test data	,	,	,			,	,	To maintain traceability of test	Secure Development Policy
.15	Supplier relationships								data	
.15.1.1	Information security in supplier relationships Information security policy for supplier relationships			,				Ţ	Because our suppliers are expected to have a	Third-Party Management Policy
.15.1.1	Addressing security potcy for supplier relationships  Addressing security within supplier agreements	,	, i	Ž			-	,	similar level of security as we do To protect our assets from our suppliers	Third-Party Management Policy
.15.1.3	Information and communication technology supply chain	,		-			,	,	Because our suppliers are expected to have a similar level of security as we do	Third-Party Management Policy
.15.2										
.15.2.1	Supplier service delivery management		1						Recause our suppliers are expected to have a	
	Supplier service delivery management  Monitoring and review of supplier services	v	,	,			~	,	Because our suppliers are expected to have a similar level of security as we do	Third-Party Management Policy
			,	v			,	,		Third-Party Management Policy Third-Party Management Policy
16	Monitoring and review of supplier services								similar level of security as we do To ensure a consistent and effective approach to security incidents	
16 16.1 16.1.1	Monitoring and review of supplier services  Managing changes to supplier services  Information security incident management Management of Information security incidents and Improvements Responsibilities and procedures	•		•		•	•	,	similar level of security as we do To ensure a consistent and effective approach to security incidents  For a consistent security management of our third parties	Third-Party Management Policy  Incident Response Plan
16 16.1 16.1.1 16.1.2	Nanaping changes to supplier services  Manaping changes to supplier services  Manaping indicate insepance  Management of information security incident insepances  Management of information security incidents and improvements  Responsibilities and procedures  Responsibilities and procedures	•		·		,	,	,	similar level of security as we do To ensure a consistent and effective approach to security incidents  For a consistent security management of our third parties To ensure traceability of security events To ensure traceability of security of secu	Third-Party Management Policy Incident Response Plan Incident Response Plan
16 16.1 16.1.1 16.1.2 16.1.3	Nontroling and review of supplier services  Managing changes to supplier services  Management of information security incident insegment  Management of information security incidents and improvements  Responsibilities and procedums	•	·	•		•	•	,	similar level of security as we do To ensure a constitute and effective approach to security incidents  For a consistent security management of our third parties To ensure traceability of security events To ensure traceability of veaknesses so we can learn from them To ensure was have the right and consistent	Third-Party Management Policy Incident Response Plan Incident Response Plan Incident Response Plan
16 16.1 16.1.1 16.1.2 16.1.3	Nanaping changes to supplier services  Manaping changes to supplier services  Manaping indicate insepance  Management of information security incident insepances  Management of information security incidents and improvements  Responsibilities and procedures  Responsibilities and procedures	•		·		,	,	,	similar level of security as we do To ensure a consistent and effective approach to security incidents  For a consistent security management of our third partie. To ensure traceability of security events To ensure traceability of security events To ensure traceability of wathresses so we can learn from them To ensure we have the right and consistent To ensure we have the right and consistent To ensure we have the right and consistent	Third-Party Management Policy  Incident Response Plan Incident Response Plan
16 16.1 16.1.1 16.1.2 16.1.3	Monitoring and review of supplier services  Managing changes to supplier services  Monation security incident immanagement  Management of Information security incidents and improvements  Responsibles and procedures  Reporting information security events  Reporting information security weaknesses  Assessment of and decision on information security events	•	•	•		,	•	•	unital teol of accurity as weld to resurve a considerat and effective approach to accurity incidents.  For a considerts security management of our hinting parties.  To ensure traceability of security overests.  To ensure traceability of security overests or to ensure traceability of security events.  To ensure traceability of security events.  To ensure the right and considerat consideration of the consideration of the purpose of traceability.  We need to response to incident according.	Third-Party Management Policy  Incident Regionse Plan
16 16.1 16.1.1 16.1.2 16.1.3	Nontroling and review of supplier services  Managing changes to supplier services  Management of information security incident insegment  Management of information security incidents and improvements  Responsibilities and procedums	•		·		,	,	,	amilar level of security as weld to resource a considerat and effective approach to security incidents.  For a consistent security management of our hint parties.  To ensure traceability of security years.  To ensure traceability of security years to resource traceability of security years.  To ensure traceability of security years to resource traceability of resource years.  To ensure we have the right and consistent classification for security years for a year parties of the parties of the years of the reports of coldent security to the procedure to avoid confusion upon security incident.	Third-Party Management Policy Incident Response Plan Incident Response Plan Incident Response Plan
16.1.1 16.1.1 16.1.1 16.1.2 16.1.3	Monitoring and review of supplier services  Managing changes to supplier services  Monation security incident immanagement  Management of Information security incidents and improvements  Responsibles and procedures  Reporting information security events  Reporting information security weaknesses  Assessment of and decision on information security events	•	•	•		,	•	•	amilar leaf of recurity as we do recurry as constant and effective approach to security incidents for a constitute curity management of our for a constitute for a constitute for a constitute for the constitute for a curity management of our for a constitute for a curity management to amount excapability of security events to amount excapability of recurring vents to manure traceability of resolutions to we can learn from them To ensure we have the right and consistent classification for security events for a purpose of traceability We need to response to incident according to the procedure to a cold confusion upon	Third-Party Management Policy  Incident Reponse Plan
16. 16.1. 16.1.1 16.1.2 16.1.3 16.1.4 16.1.5	Managing changes to supplier services  Managing changes to supplier services  Management of information security incident superservices  Management of information security incidents and improvements  Responsibilities and procedures  Responsing information security events  Reporting information security events  Assessment of and decision on information security events  Response to information security incidents  Learning from information security incidents  Collection of eventures  Collection of eventures	•		•		,	· · · · · · · · · · · · · · · · · · ·	•	unital tend of security as we do re marker as consistent and effective approach to security incidents  For a consistent security management of our thind parties. To ensure transibility of security oversis to ensure transibility to estudie to ensure the security of security oversis to ensure the base the right and consistent classification for excellently ensures for apurpose of transibility to the pro-clude transibili	Third-Party Management Policy Incident Regionse Plan
16.11 16.11 16.1.1 16.1.2 16.1.3 16.1.4 16.1.5	Managing changes to supplier services  Managing changes to supplier services  Managing incident management  Management of Information security incidents and improvements  Reporting information security events  Reporting information security events  Reporting information security events  Assessment of and decision on information security events  Response to information security incidents  Learning from information security incidents  Collection of evidence  Collection of evidence	•		•		*	•	,	unital select of security as weld to recovery a consistent security management of our third parties. For example, the consistent security management of our third parties. To ensure transability of security events. To ensure transability of security events or to ensure transability of security events for a consistent security events for a purpose of transability of security events for purpose of transability of the end to response to incident according to the pro-clude to a void confusion upon to the pro-clude transability of the end to the pro-clude transability to the pro-clude transability of the end to response to incident according to the pro-clude transability of the security and privacy systems.	Third-Party Management Policy  Incident Regionse Plan
16.1.1 16.1.1 16.1.1 16.1.2 16.1.3 16.1.4 16.1.4 16.1.5 16.1.7 17.7	Managing changes to supplier services  Managing changes to supplier services  Management of information security incident superservices  Management of information security incidents and improvements  Responsibilities and procedures  Responsing information security events  Reporting information security events  Assessment of and decision on information security events  Response to information security incidents  Learning from information security incidents  Collection of eventures  Collection of eventures	•		•		*	•	,	unital select of security as weld to resurve a consistent and effective approach to security incidents.  For a consistent security management of our third parties.  To ensure traceability of security events.  To ensure traceability of vesticeness we were consistent consistent of the consure traceability of vesticeness we were assessment when the right and consistent calculational for security events for purpose of traceability.  We need to response to incident according to the procedure to avoid confusion upon excurity incident.	Third-Party Management Policy  Incident Regionse Plan
16.11 16.1.1 16.1.1 16.1.2 16.1.3 16.1.4 16.1.5 16.1.6 16.1.7 17 17 17 17 17 17 17 17 17 17 17 17 17	Nanoping danges to supplier services  Managing changes to supplier services  Management of information security incident insegment  Management of information security incidents and improvements  Responsibilities and procedures  Responsing information security events  Reporting information security events  Assessment of and decision on information security events  Response to information security incidents  Learning from information security incidents  Collection of evidence  Enformation security incidents  Collection of evidence  Enformation security incidents					* * * * * * * * * * * * * * * * * * * *	*	•	amilar level of security as weld to resource a considerant and effective approach to security incidents.  For a consistent security management of our hind parties.  To ensure traceability of security perests.  To ensure traceability of security weeks to secure traceability of security weeks to security traceability of security security.  To ensure we have the right and consistent classification for security security or proposed for traceability or security incident.  To ensure excellent as a security and principal security and principal security in the procedure to a reconsistent for ensure continuous learning and improvement of our security and principal security in to ensure continuous learning and improvement of our security and principal security in the proposed in the the proposed in the proposed in t	Third-Party Management Policy Incident Regionse Plan
16.11 16.1.1 16.1.1 16.1.2 16.1.3 16.1.4 16.1.5 16.1.6 17.1.7 17.1.7 17.1.1	Managing changes to supplier services  Managing changes to supplier services  Managing changes to supplier services  Management of information security incident sangement  Management of information security incidents and improvements  Reporting information security events  Reporting information security events  Reporting information security weaknesses  Assessment of and decision on information security events  Response to information security incidents  Learning from information security incidents  Collection of evidence  Information security appeals of featiness continuity management.					· · · · · · · · · · · · · · · · · · ·			unital feel of fearity as we do To security readers to security management of our For a consistent security management of our Horizontal control of the cont	Third-Party Management Policy Incident Regionse Plan Budiness Continuity Plan Budiness Continuity Plan
16.16.1.1 16.1.1 16.1.2 16.1.3 16.1.4 16.1.5 16.1.6 16.1.7 17.7 17.7 17.7 17.7 17.7	Managing changes to supplier services  Managing changes to supplier services  Managing changes to supplier services  Management of information security incident management  Management of information security incidents and improvements  Responsibilities and procedures  Reporting information security events  Reporting information security wavenesses  Assessment of and decision on information security events  Response to information security incidents  Learning from information security incidents  Collection of evidence  Information security appetits of fusiones continuity management  Information security continuity  Planning information security continuity  Verify, review and evaluate information security continuity					, , , , ,	-	•	unital tend of accurity as weld to resource a consistent and effective approach to accurity incidents.  For a consistent security management of our thing parties.  To ensure traceability of security oversts.  To ensure traceability of security oversts.  To ensure traceability of security oversts.  To ensure traceability of security enders be called an incident security enders to security incident.  We meet for response to incident according to the procedure to avoid confusion upon security incident.  To ensure continuous territing and processor of the continuous territing and processor.  To ensure continuous territing end systems.  To ensure continuous territing end systems.  To ensure traceability of events.  To be prepared in case of incident and avoid confusion.	Third-Party Management Policy Incident Regionse Plan Budines Continuity Plan
16. 16. 1. 16. 1. 2 16. 1. 1 16. 1. 2 16. 1. 3 16. 1. 3 16. 1. 4 16. 1. 5 16. 1. 6 16. 1. 5 16. 1. 6 16. 1. 7 17 17. 1. 1	Managing changes to supplier services  Managing changes to supplier services  Managing changes to supplier services  Management of Information security incidents and improvements  Reporting information security incidents  Reporting information security events  Reporting information security events  Reporting information security events  Reporting information security events  Reporting information security incidents  Learning from information security incidents  Learning from information security incidents  Collection of evidence  Information security continuity  Information security continuity  Implementing information security continuity  Implementing information security continuity  Verify, review and evaluate information security continuity  Redundancies			-		· · · · · · · · · · · · · · · · · · ·			unital tend of accurity as weld to resource a consistent and effective approach to accurity incidents.  For a consistent security management of our thing parties.  To ensure traceability of security oversts.  To ensure traceability of security oversts.  To ensure traceability of security oversts.  To ensure traceability of security oversts for security incidents.  We need to response to incident according to the procedure to avoid confusion upon security incidents.  To ensure continuous terming and security incidents.  To ensure continuous terming and security incidents.  To ensure continuous terming and security incidents.  To ensure traceability of events.  To be prepared in case of incident and avoid confusion.  To ensure that our information security continuous termination security continuous continuous termination to the proposed in case of incident and avoid continuous continuous termination continuous continuous termination continuous continuous termination continuous continuo	Third-Party Management Policy  Incident Regionse Plan
16. 16. 16. 16. 16. 16. 16. 16. 16. 16.	Managing changes to supplier services  Managing changes to supplier services  Managing changes to supplier services  Management of Information security incident management  Management of Information security incidents and improvements  Reporting information security events  Reporting information security events  Reporting information security events  Reporting information security events  Reporting information security incidents  Learning from information security incidents  Learning from information security incidents  Collection of evidence  Information security assection of business continuity  Implementing information security continuity  Implementing information security continuity  Venify, review and evaluate information security continuity  Redundancies  Availability of Information processing facilities  Completions					· · · · · · · · · · · · · · · · · · ·			amilar level of security as weld to security incidents or search and effective approach to security incidents.  For a consistent security management of our thing parties.  For a consistent security management of our thing parties.  To ensure traceability of security years to security incidents.  To ensure traceability of security weens to security in consistent classification for security senses for a security incident security.  To ensure we have the right and consistent classification for security senses for a security incident.  To ensure exclude the oxident security incidents according to the procedure to avoid confusion upon security incident.  To ensure continuous learning and upon control our security and order in control oxidents.  To be prepared in case of incident according confusion.  To be prepared in case of incident according confusion.  To be prepared in case of incident and avoid confusion.  To the prepared in case of incident and avoid confusion.  To the prepared in case of incident and avoid confusion.  To the prepared in case of incident and avoid confusion.  To the prepared in case of incident and avoid confusion.  To the prepared in case of incident and avoid confusion.  To the prepared in case of incident and avoid confusion.  To the prepared in case of incident and avoid confusion.	Third-Party Management Policy Incident Regionse Plan Budines Continuity Plan Budines Continuity Plan
16 16 16 17 16 17 16 17 17 17 17 17 17 17 17 17 17 17 17 17	Nanaging changes to supplier services  Managing changes to supplier services  Managing changes to supplier services  Management of information security incident and improvements  Reponsibilities and procedures  Reporting information security verifits  Reporting information security verifits  Reporting information security events  Assessment of and decision on information security events  Response to information security incidents  Learning from information security incidents  Collection of evidence  Reformation security continuity  Planning information security continuity  Implementing information security continuity  Verify, review and evaluate information security continuity  Verify, review and evaluate information security continuity  Availability of information processing facilities  Compiliance  Compiliance with legal and contractual requirements					***			unital tend of accurity as weld to resource a consistent and effective approach to accurity incidents.  For a consistent security management of our thing parties.  To ensure traceability of security oversts.  To ensure traceability of security oversts.  To ensure traceability of security oversts.  To ensure traceability of security oversts for security incidents.  We need to response to incident according to the procedure to avoid confusion upon security incidents.  To ensure continuous terming and security incidents.  To ensure continuous terming and security incidents.  To ensure continuous terming and security incidents.  To ensure traceability of events.  To be prepared in case of incident and avoid confusion.  To ensure that our information security continuous termination security continuous continuous termination to the proposed in case of incident and avoid continuous continuous termination continuous continuous termination continuous continuous termination continuous continuo	Third-Party Management Policy  Incident Regionse Plan  Busines Continuity Plan  Business Continuity Plan
16 16.1.1 16.1 16.1 16.1.1 16.1 16.1 16.1 16.1 16.1 16.1 16.1 16.1 16.1	Managing changes to supplier services  Managing changes to supplier services  Managing changes to supplier services  Management of information security incident sangement  Management of information security incidents and improvements  Reporting information security events  Reporting information security events  Reporting information security events  Assessment of and decision on information security events  Response to information security incidents  Learning from information security incidents  Collection of evidence  Information security continuity  Planning information security continuity  Implementing information security continuity  Implementing information security continuity  Verify, review and evaluate information security continuity  Redundancies  Availability of information processing facilities  Compilation evidence  Identification of applicable legislation and contractual requirements  Identification of applicable legislation and contractual requirements					3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3			unital select of security as weld to result as a selection of security as weld to security incidents.  For a consistent security management of our third parties.  For a security management of our third parties.  To ensure traceability of security oversits.  To ensure traceability of security oversits.  To ensure traceability of security oversits for experiments of the consistent calculation for security ensures the security e	Third-Party Management Policy  Incident Regionse Plan Business Continuity Plan
16.15.1.16.1.2.16.1.2.16.1.2.16.1.3.16.1.3.16.1.3.16.1.3.16.1.4.16.1.5.1.5	Managing changes to supplier services  Managing changes to supplier services  Managing changes to supplier services  Management of Information security incident management  Management of Information security incidents and improvements.  Reporting information security events  Reporting information security events  Reporting information security events  Reporting information security events  Response to information security incidents  Learning from information security incidents  Collection of and decision on information security events  Learning from information security incidents  Collection of evidence  Information security assects of features a continuity  Implementing information security continuity  Implementing information security continuity  Venify, review and evaluate information security continuity  Redundancies  Availability of Information processing facilities  Compliance with legal and contractual requirements  Intellectual property rights				•	· · · · · · · · · · · · · · · · · · ·			unital level of leacurity as weld to recovery as weld to security incidents.  For a consistent security management of our thing particular to security management of our thing particular thing particular thing particular thing particular thing particular things and consistent to mount reaching thing security or security management of the consistent of the consistent consistent things and consistent things are purposed for travellity to the procedure to avoid consistent on purpose of travellity or to ensure the continuous things and consistent things are consistent to ensure transmitting of events.  To ensure transmitting of events  To be perspected in case of incident and avoid consistent things are consistent to the consistent things and the consistent things are consistent to the consistent things and the consistent things are consistent to the consistent things and consistent things are consistent to the consistent things and consistent things are consistent things and consistent things are consistent to the consistent things and consistent things are consistent to the consistent things and consistent things are consistent to the consistent things and consistent things are consistent things and consistent things are consistent to the consistent things and consistent things are consistent to the consistent things are consistent to the consistent things are consistent things are consistent things are consistent things are consistent to the consistent things are consistent to the consistent things are consistent things are consistent things are consistent things are consistent thi	Third-Party Management Policy  Incident Regionse Plan  Budinest Continuity Plan  Information Security Policy  Information Security Policy
16 16 16 17 16 17 16 17 17 17 17 17 17 17 17 17 17 17 17 17	Nanoging changes to supplier services  Managing changes to supplier services  Managing changes to supplier services  Management of information security incidents and improvements  Reporting information security recited services  Reporting information security events  Reporting information security events  Reporting information security events  Assessment of and decision on information security events  Response to information security incidents  Learning from information security incidents  Collection of evidence  Information security continuity  Planning information security continuity  Planning information security continuity  Verification information security continuity  Verification information security continuity  Redundancies  Availability of information processing facilities  Compliance  Learning from the legal and contractual requirements  Identification of applicable legislation and contractual requirements  Identification of applicable legislation and contractual requirements					3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3			unital level of accurity as weld to resource a considerate and effective approach to accurity incidents.  For a considerat security management of our hind parties.  For accurate transmitted or accurity process to considerate accurity management of our hind parties.  To ensure transmitting of security oversits.  To ensure transmitting or security expenses purpose of transmitting to purpose of transmitting to the procedure to avoid confusion upon security incident.  To ensure exclude to incident according to the procedure to avoid confusion upon security incident.  To ensure continuous tearning and improvement of our security and privacy to security incident.  To ensure continuous tearning and improvement of our security and privacy to security incident.  To ensure transmitting of events.  To ensure that our information security continuous contains.  To ensure that our information security continuous containsmitting of information processing facilities.  To avoid legal or contractual breaches at any time.	Third-Party Management Policy  Incident Regionse Plan
16 16.1.1 16.1.1 16.1.2 16.1.3 16.1.4 16.1.5 16.1.3 16.1.4 16.1.5 16.1.5 16.1.5 16.1.6 17.7 17.7 17.7 17.7 17.7 17.7 17	Managing changes to supplier services  Managing changes to supplier services  Managing changes to supplier services  Management of information security incidents and improvements  Reponsibilities and procedures  Reponsing information security verifits  Reporting information security events  Reporting information security events  Assessment of and decision on information security events  Assessment of and decision on information security events  Collection of and decision on information security events  Collection of evidence  Enformation security incidents  Collection of evidence  Enformation security continuity  Planning information security continuity  Implementing information security continuity  Implementing information security continuity  Verify, review and evaluate information security continuity  Availability of information processing facilities  Compliance  Compliance  Compliance with legal and contractual requirements  Intellectual property rights  Privacy and protection of personally identifiable information  Privacy and protection of personally identifiable information				·				untilar level of recorrity as we do re consumer a considerant and effective approach to security incidents  For a consistent security management of our third parties. To ensure transability of security overests To ensure transability of security overests To ensure the abouting of security overests To ensure we have the right and consistent casillation for security overtis for a purpose of transability of security overtis for a purpose of transability of the record of the re	Third-Party Management Policy  Incident Regionse Plan
16.16.11 16.1.1	Nanoging changes to supplier services  Managing changes to supplier services  Managing changes to supplier services  Management of information security incidents and improvements  Reporting information security recited services  Reporting information security events  Reporting information security events  Reporting information security events  Assessment of and decision on information security events  Response to information security incidents  Learning from information security incidents  Collection of evidence  Information security continuity  Planning information security continuity  Planning information security continuity  Verification information security continuity  Verification information security continuity  Redundancies  Availability of information processing facilities  Compliance  Learning from the legal and contractual requirements  Identification of applicable legislation and contractual requirements  Identification of applicable legislation and contractual requirements				,				untilat level of security as we do re sure as considerated and effective approach to security incidents  For a consistent security management of our third parties.  For a consistent security management of our third parties.  To ensure transability of security oversits to ensure transability of security oversits to ensure transability of security oversits to ensure the base the right and consistent classification for security oversits for purpose of transability to meet or response to incident according to the post-other to avoid confusion upon to the post-other to avoid confusion to ensure to the confusion ensuring and improvement of our security and privacy systems. To ensure the our incident and avoid constitution To be prepared in case of incident and avoid constitution To be prepared in case of incident and avoid constitution To be prepared in case of incident and avoid constitution of the properties of the properties of the prepared in case of incident and avoid constitution and prepared to avoid the prepared in avoid To ensure the avoid prepared to a service and avoid constitution and prepared to a service and avoid to be prepared in case of incident and avoid constitution and prepared to avoid the	Third-Party Management Policy  Incident Regionse Plan  Business Continuity Plan  Business Continuity Plan  Business Continuity Plan  Business Continuity Plan  Information Security Policy
16 16.11 16.11 16.12 16.13 16.14 16.15 16.	Managing changes to supplier services  Managing changes to supplier services  Managing changes to supplier services  Managing indicated management  Management of Information security incidents and improvements.  Reporting information security events  Reporting information security events  Reporting information security events  Reporting information security events  Response to information security events  Response to information security incidents  Learning from information security incidents  Confection of evidence  Information security species of fuertimess continuity  Implementing information security continuity  Implementing information security continuity  Redundancies  Availability of information processing facilities  Compilations  Compilations  Compilations with legal and contractuals requirements  Interferation of records  Interferation of processing facilities  Compilations of records  Interferation of processing facilities  Protection of records  Protection of records  Protection of records  Regulation of cryptographic controls  Regulation of cryptographic controls				,				unital is level of security as weld to reasonable the control of security management of our third parties.  For a consistent security management of our third parties.  To ensure traceability of security oversits.  To ensure traceability of security oversits.  To ensure traceability of security oversits or the consistent security oversits or security oversits or security oversits or purpose of traceability.  We need to response to incident according to the pro-cediment of security oversits for purpose of traceability.  To ensure traceability of security oversits for security oversits or security oversits or security oversits or to security oversits or to security of sevents.  To ensure that our information security effective during adverse situations.  To ensure that our information processing facilities.  To avoid legal or contractual breaches at any time.  To ensure the privacy and protection of Pit for our climits and sprite privacy and protection of Pit for our climits and sprite privacy to converte the privacy and protection of Pit for our climits and sprite privacy to cour climits and sprite privacy to converte the privacy and protection of Pit for our climits and sprite privacy to converte the sprite privacy and privacy security and privacy yearses.	Third-Party Management Policy  Incident Regionse Plan  Business Continuity Plan  Business Continuity Plan  Business Continuity Plan  Business Continuity Plan  Information Security Policy
16 16.1.1 16.1 16.1 16.1	Managing changes to supplier services  Managing changes to supplier services  Managing changes to supplier services  Management of information security incidents and improvements  Reporting information security resters  Reporting information security events  Reporting information security weaknesses  Assessment of and decision on information security events  Response to information security incidents  Learning from information security incidents  Collection of evidence  Statistics and the security incidents  Collection of evidence  Statistics and the security incidents  Collection of evidence  Variety of the security continuity  Planning information security continuity  Verify, review and evaluate information security continuity  Redundances of the security of the security continuity  Redundances of the security reviews  Redundances of the security reviews  Redundances of the security reviews  Information accountry reviews  Information of popication of personally identifiable information  Regulation of or optiographic controls  Information accountry reviews				,	3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3			amilar level of security as weld to receive a security conductor to security incidents.  For a consistent security management of our thing and the security management of our thing artists.  For a consistent security management of our thing artists.  For account of the security of security oversts.  To ensure traceability of security oversts.  To ensure traceability of security oversts or security incident.  To ensure traceability of security security of the procedure to avoid confusion upon security incident.  To ensure continuous tearning and ensuring in the procedure to avoid confusion upon security incident.  To ensure continuous tearning and ensuring in the procedure to avoid confusion upon security incident.  To ensure continuous tearning and ensuring in the procedure to avoid confusion upon security incident.  To ensure traceability of events.  To be prepared in case of incident and avoid confusion.  To ensure that our information security continuity control remain valid and effective during adverse a studient.  To avoid legal or contractual breaches at any time.  To avoid legal or contractual breaches at any time.  To ensure the avoid ballity of information processing facilities.  To ensure the avoid ballity of information processing facilities.	Third-Party Management Policy  Incident Regionse Plan  Indident Regionse Plan
1.55.22 1.56.1 1.56.1 1.66.1.1 1.66.1.1 1.66.1.5 1.66.1.5 1.66.1.5 1.66.1.6 1.66.1.7 1.77.1 1	Managing changes to suppler services  Managing changes to suppler services  Managing changes to suppler services  Management of Information security incident and improvements.  Responsible and procedures  Responsible to an optional security services  Response to information security vents  Auseument of and decision on information security events  Response to information security incidents  Learning from information security continuity  Information security continuity  Implementing information security continuity  Resultancies  Availability of information processing facilities  Compliance with legal and contractual requirements  Learnification of applicable legislation and contractual requirements  Lentification of applicable legislation and contractual requirements  Intelectual property rights  Protection of records  Privacy and protection of personally identifiable information  Regulation of cryptographic controls  Internations security reviews  Ledependent review of information security  Internations security reviews  Ledependent review of information security				,				unital select of security as we do re sure as consistent and effective approach to security incidents  for a consistent security management of our third parties. To ensure transability of security sevents To ensure transability of security sevents To ensure transability of security sevents To ensure we have the right and consistent causelears from their to ensure we have the right and consistent causelears from their their security sevents for a surption of transability of ensure the security sevents for a surption of transability of ensure continuous learning and improvement of our security and privacy system. To ensure the security of events To ensure the security of the security continuity control or ensults with a security time. To ensure that our control actual breaches at any time. To avoid right or contractual breaches at any time. To avoid right or contractual breaches at any time. To avoid right or contractual breaches at any time. To ensure that our property eventues in the eventual reaches at any time. To ensure that the pulsary presention of try to our climate and are other existing. To ensure that a supply presention to our security and privacy systems.	Third-Party Management Policy  Incident Regionse Plan  Business Continuity Plan  Business Cont

ISO27701 Statement of Applicability									
A 7	PIMS-specific reference control objectives and controls (PII Controllers)								
A 7.2	Conditions for collection and processing								
A.7.2.1	The organization shall identify and document the specific purposes for which the PII will be processed.	,	,	,	,			To identify and document the purposes for which PII are processed.	PIMS Policy - Data Controller
A.7.2.2	The organization shall determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.	,	,	,	,			To ensure that our processing activities are legally authorised	PIMS Policy - Data Controller
A.7.2.3	The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals	,	•	,	,			To have a clear mapping on consent obtention	PIMS Policy - Data Controller
A.7.2.4	The organization shall obtain and record consent from PII principals according to the documented processes.	,	,	,	,			To ensure we retain record of consent for traceability purposes	PIMS Policy - Data Controller
A.7.2.5	The organization shall assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.	•	,	,	,			To assess if an impact assessment is required for existing processing activities and new ones	PIMS Policy - Data Controller
A.7.2.6	The organization shall have a written contract with any PII processor that it uses, and shall ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B.	•	•	,	,			To ensure that we maintain a consistent approach with our processors	PIMS Policy - Data Controller
A.7.2.7	The organization shall determine respective roles and responsibilities for the processing of Pill (including Pill protection and security requirements) with any joint Pil controller.	•		,	,			We are only joint controller with our UK entity with whom we singed a joint processing agreement	PIMS Policy - Data Controller
A.7.2.8	The organization shall determine and securely maintain the necessary records in support of its obligations for the processing of PII.	,	Ţ	,	,			To maintain an up to date recording of processing activities	PIMS Policy - Data Controller
A 7.3	Obligations to PII principals								
A.7.3.1	The organization shall determine and document their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations.	,	v	,	,			To determine and document our legal, regulatory and business obligations to PII principals	PIMS Policy - Data Controller
A.7.3.2	The organization shall determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision.	,	,	`	,			To ensure we provide the appropriate information to our PII principals	PIMS Policy - Data Controller

gar							To describe the information processed to PII principale and make sure that information is	
he organization shall provide PII principals with clear and easily accessible information identifying the PII ontroller and describing the processing of their PII.	•	,	Ĭ	*			easilty available	PIMS Policy - Data Controller
he organization shall provide a mechanism for PII principals to modify or withdraw their consent.	_	_ · _	· -	-	H−Ŧ		To let PII principals amend their consent To provide a mechanism for PII principals to	PIMS Policy - Data Controller PIMS Policy - Data Controller
he organization shall provide a mechanism for PII principals to object to the processing of their PII.	~	·	~	~			object to the processing of their PII.	rims roilty - Data Controller
he organization shall implement policies, procedures and/or mechanisms to meet their obligations to PII eincipals to access, correct and/or erase their PII.	~	v	~	-			To ensure we have the rights measure in plac to let our PII principals to access, correct and/or erase their PII.	PIMS Policy - Data Controller
he organization shall inform third parties with whom PII has been shared of any modification, withdrawal or electrons pertaining to the shared PII, and implement appropriate policies, procedures and/or mechanisms do so.	v	J	·	•			The organization shall inform third parties with whom PII has been shared of any modification, withdrawal or objections pertaining to the shared PII, and implement appropriate policies, procedures and/or mechanisms to do so.	PIMS Policy - Data Controller
he organization shall be able to provide a copy of the PII that is processed when requested by the PII rincipal.	,	,	~	,			So PII principals can request a copy of the PII Processed	PIMS Policy - Data Controller
he organization shall define and document policies and procedures for handling and responding to politimate requests from PII principals.	,	,	,	~			To have a consistent approach to responding	PIMS Policy - Data Controller
The organization shall identify and address obligations, including legal obligations, to the PII principals	,	,		,			To address legal and contractual obligations	PIMS Policy - Data Controller
	,		Ľ	,			related to the automated processing of PII.	
he omanization shall first the collection of PII to the minimum that is relevant, organizational and necessary	,	,	,	~			Limit collection to what is necessary for the	PIMS Policy - Data Controller
he organization shall limit the processing of PII to that which is adequate, relevant and necessary for the			Ţ	-			To limit the collection and processing to	PIMS Policy - Data Controller
he organization shall ensure and document that PII is as accurate, complete and up-to-date as is					$\vdash$		what is strictly necessary  Accuracy and quality is paramount to ensure	PIMS Policy - Data Controller
he omanization shall define and document data minimization objectives and what mechanisms (such as de-							the integrity of our data  To ensure we have a data minimisation	PIMS Policy - Data Controller
dentification) are used to meet those objectives.			1	_			strategy	1
dentification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s).	*	,	~	~			To delete PII data when no longer necessary	PIMS Policy - Data Controller
f (e.g. erased or destroyed) following documented procedures within a specified, documented period	•	,	•	-			To ensure the safety of PII that could be present in temporary files	PIMS Policy - Data Controller
rocessed.	v		,	•	LΠ	T	To minimise the period of retention of PII data	PIMS Policy - Data Controller
r mechanisms for the disposal of PII	,	-	~	~			To clearly identify how we dispose of personal data	PIMS Policy - Data Controller
	,	,	~	,			To ensure that PII data reaches its intended	PIMS Policy - Data Controller
Il sharing, transfer and disclosure								DIME Delian Date Controller
	· ·	·	Ť				The have a clear understanding of the	PIMS Policy - Data Controller
he organization shall specify and document the countries and international organizations to which PII can ossibly be transferred	~	,	-	,			countries and international organizations to which PII can possibly be transferred.	PIMS Policy - Data Controller
he organization shall record transfers of PII to or from third parties and ensure cooperation with those arties to support future requests related to obligations to the PII principals.	v	•	·	•			We maintain a record of transfers of PII to or from third parties and ensure cooperation with those parties to support future request related to obligations to the PII principals.	PIMS Policy - Data Controller
he organization shall record disclosures of PII to third parties, including what PII has been disclosed, to shorn and at what time.	~	,	~	~			To have a system which ensure the traceability of our actions	PIMS Policy - Data Controller
PIMS-specific reference control objectives and	controls (PII							
Conditions for collection and processing								
he organization shall ensure, where relevant, that the contract to eccess Pli addresses the organization's role in providing assistance ith the customer's obligations, (taking into account the nature of	v	,	,	v		T	We need to be able to provide assistance with the customer's obligations	PIMS Policy - Data Processor
eccessing and the information available to the organization).  he organization shall ensure that PII processed on behalf of a customer re only processed for the purposes expressed in the documented statuctions of the customer.	~	,	,	,			We need to guarantee to our clients that we	PIMS Policy - Data Processor
he organization shall not use PII processed under a contract for the urposes of marketing and advertising without establishing that for consent was obtained from the appropriate PII principal. The reganization shall not make providing such consent a condition for sociting the service.	Ÿ	·	,	v			We must not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal	PIMS Policy - Data Processor
he organization shall inform the customer if, in its opinion, a processing struction infringes applicable legislation and/or regulation.	,	v	,	,			We need to inform the customer if, in our opinion, a processing instruction infringes	PIMS Policy - Data Processor
he organization shall provide the customer with the appropriate formation such that the customer can demonstrate compliance this their obligations.	,	v	v	v				PIMS Policy - Data Processor
he organization shall determine and maintain the necessary records support of demonstrating compliance with its obligations as specified in the applicable contract) for the processing of PII service of one habit of a	,	,	-	v		T	We maintain a record to support our compliance with our obligations when	PIMS Policy - Data Processor
amed out on behalf of a customer. Obligations to PII principals								
he organization shall provide the customer with the means to comply ith its obligations related to PII principals.	~		~	-			means to comply with its obligations related	PIMS Policy - Data Processor
Privacy by design and privacy by default							to PII principals.	
he organization shall ensure that temporary files created as result of the processing of Pill are disposed of (e.g. erased or estroyed) following documented procedures within a specified, ocumented period.	v	,	v	·			To ensure the safety of PII that could be present in temporary files	PIMS Policy - Data Processor
he organization shall provide the ability to return, transfer and/or liposal of Pli in a socure manner. It shall also make its policy available the customer.	•		,	Ý			To ensure that we have the ability to return, transfer and/or disposal of PII in a secure manner and that our customers have access to the relevant policy	PIMS Policy - Data Processor
he organization shall subject PII transmitted over a data-transmission etwork to appropriate controls designed to ensure that the star reaches is intended destination.	•	v	v	v			To ensure PII data are transmitted in a controlled environment	PIMS Policy - Data Processor
The sharing transfer and disclosure he organization shall inform the customer in a timely manner of the basis for PII transfers between								
urisdictions and of any intended changes in this regard, so that the customer has the ability to object to	,	•	-	,			To determine when it is justifiable to transfer data between jurisdictions  The have a clear understanding of the	PIMS Policy - Data Processor
uch changes or to terminate the contract.				-	i l		countries and international organisations to	
uch changes or to terminate the contract.  he organization shall specify and document the countries and international organizations to which PII can ossibly be transferred.	•	,	-	Ť			which PII can possibly be transferred.	PIMS Policy - Data Processor
he organization shall specify and document the countries and international organizations to which PII can	v		·	v			We maintain a record of transfers of PII to or from third parties and ensure cooperation with those parties to support future request: related to obligations to the PII principals.	PIMS Policy - Data Processor  PIMS Policy - Data Processor
The organization shall specify and document the countries and international organizations to which Pill can coasily be transferred.  The organization shall record disobsures of Pill to third parties, including what Pill has been disclosed, to thorn and when.  The organization shall notify the customer of any legally binding requests for disclosure of Pill.	•		,				We maintain a record of transfers of PII to or from third parties and ensure cooperation with those parties to support future request:	
The againstation shall specify and document the countries and international organizations to which PII can onselby be transferred.  The organization shall record disobscures of PII to third parties, including what PII has been disclosed, to horn and when.  The organization shall notify the customer of any legally binding requests for disclosure of PII.  The organization shall reject any requests for PII disclosures that one not legally binding, consult the properties of the properties of the properties of PII disclosures that one not legally binding, consult the properties of the properties of the properties of PII disclosures that one not legally binding, consult the properties of the properties of the properties of PII disclosures that one not legally binding, consult the properties of the properties of	,	,					We maintain a record of transfers of Pil to or from third parties and ensure cooperation with those parties to support future expension with those parties to support future expension for each Pil subject when we have a legally briding request for disclosure (when suthernised to disclose) So we know when to reject Pil data disclosure request (when not legally binding disclosure request (when not legally binding disclosure request (when not legally binding the pil support of the pil support of the pil support such parties of the pil support such pil support such pil support such pil support such pil support such pil such pil support such pil support such pil support such pil such pil support such pil support such pil support such pil such pil support such pil support such pil support such pil such pil such such pil such pil such such pil such pil such such pil such such pil such such pil such such pil such	PIMS Policy - Data Processor
he againstation shall exactly and document the countries and international organizations to which PII can ossibly be transferred.  In the organization shall record disclosures of PII to third parties, including what PII has been disclosed, to horn and when.  The organization shall notify the customer of any legally binding requests for disclosure of PIII.	•			·			We maintain a record of transfers of PII to or from third parties and ensure cooperation with those parties to support future request related to obligations to the PII principals. To notify PII subject when we have a legally binding request for disclosure (when authorised to disclosure).	PIMS Policy - Data Processor  PIMS Policy - Data Processor
The Part of the Pa	plimate requests from PII principals congrations had being and address obligations, including legal obligations, to the PII principals congrations had being and address obligations, including legal obligations, to the PII principals intended processing of PII.  Traces by design and privacy by default and privacy by default intended processing of PII.  Traces by design and privacy by default intended processing of PII to the minimum that is relevant, proportional and necessary for the congrations shall not the collection of PII to the winnimum that is relevant, proportional and necessary for the privacy by design and the reveal by default intended proposes.  The design of the proposes is the processed of PII to the winnimum that is relevant, proportional and necessary for the principal process.  The congration had been and document data minimum that is relevant and necessary for the privacy of the proposes for which it is processed, throughout the III-cycled of the PII.  The congration had been additional that amministant objections and what mechanisms (buch as to evaluation that the relevant design and the control and the processed) for the design and commentation objectives and what mechanisms (buch as the conjunct that the objective objectives are congrations that there design PII or ended it is a to long which does not permit destification or re- medication of PII principals, as non- as the engine PII is no longer-necessary for the design processor, in a conference of the design processor, in a congration that a longer design processor is a congration what the company files are necessary for the design processor in a congration of the processing of PII is no longer-necessary for the design processor is a congration of that have decommented policies, procedures and  **The processor of design and document the countries and international organization or and active transfer of the processor of PII between principles are organization to which PII or Insert make the processor of PII is or from third parties and en	plimate requests from PII principals.  organization hald perity and address collegations, including legal obligations, to the PII principals consisted principals and programments of the PII principals and principals	primate requests from PII principals.  organization shall enterly and address obligations, including legal obligations, to the PII principals to compare the primary of the primary of the PII principal based solely on tomated genessing of PII.  Traces by design and privacy by default and provide by default and privacy by	plimate requests from Pil principals.  organization hald perity and address obligations, including legal obligations, to the Pil principals organization or organization which are related to the Pil principals organization which are related to the Pil principal based oblig on the Pil principals organization which are related to the Pil principals organization which are directly appears to organization shall be and privacy by defining the proposes.  organization shall are decided and privacy by defining the privacy by design and privacy by defining the privacy by definite the organization of the privacy by definite the privacy by	please to expectate from Pil principals.  or cognization has a feet the processing of Pil.  or cognization has a feet the processing of Pil.  or cognization has a feet the processing of Pil.  or cognization has a feet the processing of Pil.  or cognization has a feet the processing of Pil.  or cognization has a feet the processing of Pil. to the which is adequate, preportional and necessary  or cognization has a feet the processing of Pil. to the which is adequate, revent and necessary  or cognization has a feet the processing of Pil. to the which is adequate, revent and necessary  or cognization has a feet the processing of Pil. to the which is adequate, revent and necessary for the entire of processing of Pil.  or cognization has a feet the processing of Pil. to the which is adequate, revent and necessary for the definition of the processing of Pil. to the processing of Pil. to the processing of Pil.  or cognization has a feet of the processing of Pil. to the processing of Pil. to the processing of Pil.  or cognization has a feet of the processing of Pil. to the processing of Pil. to the processing of Pil. to the processing of Pil.  or cognization has a feet of the processing of Pil. to the processing of Pil. to the processing of Pil.  or cognization has a feet of the processing of Pil. to the p	primate recognishment and processing of PII processing or comparation that foreign your and admires obligations, in this PII processing on the comparation of the comparation of the comparation of the pilot processing of PII.  **Comparation of PIII and a processing of PII and a minimum has to refer the minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and a minimum has to refer the comparation of PIII and to refer the comparation of PIII and to refer the comparation of PIII and disposed of piling disposed processing to the comparation of PIII and the comparation of PIII	planties requestly from PEI principals.  In the Committee of the Committee	princes requested from Plance outputs.  In address again, parties and process.  In address again, parties and part