IPS • Statement of applicability ISO 27001
v 1.3 | 09-08-2017

Index: LR: Legal Requirements, **CO**: Contractual Obligations, **BR**: Business Requirements/Best Practice), **RRA**: Results of Risk Assessment

Nr.	Control objectives and controls ISO 27001:2013	Applicable & Implemented Y/N	Substantation (when not applicable)	Reason of selection (see index) LR	CO	BR/BP	RRA
A.5	**Information security policies**						
A.5.1	**Management direction for information security**						
A.5.1.1	Policies for information security	Yes				■	
A.5.1.2	Review of the policies for information security	Yes				■	
A.6	**Organization of information security**						
A.6.1	**Internal organization**						
A.6.1.1	Information security roles and responsibilities	Yes				■	■
A.6.1.2	Segregation of duties	Yes				■	■
A.6.1.3	Contact with authorities	Yes		■			
A.6.1.4	Contact with special interest groups	Yes				■	
A.6.1.5	Information security in project management	No	IPS does not conduct project-based work.				
A.6.2	**Mobile devices and teleworking**						
A.6.2.1	Mobile device policy	Yes				■	
A.6.2.2	Teleworking	Yes					■
A.7	**Human resource security**						
A.7.1	**Prior to employment**						
A.7.1.1	Screening	Yes					■
A.7.1.2	Terms and conditions of employment	Yes				■	■
A.7.2	**During employment**						
A.7.2.1	Management responsibilities	Yes				■	
A.7.2.2	Information security awareness, education and training	Yes					■
A.7.2.3	Disciplinary process	Yes					■
A.7.3	**Termination and change of employment**						
A.7.3.1	Termination or change of employment responsibilities	Yes					■
A.8	**Asset management**						
A.8.1	**Responsibility for assets**						
A.8.1.1	Inventory of assets	Yes				■	■
A.8.1.2	Ownership of assets	Yes				■	■
A.8.1.3	Acceptable use of assets	Yes				■	
A.8.1.4	Return of assets	Yes				■	
A.8.2	**Information classification**						
A.8.2.1	Classification of information	Yes				■	■
A.8.2.2	Labelling of information	Yes				■	■
A.8.2.3	Handling of assets	Yes				■	
A.8.3	**Media handling**						
A.8.3.1	Management of removable media	Yes				■	
A.8.3.2	Disposal of media	Yes				■	
A.8.3.3	Physical media transfer	Yes				■	
A.9	**Access control**						
A.9.1	**Business requirements of access control**						
A.9.1.1	Access control policy	Yes				■	■
A.9.1.2	Acces to networks and network services	Yes					■
A.9.2	**User access management**						
A.9.2.1	User registration and de-registration	Yes					■
A.9.2.2	User access provisioning	Yes					■
A.9.2.3	Management of privileged access rights	Yes					■
A.9.2.4	Management of secret authentication information of users	Yes					■
A.9.2.5	Review of user access rights	Yes					■
A.9.2.6	Removal or adjustment of access rights	Yes					■
A.9.3	**User responsibilities**						
A.9.3.1	Use of secret authentication information	Yes				■	■
A.9.4	**System and application access control**						
A.9.4.1	Information access restriction	Yes				■	■
A.9.4.2	Secure log-on procedures	Yes				■	■
A.9.4.3	Password management system	Yes				■	■
A.9.4.4	Use of privileged utility programs	Yes				■	■
A.9.4.5	Access control to program source code	Yes			■	■	■
A.10	**Cryptography**						
A.10.1	**Cryptographic controls**						
A.10.1.1	Policy on the use of cryptographic controls	Yes					■
A.10.1.2	Key Management	Yes				■	
A.11	**Physical and environmental security**						
A.11.1	**Secure areas**						
A.11.1.1	Physical security perimeter	Yes					■
A.11.1.2	Physical entry controls	Yes					■
A.11.1.3	Securing offices, rooms and facilities	Yes					■
A.11.1.4	Protecting against external and environmental threats	Yes					■
A.11.1.5	Working in secure areas	Yes					■
A.11.1.6	Delivery and loading areas	No	IPS does not make use of a loading and unloading area.				
A.11.2	**Equipment**						
A.11.2.1	Equipment siting and protection	Yes				■	
A.11.2.2	Supporting utilities	Yes					■
A.11.2.3	Cabling security	Yes				■	
A.11.2.4	Equipment maintenance	Yes					■
A.11.2.5	Removal of assets	Yes					■
A.11.2.6	Security of equipment and assets off-premises	Yes					■
A.11.2.7	Secure disposal or re-use of equipment	Yes					■
A.11.2.8	Unattended user equipment	Yes				■	
A.11.2.9	'Clear desk'- en 'clear screen'-policy	Yes				■	■
A.12	**Operations security**						
A.12.1	**Operational procedures and responsibilities**						
A.12.1.1	Documented operating procedures	Yes				■	

Nr.	Control objectives and controls ISO 27001:2013	Applicable & Implemented Y/N	Substantation (when not applicable)	LR	CO	BR/BP	RRA
A.12.1.2	Change management	Yes				■	
A.12.1.3	Capacity management	Yes			■	■	
A.12.1.4	Separation of development, testing and operational environments	Yes					■
A.12.2	**Protection from malware**						
A.12.2.1	Controls against mal-ware	Yes				■	■
A.12.3	**Back-up**						
A.12.3.1	Information backup	Yes				■	■
A.12.4	**Logging and monitoring**						
A.12.4.1	Event logging	Yes				■	■
A.12.4.2	Protection of log information	Yes				■	
A.12.4.3	Administrator and operator logs	Yes				■	
A.12.4.4	Clock synchronisation	Yes				■	
A.12.5	**Control of operational software**						
A.12.5.1	Installation of software on operational systems	Yes				■	
A.12.6	**Technical vulnerability management**						
A.12.6.1	Management of technical vulnerabilities	Yes				■	
A.12.6.2	Restrictions on software installation	Yes				■	■
A.12.7	**Information systems audit considerations**						
A.12.7.1	Information systems audit controls	Yes				■	
A.13	**Communications security**						
A.13.1	**Network controls**						
A.13.1.1	Beheersmaatregelen voor netwerken	Yes					■
A.13.1.2	Security of network services	Yes					■
A.13.1.3	Segregation in networks	Yes				■	■
A.13.2	**Information transfer**						
A.13.2.1	Information transfer policies and procedures	Yes					■
A.13.2.2	Agreements on information transfer	Yes			■		■
A.13.2.3	Electronic messaging	Yes				■	■
A.13.2.4	Confidentiality or non disclosure agreements	Yes			■		■
A.14	**System acquisition, development and maintenance**						
A.14.1	**Security requirements of information systems**						
A.14.1.1	Information security requirements analysis and specification	Yes				■	■
A.14.1.2	Securing application services on public networks	Yes					■
A.14.1.3	Protecting applications services transactions	No	No transactions are taking place in the systems of IPS.				
A.14.2	**Security in development and support processes**						
A.14.2.1	Secure development policy	Yes			■	■	
A.14.2.2	System change control	Yes				■	
A.14.2.3	Technical review of applications after operating platform changes	Yes				■	
A.14.2.4	Restrictions on changes to software packages	Yes				■	
A.14.2.5	Secure system engineering principles	Yes			■	■	
A.14.2.6	Secure development environment	Yes			■	■	
A.14.2.7	Outsourced development	Yes			■	■	
A.14.2.8	System security testing	Yes				■	
A.14.2.9	System acceptance testing	Yes				■	
A.14.3	**Test data**						
A.14.3.1	Protection of test data	Yes			■	■	
A.15	**Supplier relationships**						
A.15.1	**Information security in supplier relationships**						
A.15.1.1	Information security policy for supplier relationships	Yes					■
A.15.1.2	Addressing security within supplier agreements	Yes			■		■
A.15.1.3	Information and communication technology supply chain	Yes					■
A.15.2	**Supplier service delivery management**						
A.15.2.1	Monitoring and review of supplier services	Yes				■	■
A.15.2.2	Managing changes to supplier services	Yes				■	■
A.16	**Information security incident management**						
A.16.1	**Management of information security incidents and improvements**						
A.16.1.1	Responsibilities and procedures	Yes				■	
A.16.1.2	Reporting information security events	Yes				■	
A.16.1.3	Reporting information security weaknesses	Yes				■	
A.16.1.4	Assessment of and decision on information security events	Yes				■	
A.16.1.5	Response to information security incidents	Yes				■	
A.16.1.6	Learning from information security incidents	Yes				■	
A.16.1.7	Collection of evidence	Yes				■	
A.17	**Information security aspects of business continuity management**						
A.17.1	**Information security continuity**						
A.17.1.1	Planning information security continuity	Yes				■	■
A.17.1.2	Implementing information security continuity	Yes				■	■
A.17.1.3	Verify, review and evaluate information security continuity	Yes				■	■
A.17.2	**Redundancies**						
A.17.2.1	Availability of information processing facilities	Yes					■
A.18	**Compliance**						
A.18.1	**Compliance with legal and contractual requirements**						
A.18.1.1	Identification of applicable legislation and contractual requirements	Yes		■	■		■
A.18.1.2	Intellectual property rights	Yes		■	■		■
A.18.1.3	Protection of records	Yes		■		■	■
A.18.1.4	Privacy and protection of personally identifiable information	Yes		■	■		■
A.18.1.5	Regulation of cryptographic controls	Yes		■			■
A.18.2	**Information security reviews**						
A.18.2.1	Independent review of informtation security	Yes				■	
A.18.2.2	Compliance with security policies and standards	Yes				■	
A.18.2.3	Technical compliance review	Yes				■	