ISO 27001 COMPLIANCE CHECKLIST TEMPLATE

ISO 27001 STANDARD	ISO 27001 SUB-SECTION	RELEVANT?	IN COMPLIANCE?	REMARKS
A. 5. IS Policies				
5.1. Management direction for information security				
5.1.1	Policies for IS			
A. 6. Organization of information security				
6.1. Internal organization				
6.1.1	IS roles / responsibilities			
6.1.2	Segregation of duties			
6.2. Mobile devices and teleworking				
6.2.1	Mobile devices policy			
6.2.2	Teleworking			
A. 7. Human resources security				
7.1. Prior to employment				

7.1.1	Screening			
7.1.2	Terms and conditions of employment			
7.2. During employment				
7.2.1	Management responsibilities			
7.2.2	IS awareness, education, and training			
A. 8. Asset management				
8.1. Responsibilities for assets				
8.1.1	Inventory of assets			
8.1.2	Ownership of assets			
8.1.3	Acceptable use of assets			
8.1.4	Return of assets			
8.2. Information classification				
8.2.1	Classification of information			
8.2.2	Labeling of information			
A. 9. Access control				
9.1. Responsibilities for assets				
9.1.1	Access control policy			
9.1.2	Access to networks and network services			
9.2. Responsibilities for assets				

9.2.1	User registration and de-registration			
9.2.3	Management of privileged access rights			
9.2.4	Management of secret authentication information of users			
9.2.5	Review of user access rights			
9.2.6	Removal or adjustment of access rights			
9.3. User responsibilities				
9.3.1	Use of secret authentication information			
9.4. System and application access control				
9.4.1	Information access restrictions			
9.4.2	Secure log-in procedures			
9.4.3	Password management system			
A. 10. Cryptography				
10.1. Cryptographic controls				
10.1.1	Policy on the use of cryptographic controls			
10.1.2	Key management			
A. 11. Physical and environmental security				
11.1. Secure areas				
11.1.1	Physical security perimeter			

11.1.2	Physical entry controls			
11.1.3	Securing offices, rooms, and facilities			
11.1.4	Protection against external and environmental threats			
11.1.5	Working in secure areas			
11.1.6	Delivery and loading areas			
11.2. Equipment				
11.2.1	Equipment siting and protection			
11.2.2	Support utilities			
11.2.3	Cabling security			
11.2.4	Equipment maintenance			
11.2.5	Removal of assets			
A. 12. Operations security				
12.1 Operational procedures and responsibilities				
12.1.1	Documented operating procedures			
12.1.2	Change management			
12.1.3	Capacity management			
12.1.4	Separation of development, testing, and operational environments			

12.2. Protection from malware				
12.2.1	Controls against malware			
12.3. Backup				
12.3.1	Information backup			
12.4. Logging and monitoring				
12.4.1	Event logging			
12.4.2	Protection of log information			
12.4.3	Administrator and operator log			
12.5. Control of operational software				
12.5.1	Installation of software on operational systems			
12.6. Technical vulnerability management				
12.6.1	Management of technical vulnerabilities			
A. 13. Communication security				
13.1. Network security management				
13.1.1	Network controls			
13.1.2	Security of network services			
13.1.3	Segregation in networks			
13.2. Information transfer				
13.2.1	Information transfer policies and procedures			
13.2.2	Agreements on information transfer			

A. 14. System acquisition, development, and maintenance				
14.1. Security requirements of information systems				
14.1.1	IS requirements analysis and specification			
14.1.2	Securing application services on public networks			
14.1.3	Protecting application service transactions			
A. 15. Supplier relationships				
A. 16. IS incident management				
16.1.1	IS management			
A. 17. IS aspects of business continuity management				
17.1.1	IS continuity			
17.2.1	Redundancies			
A. 18. Compliance				
18.1. Compliance with legal and contractual requirements				
18.1.1	Identification of applicable legislation and contractual requirements			
18.1.2	Intellectual property rights			
18.1.3	Protection of records			
18.1.4	Privacy and protection of personally identifiable information			
18.1.5	Regulation of cryptographic controls			
18.2. Independent review of information security				

18.2.1	Independent review of information security			

Checked by _____

Date _____

DISCLAIMER

Any articles, templates, or information provided by CyberShield Tanzania inc. on the website are for reference only. While we strive to keep the information up to date, relevance and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, articles, templates, or related graphics contained on the website. Any reliance you place on such information is therefore strictly at your own risk and we shall not guarantee claim.

This template is provided as a sample only. This template is in no way meant as legal or compliance advice. Users of the template must determine what information is necessary and needed to accomplish their objectives.
Your advice to visit the institutional website to understand how to use the checklist, in regard to brief information that we provide here.