Statement of Applicability

Section		Roamler International
5	**Information security policies**	**Applicable YES / NO**
5.1	Management direction for information security	
5.1.1	Policies for information security	YES
5.1.2	Review of the policies for information security	YES
6	**Organization of information security**	
6.1	Internal organization	
6.1.1	Information security roles and responsibilities	YES
6.1.2	Segregation of duties	YES
6.1.3	Contact with authorities	YES
6.1.4	Contact with special interest groups	YES
6.1.5	Information security in project management	YES
6.2	Mobile devices and teleworking	
6.2.1	Mobile device policy	YES
6.2.2	Teleworking	YES
7	**Human resource security**	
7.1	Prior to employment	
7.1.1	Screening	YES
7.1.2	Terms and conditions of employment	YES
7.2	During employment	
7.2.1	Management responsibilities	YES
7.2.2	Information security awareness, education and training	YES
7.2.3	Disciplinary process	YES
7.3	Termination and change of employment	
7.3.1	Termination or change of employment responsibilities	YES
8	**Asset management**	
8.1	Responsibility for assets	
8.1.1	Inventory of assets	YES
8.1.2	Ownership of assets	YES
8.1.3	Acceptable use of assets	YES
8.1.4	Return of assets	YES
8.2	Information classification	
8.2.1	Classification of information	YES
8.2.2	Labelling of information	NO
8.2.3	Handling of assets	YES
8.3	Media handling	
8.3.1	Management of removable media	YES
8.3.2	Disposal of media	YES
8.3.3	Physical media transfer	YES
9	**Access control**	
9.1	Business requirements of access control	
9.1.1	Access control policy	YES
9.1.2	Access to networks and network services	YES
9.2	User access management	
9.2.1	User registration and de-registration	YES
9.2.2	User access provisioning	YES
9.2.3	Management of privileged access rights	YES
9.2.4	Management of secret authentication information of users	YES
9.2.5	Review of user access rights	YES
9.2.6	Removal or adjustment of access rights	YES
9.3	User responsibilities	
9.3.1	Use of secret authentication information	YES
A.9.4	System and application access control	
9.4.1	Information access restriction	YES
9.4.2	Secure log-on procedures	YES
9.4.3	Password management system	YES
9.4.4	Use of privileged utility programs	YES
9.4.5	Access control to program source code	YES
10	**Cryptography**	
10.1	Cryptographic controls	
10.1.1	Policy on the use of cryptographic controls	YES
10.1.2	Key management	YES
11	**Physical and environmental security**	
11.1	Secure areas	
11.1.1	Physical security perimeter	YES
11.1.2	Physical entry controls	YES
11.1.3	Securing offices, rooms and facilities	YES
11.1.4	Protecting against external and environmental threats	YES
11.1.5	Working in secure areas	YES
11.1.6	Delivery and loading areas	NO
11.2	Equipment	
11.2.1	Equipment siting and protection	YES
11.2.2	Supporting utilities	YES

11.2.3	Cabling security	YES
11.2.4	Equipment maintenance	YES
11.2.5	Removal of assets	YES
11.2.6	Security of equipment and assets off-premises	YES
11.2.7	Secure disposal or reuse of equipment	YES
11.2.8	Unattended user equipment	YES
11.2.9	Clear desk and clear screen policy	YES
12	**Operations security**	
12.1	Operational procedures and responsibilities	
12.1.1	Documented operating procedures	YES
12.1.2	Change management	YES
12.1.3	Capacity management	YES
12.1.4	Separation of development, testing and operational environments	YES
12.2	Protection from malware	
12.2.1	Controls against malware	YES
12.3	Backup	
12.3.1	Information backup	YES
12.3	Logging and monitoring	
12.4.1	Event logging	YES
12.4.2	Protection of log information	YES
12.4.3	Administrator and operator logs	YES
12.4.4	Clock synchronisation	YES
12.5	Control of operational software	
12.5.1	Installation of software on operational systems	YES
12.6	Technical vulnerability management	
12.6.1	Management of technical vulnerabilities	YES
12.6.2	Restrictions on software installation	YES
12.7	Information systems audit considerations	
12.7.1	Information systems audit controls	YES
13	**Communications security**	
13.1	Network security management	
13.1.1	Network controls	YES
13.1.2	Security of network services	YES
13.1.3	Segregation in networks	YES
13.2	Information transfer	
13.2.1	Information transfer policies and procedures	YES
13.2.2	Agreements on information transfer	YES
13.2.3	Electronic messaging	YES
13.2.4	Confidentiality or nondisclosure agreements	YES
14	**System acquisition, development & maintenance**	
14.1	Security requirements of information systems	
14.1.1	Information security requirements analysis and specification	YES
14.1.2	Securing application services on public networks	YES
14.1.3	Protecting application services transactions	YES
14.2	Security in development and support processes	
14.2.1	Secure development policy	YES
14.2.2	System change control procedures	YES
14.2.3	Technical review of applications after operating platform changes	YES
14.2.4	Restrictions on changes to software packages	YES
14.2.5	Secure system engineering principles	YES
14.2.6	Secure Development Environment	YES
14.2.7	Outsourced development	YES
14.2.8	System security testing	YES
14.2.9	System acceptance testing	YES
14.3	Test data	
14.3.1	Protection of test data	YES
15	**Supplier relationships**	
15.1	Information security in supplier relationships	
15.1.1	Information security policy for supplier relationships	YES
15.1.2	Addressing security within supplier agreements	YES
15.1.3	ICT supply chain	YES
15.2	**Supplier service delivery management**	
15.2.1	Monitoring and review of supplier services	YES
15.2.2	Managing changes to supplier services	YES
16	**Information security incident management**	
16.1	Management of information security incidents & improvements	
16.1.1	Responsibilities and procedures	YES
16.1.2	Reporting information security events	YES
16.1.3	Reporting information security weaknesses	YES
16.1.4	Assessment of and decision on information security events	YES
16.1.5	Response to information security incidents	YES
16.1.6	Learning from information security incidents	YES
16.1.7	Collection of evidence	YES
17	**Information security aspects of BCM**	
17.1	Information security continuity	
17.1.1	Planning information security continuity	YES
17.1.2	Implementing information security continuity	YES
17.1.3	Verify, review and evaluate information security continuity	YES
17.2	Redundancies	
17.2.1	Availability of information processing facilities	YES

18	Compliance	
18.1	**Compliance with legal and contractual requirements**	
18.1.1	Identification of applicable legislation and contractual requirements	YES
18.1.2	Intellectual property rights	YES
18.1.3	Protection of records	YES
18.1.4	Privacy and protection of personally identifiable information	YES
18.1.5	Regulation of cryptographic controls	YES
18.2	**Information security reviews**	
18.2.1	Independent review of information security	YES
18.2.2	Compliance with security policies and standards	YES
18.2.3	Technical compliance review	YES