BettyBlocks ISMS Tracker - Statement of Applicability

Scope		**The technical development and delivery of the Betty Blocks application platform.**				
Implemented	**Chapter**	**Description**	**Applicable**	**Not applicable**	**Reason for selection**	**Motivation**
---	**5.1**	**Management direction for information security**	---	---	---	
x	5.1.1	Policies for information	x		BR	
x	5.1.2	Review of the policies for information security	x		BR	
---	**6.1**	**Internal organisation**	---	---	-	
x	6.1.1	Information security roles and responsibilities	x		BR	
x	6.1.2	Segregation of duties	x		BR	
x	6.1.3	Contact with authorities	x		LR	
x	6.1.4	Contact with special interest groups	x		CR	
x	6.1.5	Information security in project management	x		RA	
---	**6.2**	**Mobile devices and teleworking**	---	---	---	
x	6.2.1	Mobile device policy	x		BR	
x	6.2.2	Teleworking	x		BR	
---	**7.1**	**Prior to employment**	---	---	---	
x	7.1.1	Screening	x		BR	
x	7.1.2	Terms and conditions of employment	x		BR	
---	**7.2**	**During employment**	---	---	---	
x	7.2.1	Management responsibilities	x		BR	
x	7.2.2	Information security awareness, education and training	x		BR	
x	7.2.3	Disciplinary process	x		RA/BR	
---	**7.3**	**Termination and change of employment**	---	---	---	
x	7.3.1	Termination or change of employment responsibilities	x		BR	
---	**8.1**	**Responsibility for assets**	---	---	---	
x	8.1.1	Inventory of assets	x		BR	
xx	8.1.2	Ownership of assets	x		BR	
x	8.1.3	Acceptable use of assets	x		BR	
x	8.1.4	Return of assets	x		BR	
---	**8.2**	**Information classification**	---	---	---	
x	8.2.1	Classification of information	x		CR/BR	
x	8.2.2	Labeling of information	x		CR	
x	8.2.3	Handling of assets	x		BR	
---	**8.3**	**Media handling**	---	---	---	
x	8.3.1	Management of removable media	x		BR	
x	8.3.2	Disposal of media	x		BR	
x	8.3.3	Physical media transfer	x		BR	
---	**9.1**	**Business requirements of access control**	---	---	---	
x	9.1.1	Access control policy	x		BR/CR	
x	9.1.2	Access to networks and network services	x		BR	
---	**9.2**	**User access management**	---	---	---	
x	9.2.1	User registration and de-registration	x		BR	
x	9.2.2	User access provisioning	x		BR	
x	9.2.3	Management of privileged access rights	x		BR/CR	
x	9.2.4	Management of secret authentication information of users	x		BR	
x	9.2.5	Review of user access rights	x		BR/CR	
x	9.2.6	Removal or adjustment of access rights	x		BR/CR	
---	**9.3**	**User responsibilities**	---	---	---	
x	9.3.1	Use of secret authentication information	x		BR	
---	**9.4**	**System and application access control**	---	---	---	
x	9.4.1	Information access restriction	x		BR/CR	
x	9.4.2	Secure log-on procedures	x		BR	
x	9.4.3	Password management system	x		BR	
x	9.4.4	Use of privileged utility programs	x		BR	
x	9.4.5	Access control to program source code	x		BR	
---	**10.1**	**Cryptographic controls**	---	---	---	
x	10.1.1	Policy on the use of cryptographic controls	x		BR	
x	10.1.2	Key management	x		BR	
---	**11.1**	**Secure areas**	---	---	---	
x	11.1.1	Physical security perimeter	x		BR	
x	11.1.2	Physical entry controls	x		BR	
x	11.1.3	Securing office, room and facilities	x		BR	
x	11.1.4	Protecting against external end environmental threats	x		BR	No safeguards made since not applicable or inpreventable; backups arranged offsite so handled in other controls.
---	11.1.5	Working in secure areas		x		There are no areas designated as a secure area; no work is performed that requires a seperate secure area.
x	11.1.6	Delivery and loading areas	x		BR	There are no delivery and loading areas.
---	**11.2**	**Equipment**	---	---	---	
x	11.2.1	Equipment siting and protection	x		RA	Risk fully accepted
x	11.2.2	Supporting utilities	x		RA	Risk fully accepted
x	11.2.3	Cabling security	x		RA	Risks fully accepted, no network cabling
x	11.2.4	Equipment maintenance	x		BR	
x	11.2.5	Removal of assets	x		BR	
x	11.2.6	Security of equipment and assets off-premises	x		BR	
x	11.2.7	Secure disposal or re-use of equipment	x		BR	
x	11.2.8	Unattended user equipment	x		BR	
x	11.2.9	Clear desk and clear screen policy	x		BR	In employee handbook
---	**12.1**	**Operational procedures and responsibilities**	---	---	---	
x	12.1.1	Documented operating procedures	x		BR	In employee handbook
x	12.1.2	Change management	x		CR	
x	12.1.3	Capacity management	x		CR	
x	12.1.4	Separation of development, testing and operational environments	x		BR	
---	**12.2**	**Protection from malware**	---	---	---	
x	12.2.1	Controls against malware	x		BR	
	12.3	**Backup**	---	---	---	
x	12.3.1	Information backup	x		CR	
---	**12.4**	**Logging and monitoring**	---	---	---	
x	12.4.1	Event logging	x		BR	
x	12.4.2	Protection of log information	x		BR	
x	12.4.3	Administrator and operator logs	x		BR	
x	12.4.4	Clock synchronisaton	x		BR	
---	**12.5**	**Control of operational software**	---	---	---	
x	12.5.1	Installation of software on operational systems	x		BR	
---	**12.6**	**Technical vulnerability management**	---	---	---	
x	12.6.1	Management of technical vulnerabilities	x		BR	
x	12.6.2	Restrictions on software installation	x		BR	
---	**12.7**	**Information systems audit considerations**	---	---	---	
x	12.7.1	Information systems audit controls	x		CR	
---	**13.1**	**Network security management**	---	---	---	
x	13.1.1	Network controls	x		BR	
x	13.1.2	Security of network services	x		BR	
x	13.1.3	Segregation in networks	x		BR	
---	**13.2**	**Information transfer**	---	---	---	
X	13.2.1	Information transfer policies and procedures	x		BR	
X	13.2.2	Agreements on information transfer	x		BR	
X	13.2.3	Electronic messaging	x		BR	
X	13.2.4	Confidentiality or non-disclosure agreements	x		BR	
---	**14.1**	**Security requirements of information systems**	---	---	---	
X	14.1.1	Information security requirements analysis and specification	x		BR	
X	14.1.2	Securing applications services on public networks	x		BR	
X	14.1.3	Protecting application services transactions	x		BR	
---	**14.2**	**Security in development and support processes**	---	---	---	
X	14.2.1	Secure development policy	x		BR	

Reason for selection is to be chosen from	
LR	Legal Requirement
CR	Contractual Requirement
BR	Business Requirement
RA	Risk Assessment

X	14.2.2	System change control procedures	x		BR					
X	14.2.3	Technical review of applications after operating platform changes	x		BR					
X	14.2.4	Restrictions on changes to software packages	x		BR					
X	14.2.5	Secure system engineering principles	x		BR					
X	14.2.6	Secure development environment	x		BR					
X	14.2.7	Outsourced development	x		BR					
X	14.2.8	System security testing	x		BR					
X	14.2.9	System acceptance testing	x		BR					
---	**14.3**	**Test data**	**---**	**---**	**---**					
X	14.3.1	Protection of test data	x		CR					
---	**15.1**	**Information security in supplier relationships**	**---**	**---**	**---**					
x	15.1.1	Information security policy for supplier relationships	x		BR					
x	15.1.2	Addressing security within supplier agreements	x		BR					
x	15.1.3	Information and communication technology supply chain	x		BR					
---	**15.2**	**Supplier service delivery management**	**---**	**---**	**---**					
x	15.2.1	Monitoring and review of supplier services	x		BR					
x	15.2.2	Managing changes to supplier services	x		BR					
---	**16.1**	**Management of information security incidents and improvements**	**---**	**---**	**---**					
x	16.1.1	Responsibilities and procedures	x		BR					
x	16.1.2	Reporting information security events	x		BR					
x	16.1.3	Reporting information security weaknesses	x		BR					
x	16.1.4	Assessment of and decision on information security events	x		BR					
x	16.1.5	Response to information security incidents	x		BR					
x	16.1.6	Learning from information security incidents	x		BR					
x	16.1.7	Collection of evidence	x		BR					
---	**17.1**	**Information security continuity**	**---**	**---**	**---**					
x	17.1.1	Planning information security continuity	x		BR					
x	17.1.2	Implementing information security continuity	x		BR					
x	17.1.3	Verify, review and evaluate information security continuity	x		BR					
---	**17.2**	**Redundancies**	**---**	**---**	**---**					
x	17.2.1	Availability of information processing facilities	x		BR					
---	**18.1**	**Compliance with legal and contractual requirements**	**---**	**---**	**---**					
x	18.1.1	Identification of applicable legislation and contractual requirements	x		BR					
x	18.1.2	Intellectual property rights	x		BR					
x	18.1.3	Protection of records	x		BR					
x	18.1.4	Privacy and protection of personally identifiable information	x		BR					
x	18.1.5	Regulation of cryptographic controls	x		BR					
---	**18.2**	**Information security reviews**	**---**	**---**	**---**					
x	18.2.1	Independent review of information security	x		BR					
x	18.2.2	Compliance with security policies and standards	x		BR					
x	18.2.3	Technical compliance review	x		BR					