Appendix A

Questionnaire Form

جامعة السودان للعلوم و التكنلوجيا - كلية الدراسات العليا - ماجستير تقنية المعلومات

استمارة استبيان (----------)

التاريخ / / 2108 الرقم : .....

إيماناً منا على دور البحث العلمي في التقدم ،أضع بين أيديكم هذه الإستبانة وهي إحدى المتطلبات الدراسية للحصول على درجة الماجستيرعلوم الحاسوب و تقنية المعلومات تخصص شبكات ، بعنوان فعالية سرية امن المعلومات في القطاعات العامة و الهدف من البحث لتقييم فعالية سياسات أمن المعلومات, وتحسين وتطوير قي القطاعات العامة . وحيث أنني أؤمن بأنكم خيرمصدرللمعلومات المطلوبة ، وأعهدبكم الاهتمام والاستعداد لمؤازرة الأبحاث العلمية التي تهتم بخدمة مجتمعنا وتطويره،لذا توجهت إليكم وكلي أمل في أن أجد التعاون المطلق منقبلكم وذلك من خلال الإجابةعلى أسئلةهذه الإستبانة. أرجومن سيادتكم التكرم بقراءة كل فقرة بعناية و وضع إشارة X أمامالاختيارالمناسب للوصول إلى نتائج دقيقة وموضوعية علماً بأن الإجابة ستعامل بسرية وتستخدم لغرض البحث العلمي فقط ، شاكراً لكم حسن تعاونكم.

اسم الباحث / نور محمد عثمان الامين **ت:0911158929**

أولا:بيانـــات أساسية:

الاسم: (اختياري) .....

1. المؤسسة:	☐			
2. الجنس:	☐ ذكر		☐ أنثى	
3. الوظيفة	☐	☐	☐	☐اخري
4. المهنة	☐ مدير عام	☐ مدير IT	☐ مهندس	☐ تقني
5. سنوات الخبرة	☐ 5 سنوات فأقل	☐ من 6-10	☐ أكثر من 10 سنوات	
6. العمر	☐ أقل من 35	☐ 35-45	☐ أكثر من 45	

ثانيا: أسئلة الاستبيان :

م	العبارات	درجة التوافر				
		عالية جدا	عالية	إلى حد ما	منخفضة	منخفضة جدا
1	Does the organization have a written information security policy? هل لدى المنظمة سياسة أمن معلومات مكتوبة؟					
2	Is information security policy approved by the top management? هل يتم اعتماد سياسة أمن المعلومات من قبل الإدارة العليا؟					
3	Is the information security policy communicated to all employees? هل يتم إبلاغ سياسة أمن المعلومات لجميع الموظفين؟					
4	Does the organization have a dedicated information security team? هل لدى المنظمة فريق مخصص لأمن المعلومات؟					
5	Does the informationuseful to conduct an information security awareness program for employees? هل تستخدم المعلومات لإجراء برنامج التوعية بأمن المعلومات للموظفين؟					
6	Does the organization implemented information security solutions: Firewall at intent gateways, Anti-virus - anti-spam هل نفذت المنظمة حلول أمن المعلومات : The firewall at intent gateways, Anti-virus - anti-spam					
7	Does the organization have any procedure to update and batch computer OS and anti-virus? هل لدى المنظمة أي إجراء لتحديث نظام تشغيل الكمبيوتر ومكافحة الفيروسات؟					
8	Does the organization have any user access control policy? هل لدى المنظمة أي سياسة تحكم في وصول المستخدم؟					
9	Does the organization have a password policy? هل لدى المنظمة سياسة كلمة مرور؟					
10	Does the organization have any user's access review policy? هل لدى المنظمة سياسة مراجعة الوصول لأي مستخدم؟					

					How frequently per year the access review is conducted? كم مرة يتم إجراء مراجعة الوصول() access reviewفي كل عام؟	11
					Is the top management supporting and enforcing information security policy implementation? هل الإدارة العليا تدعم تنفيذ سياسة أمن المعلومات وتنفذها؟	12
					Does the organization following any information security standards or guideline? هل تتبع المنظمة أي معايير أو مبادئ توجيهية لأمن المعلومات؟	13
					Does the organization have cybersecurity incident response plan? هل لدى المنظمة خطة استجابة للحوادث الأمنية على الإنترنت؟	14
					Does the organizationimplement any business continuity program? هل تقوم المنظمة بتنفيذ أي برنامج لاستمرارية العمل؟	15
					Does the organization have documented disaster recovery plan? هل لدى المنظمة خطة موثقة لاستعادة القدرة على العمل بعد الكوارث؟	16
					How frequently is the disaster recovery plan tested? كم مرة يتم اختبار خطة التعافي disaster recovery() من الكوارث؟	17
					Does the organization have any information systems audit program? هل لدى المنظمة برنامج تدقيق لأنظمة المعلومات؟	18
					How frequently is information systems audit conducted? كم مرة بتكرر إجراء تدقيق نظم المعلومات؟	19
					Does the information system audit is part of internal audit responsibility? هل يعتبر تدقيق نظام المعلومات جزءًا من مسؤولية قسم التدقيق الداخلي؟	20
					Can you describe in detail the methods and techniques are used for measuring the effectiveness of information security policies in a sense as to mitigate the threats, vulnerabilities or risk associated withorganizational assets? هل يمكن أن تصف بالتفصيل الطرق والتقنيات المستخدمة لقياس فعالية سياسات أمن المعلومات بمعنى الحد من التهديدات أو نقاط الضعف أو المخاطر المرتبطة بالأصول التنظيمية؟	21
					Do you have a policy monitoring system to monitor and assess your institution network security policies? هل لديك نظام رصد ومراقبة السياساتالامنية وتقيمها لشبكة مؤسستك؟	22

يرجى ذكر أي ملاحظة تريد إضافتها والتي قد أغفلتهاالإستبانة أولم يعطيهاالباحث حقها من وجهـــة نظـــــــــــرك

Appendix B

Interview Questions

اسئلة المقابلة

1- What are the regulations regarding information security that needs to be followed by your organization? To what extent is your company following these regulations?

ما هي اللوائح المتعلقة بأمن المعلومات التي يجب أن تتبعها منظمتك؟إلى أي مدى تتبع شركتك هذه اللوائح؟

2- How many information security professionals are specifically involved in information security tasks? How many of them have professional certifications?

كم عدد محترفي أمن المعلومات الذين يشاركون بشكل محدد في مهام أمن المعلومات؟كم منهم لديهم شهادات مهنية؟

3- Approximately what percentage of your total budget is being allotted to information security measures? Is this percentage serving organization's information security needs well enough?

ما هي النسبة المئوية تقريبا من إجمالي ميزانيتك التي يتم تخصيصها لتدابير أمن المعلومات؟هل هذه النسبة التي تخدم احتياجات أمن المعلومات للمنظمة كافية بما فيه الكفاية؟

4- How often do you organize internal information security audits?

كم مرة تقوم بتنظيم عمليات تدقيق أمن المعلومات الداخلية؟

5- How do you tackle socio-technical issues and risks with respect to information security in your organization?

كيف تتعامل مع القضايا والمخاطر الاجتماعية والتقنية فيما يتعلق بأمن المعلومات في منظمتك؟

6- Has the top management defined its security objectives with respect to business objectives? To what extent is the information security team involved in modifying and developing the policies that can achieve these objectives?

هل حددت الإدارة العليا أهدافها الأمنية فيما يتعلق بأهداف العمل؟إلى أي مدى يشارك فريق أمن المعلومات في تعديل وتطوير السياسات التي يمكن أن تحقق هذه الأهداف؟

7- What are these objectives? How do you formalize information security policies based on those objectives in your organization?

ما هي هذه الأهداف؟كيف يمكنك إضفاء الطابع الرسمي على سياسات أمان المعلومات بناءً على تلك الأهداف في مؤسستك؟

8- Have the details about these information security policies and priorities been properly communicated to employees? If yes, how are these communicated and what communication model you are following and why you have chosen it?

هل تم توصيل التفاصيل المتعلقة بسياسات وأولويات أمن المعلومات بشكل صحيح إلى الموظفين؟إذا كانت الإجابة بنعم ، فكيف يتم توصيل هذه النماذج وما هو نموذج الاتصال الذي تتبعه ولماذا اخترته؟

9- How confident are you that whether these policies defined by the information security department are being followed by employees? Can you elaborate it with some example?

كم أنت واثق من أن ما إذا كانت هذه السياسات التي يحددها قسم أمن المعلومات يتبعها الموظفون؟يمكنك وضع ذلك مع أي مثال؟

10- If any incident occurs due to information security lapse, who is held responsible for it?

في حالة وقوع أي حادث بسبب هفوة أمن المعلومات ، من يتحمل مسؤولية ذلك؟

11- Are the information security policies documented? Also are these policies authorized by the top management? If yes, how often these policies are reviewed and modified?

هل تم توثيق سياسات أمن المعلومات؟أيضا هذه السياسات أذن بها الإدارة العليا؟إذا كانت الإجابة نعم ، فكم مرة يتم مراجعة هذه السياسات وتعديلها؟

هل يمكنك أن تصف بالتفصيل ما هي الأساليب والتقنيات التي تستخدمها لقياس فعالية سياسات أمن المعلومات؟ فعالية بمعنى الحد من التهديدات أو نقاط الضعف أو المخاطر المرتبطة بالأصول التنظيمية ؟.

12- What steps you generally follow up in order to implement thesepolicies ?

.ما هي الخطوات التي تتبعونها بشكل عام من أجل تنفيذ هده السياسات؟

13- What mechanisms are being used for keeping records of information security incidents and risks ?

ما هي الآليات المستخدمة للحفاظ على سجلات حوادث وأخطار أمن المعلومات؟

14-What are the primary assets that the information security department is supposed to protect in your company? What are the risks associated with them ?

ما هي الأصول الأساسية التي يفترض أن تقوم إدارة أمن المعلومات بحمايتها في شركتك؟ ما هي المخاطر المرتبطة بها؟

15- What are your objectives while designing and conducting security awareness programs and trainings? How well the employees follow your training? Has the threat level gone down after these training?

ما هي أهدافك أثناء تصميم وتنفيذ برامج التوعية الأمنية والتدريب؟ كيف يتابع الموظفون تدريباتك؟ هل انخفض مستوى التهديد بعد هذه التدريبات؟

16- Can you describe in detail what methods and techniques you use for measuring the effectiveness of information security policies? Effectiveness in a sense as to mitigate the threats, vulnerabilities or risk associated with organizational assets?

هل يمكنك أن تصف بالتفصيل ما هي الأساليب والتقنيات التي تستخدمها لقياس فعالية سياسات أمن المعلومات؟ فعالية بمعنى الحد من التهديدات أو نقاط الضعف أو المخاطر المرتبطة بالأصول التنظيمية ؟.

Appendix C

Study Participants Information

Table Gender, Occupation and Year of Experiences

Institution	Sex		Occupation				Year of experiences		
	Male	Female	General manager	IT Manager	Engineer	Technician	Less than 5 years	(6-10)	Over 10 years
Ministers and Bank Of Sudan	14	10	1	2	9	15	3	8	13
National Centre of information	9	7	0	1	12	3	13	0	3
Ministry of Finance	5	9	0	1	5	9	8	3	3

Appendix D

Study Questioner Result for Institutions

Table Questioner Result to Ministry of Finance

Ministry of Finance										
NO of Q	Very high	%	□□□□	%	To some extent	%	□□□	%	very low	%
1	0	0	5	21	6	25	2	8	1	4
2	0	0	7	29	3	13	3	13	1	4
3	1	4	1	4	7	29	2	8	3	13
4	2	8	4	17	2	8	3	13	1	4
5	0	0	1	4	9	38	1	4	2	8
6	0	0	4	17	5	21	2	8	2	8
7	2	8	8	33	2	8	0	0	2	8
8	1	4	6	25	5	21	2	8	0	0

9	6	25	7	29	1	4	0	0	0	0
10	0	0	6	25	2	8	2	8	1	4
11	2	8	2	8	5	21	1	4	2	8
12	1	4	9	38	2	8	1	4	1	4
13	1	4	7	29	5	21	5	21	1	4
14	0	0	6	25	7	29	1	4	1	4
15	0	0	7	29	5	21	1	4	1	4
16	0	0	8	33	3	13	0	0	1	4
17	0	0	2	8	7	29	1	4	3	13
18	1	4	5	21	4	17	2	8	1	4
19	0	0	2	8	7	29	2	8	2	8
20	0	0	6	25	4	17	1	4	2	8
21	0	0	4	17	6	25	0	0	1	4
Total %		3		21		19		6		6

Table Questioner Result to National Centre of information.

National Centre of information										
NO of Q	very high	%	□□□□	%	To some extent	%	□□□	%	very low	%
1	7	29	5	21	3	13	1	4	0	0
2	5	21	5	21	3	13	1	4	0	0
3	4	17	2	8	6	25	3	13	1	4
4	11	46	3	13	1	4	0	0	0	0
5	4	17	3	13	8	33	0	0	0	0
6	6	25	5	21	5	21	1	4	0	0
7	4	17	4	17	5	21	0	0	3	13
8	4	17	6	25	5	21	0	0	0	0
9	7	29	4	17	4	17	1	4	0	0
10	3	13	4	17	5	21	3	13	2	8
11	1	4	2	8	5	21	4	17	3	13
12	5	21	5	21	5	21	0	0	1	4
13	6	25	3	13	5	21	0	0	0	0
14	4	17	6	25	4	17	1	4	1	4
15	2	8	4	17	7	29	0	0	1	4
16	2	8	6	25	4	17	2	8	2	8

17	1	4	2	8	7	29	2	8	5	21
18	1	4	5	21	6	25	3	13	0	0
19	1	4	2	8	5	21	5	21	2	8
20	2	8	6	25	4	17	2	8	2	8
21	2	8	4	17	4	17	2	8	2	8
Total %		16		17		20		6		5

Table Questioner Result to Bank of Sudan

Ministers and Bank Of Sudan										
NO of Q	very high	%	□□□□	%	To some extent	%	□□□	%	very low	%
1	7	29	11	46	5	21	0	0	0	0
2	12	50	9	38	3	13	0	0	0	0
3	6	25	10	42	8	33	0	0	0	0
4	11	46	11	46	2	8	0	0	0	0
5	5	21	13	54	4	17	2	8	0	0
6	12	50	9	38	3	13	0	0	0	0
7	15	63	8	33	1	4	0	0	0	0
8	12	50	10	42	2	8	0	0	0	0
9	14	58	8	33	1	4	0	0	0	0
10	5	21	11	46	7	29	0	0	0	0
11	4	17	8	33	4	17	3	13	0	0
12	9	38	12	50	2	8	1	4	0	0
13	3	13	18	75	3	13	0	0	0	0
14	6	25	10	42	7	29	1	4	0	0
15	3	13	15	63	5	21	1	4	0	0
16	1	4	8	33	10	42	4	17	0	0
17	1	4	4	17	11	46	7	29	1	4
18	3	13	11	46	6	25	2	8	2	8
19	6	25	6	25	7	29	3	13	1	4
20	7	29	10	42	5	21	0	0	1	4
21	1	4	9	38	8	33	0	0	0	0
Total %		28		42		21		5		1

Appendix E

Code to monitor policy in Network

```
#############################################################################
###
 This Code To monitor Specific Firewall Rule is applied or not & Send SMS if it's not working
#######    OS : Redhat 6.5
#############################################################################
###
#############################################################################

## CHECK FIREWALL STATUS
service iptablesstaus
#############################################################
#[root@test ~]# service iptables status
#iptables: Firewall is not running.
#############################################################
CHECK_STATUS=$(service iptables status)
if (( $CHECK_STATUS == "iptables: Firewall is not running." ))
then
$SEND_SMS 249xxxxxxxxx "Firewall is not running"
if
#CHECK_IP TAPLES ACTIVE RULES

iptabels -L

################################### result of ABOVE command ####################
#-A INPUT -p tcp --dport 22 -m state --state NEW -j DROP    # Deny  SSH connections.
#-A INPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT  #ALLOW HTTP
#-A INPUT -p tcp --dport 443 -m state --state NEW -j ACCEPT    #ALLOW HTTPS
#############################################################################
####
CHECK_STAT=$(iptables -L | grep -i ssh | awk '{print $12}')

if (( $CHECK_STAT == "DROP" ))
then
$SEND_SMS 249xxxxxxxxx "XXX rule drop the connection from outside"
else
$SEND_SMS 249xxxxxxxxx "XXX rule not drop the connection from outside, please check it"

#################################################
# check number of bytes drooped in some rule
iptables -L -n -v
### OUTPUT WILL BE like THIS
#Chain INPUT (policy DROP 0 packets, 0 bytes)
#pkts bytes target     prot opt in     out     source           destination
#1000  2340  DROP       ssh  --  *      *       x.x.x.x          x.x.x.x
BYTES_DROOPED=$(iptables -L -n -v | grepssh  | awk '{print $2}')
$SEND_SMS 249xxxxxxxxx "Bytes drop XXX rule is $BYTES_DROOPED "
```