Information Security Questionnaire

Fill in Table 1 by providing general information regarding your Company, IT infrastructure and Information Security systems.

Table 1 – General Information

1	Company Name	
2	Company Executive (position, full name)	
3	Contacts (phones, e-mail, etc.).	
4	Type of Legal entity e.g. (Pvt.) Ltd., Limited, Government, etc.	
5	Main business of the Company	
6	Legal and Mailing addresses of the Company	
7	Number of headquarters, branch offices, additional offices, etc. (including offices abroad)	
8	Total number of staff members	
9	Total number of staff members in departments responsible for Company's IT Infrastructure	
10	Total number of staff members in departments responsible for Company's information security	
11	Total number of servers	
12	Total number of users' workstations	
13	Date of the Company business beginning	
14	Does Company's Quality Management System conform to ISO 9000 requirements? (specify the Certificate issue date)	
15	Does the Company comply to other Cross-industry Standards (SOX, Basel II, etc.) and Information Security Standards (ISO 27001:2013, NIST, PCI DSS)	
16	Please describe organizational structure of your Company and organizational structure of Information Security (IS) departments (provide graphical schemes if possible)	

Fill in Table 2 by specifying name and description of the services provided by the Company to Customers and Partners.

Table 2 – Services Provided by the Company

N	Service Name	Short Description of Service
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		

List all existing corporate documents related to Information Security, in Table 3.

Table 3 – Information Security Documentation

N	Document Name	Document Destination
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		

In Table 4, list business critical Information Systems to be considered in the information security scope (e.g. ATM Authentication, Customer Evaluation, etc.)

Table 4 – Critical Information Systems

N	Information System Name	Short Description of Information System Functions
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		

In Table 5, Please specify equipment used by the systems (DBMS servers, file servers, network devices, workstations, etc.), and the total number of devices of each type.

Table 5 – Information Systems in the Company

N	Information System Name	Location of system components (addresses of sites)	Types of Equipment Used in the Information System, the Number of Devices of Each Type
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			

In Table 6, describe Information Security Tools used in the Company by specifying their title, manufacturer and version.

Table 6 - Information Security Practices/Tools

N	Information Security Practices/Tool	Description
1.	Firewalls	
2.	VPN tools	
3.	Authentication tools	
4.	Antivirus software	
5.	Intrusion Detection System/Intrusion Prevention System	
6.	Cryptographic tools	
7.	Integrity control tools	
8.	Access control tools	
9.	Content analysis tools	
10.	Information security scanners	
11.	Physical Protection	
12.	Document Control System	
13.	Access Control e.g. CCTV	
14.	Filing System	
15.	Fire Protection	
16.	Fire Extinguishing Protection e.g. Sprinkler System	
17.	Physical Intrusion Detection Systems	
18.	Others	

Please, answer the questions provided in Table 7.

Table 7 - Questions

1.	Do you have documented Information Security Policy?	☐ Yes ☐ No
2.	Do you deliver Information Security Policy to all personnel? Which way?	
3.	In what cases do you reconsider Information Security Policy?	
4.	How Top Management demonstrate its concern in Information Security issues? Does Top Management analyze results of Information Security System's performance?	
5.	How do employees in different departments coordinate their activity on Information Security (are there dedicated employees in charge of Information Security)?	
6.	Have you defined security roles and responsibilities of employees?	☐ Yes ☐ No
7.	Do you conduct Information Security Risk Analysis within the organization: threat analysis, vulnerabilities analysis, definition of acceptable risk level, etc?	☐ Yes ☐ No
8.	Have you formalized the procedure of information security risk analysis?	☐ Yes ☐ No
9.	Do you arrange external audits? What is their periodicity? How do you determine the necessity of an external audit?	
10.	Do you arrange internal audit of compliance with requirements of Company's organizational documents?	
11.	Is the access to information systems auditing tools restricted? If yes, how?	
12.	Have you formalized the procedures of document management (creating, storing, versioning, etc)?	

13.	Have you formalized the procedures of event record management available (event logs, conference results, etc)?	
14.	How does Top Management approve purchasing of new information processing facilities and systems?	
15.	Which organizations, communities, governmental institutions do you contact with on Information Security issues?	
16.	How do you cooperate with third-party organizations in the framework of Information Security? What are the requirements to third-party organizations?	
17.	Do you perform inventory of Company's assets? If yes, how frequently and in what extent?	
18.	Do you use "Information Owner" or "Resource Owner" concept, or any similar term to identify an employee or division being administratively responsible for information assets development, utilization, maintenance, for their efficiency and security?	☐ Yes ☐ No
19.	What are the rules of information assets usage established in your Company?	
20.	Have you documented the list of confidential information?	☐ Yes ☐ No
21.	What are the established procedures in your Company, for marking and treatment of information with respect to its classification?	
22.	Do you sign confidentiality agreements with personnel?	☐ Yes ☐ No
23.	What are the Information Security documents which a new staff is made familiar with, by employment?	
24.	How do you verify personal information of employees during the employment?	
25.	How do you examine academic and professional qualifications of staff during the employment?	

26.	How do you manage information security awareness, training and education?	
27.	How do you notify the staff about information security policies and procedure change?	
28.	What disciplinary process is set for employees who have committed security breach?	
29.	Who is responsible for employment and termination procedures?	
30.	How do you manage information security during employment, termination and change of employment? Are employee's assets returned and rights abolished before the employee is dismissed or the labor contract is terminated, etc?	
31.	How do you provide a physical protection of perimeter, room access control?	
32.	How do you provide protection of equipment against unauthorized access?	
33.	Do all employees, contractors and third party users return all of the organization's assets in their possession upon termination of their employment, contract or agreement?	☐ Yes ☐ No
34.	What controls do you use to protect company facilities from external threats (fire, flood, etc)?	
35.	How do you control public access, delivery and loading areas?	
36.	How do you consider information security requirements with respect to equipment allocation?	
37.	How do you protect equipment from power failures?	
38.	How do you manage equipment maintenance by internal departments and by external organizations (for example warranty repairs)?	
39.	How do you secure equipment outside organization premises (for example notebooks, PDA, flash disks, hardware on sale points, etc)?	

40.	How do you manage secure disposal or re-use of equipment? Do you ensure that any sensitive data or licensed software has been removed or securely overwritten prior to disposal?	
41.	Could equipment be taken off-site without prior authorization?	
42.	What operating procedures such as Back-Up, Equipment Maintenance etc. are documented and maintained? Are they available for all users who need them?	
43.	How do you manage changes to information processing facilities and systems?	
44.	How do you monitor capacity demands and future capacity requirements to ensure that adequate processing power and storage are available? (Example: monitoring hard disk space, RAM, CPU on critical servers, etc.)	
45.	Which measures do you use for protection against malicious software code and mobile code?	
46.	How do you make back-up of information? Which information is to be backed-up?	
47.	By what means do you control and protect networks and network services in your Company?	
48.	In what extent the policies and procedures for information exchange protection, both internal and external, are developed and being implemented?	
49.	What are the requirements to the level of network services availability within the Company?	
50.	How do you manage development, testing and acceptance of new information systems?	
51.	How do you protect removable media in the processes of usage, storage, disposal and transporting?	
52.	How do you protect system documentation	

	against unauthorized access?	
53.	What controls do you use to protect information involved in electronic commerce (protection from fraudulent activity, contract dispute, unauthorized disclosure and modification)?	
54.	How do you protect the integrity of information being made available in publicly available systems?	
55.	What procedures are set up for monitoring the use of information processing facility?	
56.	How do you analyze the results of the monitoring activities?	
57.	How do you manage clock synchronization for computers and communication devices?	
58.	How do you manage logging of faults reported by users or by system programs related to problems with information processing or communication systems?	
59.	Which procedures do you have for user's registration in a system?	
60.	How do you offer access privileges to users, recall or change them?	
61.	How do you manage to control users using their rights?	
62.	In what cases you regularly reconsider the privileges?	
63.	How do you manage password control process (password policy, automated systems)?	
64.	How do you protect user's equipment left unattended?	
65.	Does clean-table policy established in your Company?	☐ Yes ☐ No
66.	Do you have a documented access control policy in your Company?	☐ Yes ☐ No
67.	How do you grant and monitor users' access to network resources (Web, E-mail, etc.)?	

68.	Which way is equipment identified (eg. MAC-address identification)? How are groups of network services distributed (eg. with VLAN technology) in your Company?	
69.	How is the access of external (remote) users to internal networks regulated, organized and controlled?	
70.	How is routing organized in Company's networks?	
71.	What measures are used to secure the access to information systems (enter procedures, identification and authentication, ID management system, session time blocking, limitation of connect time, etc)?	
72.	How is remote personnel work organized?	
73.	Do you have a documented policy of using cryptographic tools for information security?	■ Yes ☐ No
74.	How is key management organized to maintain using of cryptographic methods?	
75.	What are the procedures of software installation monitoring?	
76.	How does your Company monitor and check the process of software development being implemented by third-party companies?	
77.	Do you receive timely updates about technical vulnerabilities of information systems in use, and how is their timeliness provided?	
78.	How is Company's exposure to these vulnerabilities assessed, and which way do you take adequate measures to eliminate risks connected with them?	
79.	How do you monitor and assess the types, volumes and costs of information security incidents?	
80.	How do you collect, keep and deliver witnesses to law enforcement authorities?	
81.	How do you determine and track changes in legislation, regulating and contractual requirements? How is the compliance with	

	these requirements guaranteed?	
82.	How is the compliance of cryptographic controls correlated with all relevant agreements, legislation and regulations?	
83.	Have you elaborated a process of business continuity provision? How is it supported? How does it recognize information security requirements necessary for business continuity?	
84.	Have you elaborated plans of disaster recovery after failures?	☐ Yes ☐ No
85.	Do you have a time-table for regular testing disaster recovery plans?	☐ Yes ☐ No
86.	What is a procedure of reconsidering recovery plans?	
87.	What is a procedure of response to incidents, and how is this procedure documented?	
88.	Have you fixed responsibilities of the management and employees for incident responding?	☐ Yes ☐ No
89.	Is your personnel, as well as contractors and third-party users of information systems and services, obliged to notice and alarm about all weaknesses, observed or eventual, in protection of systems or services? Which way is this provided?	

Email please filled form to us with a scanned/signed NDA: support@thekernel.com

Contact us:

Middle East & Africa

Tel. +971 4 7017 260/1
Fax +971 4 7017 262

Dubai Airport Free Zone 6EA, #209
P.O. Box 54808, Dubai – United Arab Emirates
Email: info@thekernel.com
Web: https://www.thekernel.com

Russian Federation & CIS countries

Tel. +7 (495) 2318224

Smolenskaya Ploshad, dom 3, #49
121099, Moscow, Russian Federation
Email: info@thekernel.ru
Web: https://www.thekernel.ru