[الشعار]

اتفاق إداري

بين

[الكيان المسؤول] نيابة عن حكومة [اسم البلد]

و

الاتحاد الدولي للاتصالات

بشأن

مشروع إنشاء فريق وطني للتصدي للحوادث الحاسوبية (CIRT)

يُبرم هذا الاتفاق الإداري

بين

حكومة [البلد] (يُشار إليها فيما يلي باسم "**الدولة العضو**")، ويمثلها [الكيان المسؤول] التابع لها،

و

الاتحاد الدولي للاتصالات (يُشار إليه فيما يلي باسم "**الاتحاد**")، وهو منظمة حكومية دولية ووكالة متخصصة من وكالات منظمة الأمم المتحدة ويوجد مقره الرئيسي في Place des Nations، جنيف، سويسرا.

وحيث إن الدولة العضو تلتمس تعاون الاتحاد للحصول على المساعدة التقنية المتخصصة لإنشاء مركز فريق وطني للتصدي للحوادث الحاسوبية (CIRT) (يُشار إليه فيما يلي باسم "المركز") يعمل بالتواصل مع شبكة أفرقة التصدي للحوادث الحاسوبية التي أنشئت في إطار التعاون بين الاتحاد والشراكة العالمية المتعددة الأطراف لمكافحة التهديدات السيبرانية (IMPACT)؛

وحيث إن الاتحاد على استعداد لتوفير هذه المساعدة التقنية وفقاً لأحكام وشروط هذا الاتفاق؛

وبالنظر إلى أن الدور الذي يضطلع به البرنامج 2 من خطة عمل حيدر آباد هو دعم الدول الأعضاء في الاتحاد، وخاصة البلدان النامية، لمعالجة القضايا المحددة في المؤتمر العالمي لتنمية الاتصالات لعام 2010 (WTDC-10) الذي عقده الاتحاد، ومن بينها إنشاء هياكل تنظيمية، مثل أفرقة التصدي للحوادث الحاسوبية، بغية تحديد التهديدات السيبرانية وإدارتها والتصدي لها، ووضع آليات للتعاون على الصعيدين الإقليمي والدولي. ويدعو القرار 69 (WTDC-10) إلى "إنشاء أفرقة استجابة وطنية للحوادث الحاسوبية، خاصةً في البلدان النامية، والتعاون فيما بينها"؛

ولذلك، اتفقت الدولة العضو والاتحاد (المشار إليهما معاً فيما يلي باسم "الطرفان") على إبرام هذا الاتفاق الإداري (المشار إليه فيما يلي باسم "هذا الاتفاق").

المادة 1

الغرض من الاتفاق وتنفيذه

1.1 يرسي هذا الاتفاق الأحكام والشروط والإجراءات التي تنظم المساعدة التقنية التي يقدمها الاتحاد للدولة العضو فيما يتعلق بإنشاء المركز، على النحو الموضح في وثيقة المشروع المرفقة والواردة في الملحق 1 بهذا الاتفاق (المشار إليها فيما يلي باسم "المشروع").

2.1 وسيتم وضع وثيقة مشروع منفصلة لكل مشروع آخر قد يُنفذ في إطار هذا الاتفاق وستشكل كل وثيقة مشروع جزءاً لا يتجزأ من هذا الاتفاق.

المادة 2

مسؤوليات الطرفين

1.2 مسؤوليات الاتحاد

يضطلع الاتحاد، وفقاً لقواعده ولوائحه وسياساته وإجراءاته الإدارية والمالية، بمسؤولية توفير المساعدة للدولة العضو على النحو الموضح في هذا الاتفاق وفي وثيقة المشروع المرفقة والواردة في الملحق 1 (المشار إليها فيما يلي باسم "وثيقة المشروع"). ولا يعتبر الاتحاد مسؤولاً عن أي تأخير في تنفيذ الأنشطة المزمعة بموجب هذا الاتفاق بسبب إخفاق الدولة العضو في الوفاء بمسؤولياتها والتزاماتها وفقاً لهذا الاتفاق.

2.2 مسؤوليات الدولة العضو

بغض النظر عن الأحكام الأخرى لهذا الاتفاق وتلك الواردة في وثيقة المشروع، تتحمل الدولة العضو مسؤولية توفير الأموال للاتحاد، والبُنى التحتية المحلية، والمعلومات والمرافق الضرورية التي تتيح التنفيذ المناسب للأنشطة المبينة في هذا الاتفاق وفي وثيقة المشروع. وتلتزم الدولة العضو بأن تحيط الاتحاد علماً على النحو الواجب بكل التدابير المتخذة لتنفيذ هذا الاتفاق والتي قد تؤثر عليه.

المادة 3

الأحكام المالية

1.3 ترد تفاصيل التكاليف المقدرة للمشروع في وثيقة المشروع.

2.3 تضع الدولة العضو، لأغراض تنفيذ المشروع، تحت تصرف الاتحاد مساهمة نقدية يرد مقدارها في وثيقة المشروع (المشار إليها فيما يلي باسم "المساهمة").

3.3 تُودع المساهمة بالفرنك السويسري في الحساب التالي في غضون 30 يوماً بعد التوقيع على وثيقة المشروع:

Account Name: International Telecommunication Union
United Bank of Switzerland (UBS) SA
Case Postale 2600
CH - 1211 Genève 2 (Suisse)
SWIFT Code: UBSWCHZH80A
Account No.: 240-C8108400.2
IBAN: CH58 0024 0240 C810 8400 2

الغرض: مشروع إنشاء مركز فريق وطني للتصدي للحوادث الحاسوبية (CIRT) في [البلد]

4.3 لا يجوز، بأي حال من الأحوال، أن يتعهد الاتحاد بأي التزام فيما يتعلق بتنفيذ الأنشطة الموضحة في وثيقة المشروع (المشار إليها فيما بعد باسم "الأنشطة") قبل تلقيه للمساهمة الكاملة من الدولة العضو. ولا يعتبر الاتحاد مسؤولاً عن حالات التأخير في تنفيذ هذا الاتفاق أو المشروع بسبب تخلف الدولة العضو عن تسديد مساهمتها في الوقت المناسب.

5.3 يستعمل الاتحاد المساهمة، وكل الفوائد المصرفية التي يجنيها على المساهمة، من أجل تنفيذ المشروع.

6.3 يقوم الاتحاد بإدارة المساهمة والأنشطة الممولة منها وفقاً لقواعد الاتحاد ولوائحه وإجراءاته السارية. وبناءً على ذلك، يتم تعيين الموظفين وإدارتهم وشراء المعدات واللوازم والخدمات وإبرام العقود وفقاً لأحكام مثل هذه القواعد واللوائح والإجراءات.

7.3 ووفقاً لطلب صريح من الدولة العضو، ولأغراض هذا الاتفاق والمشروع، يقوم الاتحاد، على وجه الخصوص، باستعمال المساهمة للخدمات التي تتيحها الشراكة العالمية المتعددة الأطراف لمكافحة التهديدات السيبرانية.

8.3 تقوَّم الحسابات والبيانات المالية المتعلقة بالمساهمة والمشروع بالفرنكات السويسرية.

9.3 يضع الاتحاد سجلات محاسبة منفصلة لاستعمالها في المساهمة. وتخضع المساهمة لإجراءات تدقيق المحاسبة الداخلية والخارجية التي تنص عليها القواعد المالية للاتحاد ولوائحه وإجراءاته.

10.3 يُطبق الاتحاد رسوماً إدارية للخدمات العامة بنسبة 7,5 في المائة على جميع النفقات المتكبدة من أموال المساهمة.

11.3 تعاد إلى الدولة العضو كل الأموال المتبقية دون استعمال بعد إكمال جميع الأنشطة أو تُستخدم على النحو المقرر في اتفاق خطي مشترك مبرم بين الطرفين.

12.3 يتقدم الاتحاد إلى الدولة العضو بتقرير نهائي عن المشروع، وفقاً لإجراءات الاتحاد الخاصة بالمحاسبة وتقديم التقارير في غضون ستة (6) أشهر بعد إقفال حسابات السنة التي يتم فيها إكمال المشروع والأنشطة الممولة من المساهمة.

المادة 4

دخول هذا الاتفاق حيز النفاذ ومدته

يدخل هذا الاتفاق حيز التنفيذ اعتباراً من تاريخ توقيعه من كلا الطرفين. وتبقى أحكام هذا الاتفاق سارية المفعول إلى أن يفي الطرفان بجميع الالتزامات والحقوق وفقاً لأحكامه وشروطه.

المادة 5

تعديل الاتفاق وإنهاؤه

1.5 يجوز تمديد هذا الاتفاق أو تنقيحه بواسطة تعديل خطي متفق عليه ويوقع عليه كلا الطرفين بهذه الوثيقة. ويُرفق أي تعديل بهذا الاتفاق ويُشكل جزءاً لا يتجزأ منه.

2.5 يجوز لأي من الطرفين إنهاء هذا الاتفاق بإرسال إشعار إلى الطرف الآخر. ويصبح الإنهاء نافذاً خلال ثلاثين (30) يوماً تقويمياً من استلام الطرف للإشعار المرسل إليه.

3.5 وفي حال إنهاء هذا الاتفاق لأي سبب من الأسباب، يتخذ الاتحاد جميع الخطوات اللازمة ليستكمل المشروع حتى نهايته على نحو سريع ومنظم ويبذل جميع الجهود المعقولة للحفاظ على النفقات المخصصة لهذا الغرض إلى أدنى حد. ولا يتعهد الاتحاد بأي التزام اعتباراً من تاريخ إرسال إشعار كتابي لإنهاء الاتفاق أو استلامه لهذا الإشعار. وتسدَّد من ميزانية المشروع ذات الصلة جميع التكاليف التي يتكبدها الاتحاد وجميع التعويضات المستحقة للاتحاد عن الخدمات المقدمة بموجب هذا الاتفاق وبموجب وثيقة المشروع، في كل حالة وحتى التاريخ الفعلي لإنهاء الاتفاق. وإذا تبقت أي أموال من المساهمة بعد إنهاء المشروع وإنهاء هذا الاتفاق، تُطبق المادة 11.3.

4.5 وبغض النظر عن إنهاء الاتفاق، تبقى أحكامه سارية بقدر ما يكون ذلك ضرورياً للسماح بتصفية الالتزامات المبرمة بين الطرفين بصورة منظمة.

المادة 6

تمثيل الطرفين وعنوان كل منهما

1.6 يعتبر أي إشعار يرسل إلى أحد الطرفين فيما يتعلق بالاتفاق على أنه قد أُرسل فعلياً إذا تم تسليمه أو إرساله برسالة (مع إشعار بالاستلام) أو بواسطة الفاكس أو البريد الإلكتروني الموجه إلى أحد الطرفين على العنوان المذكور أدناه. ويصبح أي إشعار نافذاً اعتباراً من يوم استلامه من الطرف المرسل إليه. ويمكن أن يتغير عنوان أحد الطرفين بإرسال إشعار ملائم إلى الطرف الآخر.

2.6 يوجه كل إشعار إلى الدولة العضو إلى العنوان التالي:

[الكيان المسؤول والبلد]
إلى عناية: [اسم جهة الاتصال]
[عنوان جهة الاتصال]
الهاتف: XXX
الفاكس: XXX
البريد الإلكتروني: XXX

3.6 يوجه كل إشعار يخص الاتحاد إلى العنوان التالي:

International Telecommunication Union
Attn: Mr. Mario Maniewicz
Telecommunication Development Bureau (BDT)
Place des Nations,
CH-1211 Geneva 20, Switzerland
الهاتف: +41 22 730 5421
الفاكس: +41 22 730 5484
البريد الإلكتروني: mario.maniewicz@itu.int

المادة 7

الظروف القاهرة

1.7 في حالة حدوث ظروف قاهرة – أي في حالةٍ يتعذر فيها السيطرة ولا يمكن التنبؤ بها بشكل معقول من قبل أحد الطرفين الذي يُبدي ما يتوجب من اهتمام وعناية – يمكن أن ينجم عنها تأخير أو إعاقة بخلاف ذلك للإنجاز الناجح للمشروع (المشاريع) قيد التنفيذ في إطار هذا الاتفاق، ينبغي أن يبلغ الطرف الذي يواجه هذا الحدث الطرف الآخر كتابةً في غضون (10) عشرة أيام عمل.

2.7 وفي أقرب وقت ممكن بعد استلام هذا الإشعار، يتشاور الطرفان للتحقق من وجود الظروف القاهرة ويحددا تأثيرها على الإنجاز الناجح لأي مشروع (مشاريع) قيد التنفيذ.

3.7 ويبت الطرفان أيضاً بشأن ضرورة إنهاء هذا الاتفاق أو مشروع أو أكثر من المشاريع قيد التنفيذ. وفي حالة الإنهاء، تنطبق الأحكام ذات الصلة الواردة في المادة 3.5.

المادة 8

السرية

يوافق الطرفان على التعامل بسرية فائقة مع جميع الوثائق والمعلومات و/أو البيانات المتحصل عليها خلال إنجاز هذا الاتفاق.

المادة 9

تخلف الاتحاد عن الوفاء بالتزاماته

تُبلِّغ الدولة العضو الاتحاد بواسطة رسالة مسجلة بإشعار بالاستلام، إذا رأت عن حق أن الاتحاد لا يفي بالتزاماته بموجب هذا الاتفاق على أن توضح أسباب رأيها هذا. وإذا لم يقم الاتحاد بالإجابة على هذا الإشعار في غضون خمسة عشر (15) يوم عمل من استلامه الإشعار، يمكن للدولة العضو أن تعتبر الاتفاق منتهياً. وفي هذه الحالة، تُطبَّق أحكام الفقرة 3.5 أعلاه.

المادة 10

تسوية المنازعات

يجب تسوية أي منازعة تنشأ أو تتصل بهذا الاتفاق أو وثيقة المشروع بصورة مباشرة عن طريق التفاوض بين طرفي الاتفاق أو بواسطة وسائل أخرى متفق عليها بين الطرفين كتابةً.

المادة 11

حقوق الطرفين وواجباتهما

تقتصر حقوق كل طرف وواجباته على أحكام وشروط هذا الاتفاق ووثيقة المشروع.

المادة 12

الامتيازات والحصانات والتسهيلات

1.12 إن الاتحاد الدولي للاتصالات هو منظمة حكومية دولية ووكالة متخصصة من وكالات الأمم المتحدة، وعلى ذلك فإنه يتمتع بامتيازات وحصانات وتسهيلات يستمدها من وضعه هذا على نحو ما تُقر الاتفاقات الدولية النافذة والقوانين الوطنية ذات الصلة.

2.12 ليس في هذا الاتفاق أو فيما يتصل به ما يعتبر تنازلاً، صريحاً أو ضمنياً، عن أي امتيازات أو حصانات أو تسهيلات يتمتع بها الاتحاد الدولي للاتصالات.

المادة 13

الاتفاق الكامل، والملحقات

تُمثل الأحكام والشروط المذكورة في هذا الاتفاق وفي وثيقة المشروع الاتفاق الكامل بين الدولة العضو والاتحاد فيما يتعلق بموضوع الاتفاق ووثيقة المشروع، وتُلغي كل ما سبق من اتفاقات أو ترتيبات أو مراسلات أو مفاوضات أو مقترحات أو أي ترتيبات تفاهم أخرى، سواء أكانت مكتوبة أو شفوية، فيما بين الطرفين بشأن الموضوع المذكور. ويتضمن هذا الاتفاق ووثيقة المشروع جميع التعهدات والاشتراطات والأحكام المتفق عليها بين الطرفين. ولا يتمتع وكيل أو ممثل لأي من الطرفين بسلطة الإدلاء بتصريح أو القيام بتمثيل أو إعطاء وعد أو إبرام اتفاق لم ينص عليه طيه، ولن يكون الطرفان ملزمين أو مسؤولين عن ذلك. وجميع الملحقات المرفقة بهذا الاتفاق تشكل جزءاً لا يتجزأ منه.

المادة 14

التنازل

لا يحق لأي الطرفين بأي حال من الأحوال أن يتنازل عن هذا الاتفاق أو أن ينقل جميع الحقوق أو الالتزامات الواردة أدناه أو جزءاً منها لأي طرف ثالث أو كيان آخر دون الموافقة الخطية المسبقة للطرف الآخر.

وإثباتاً لذلك، قام الموقعان أدناه، المصرح لهما بذلك حسب الأصول، بالتوقيع على هذا الاتفاق في نسختين (2) أصليتين باللغة الإنكليزية.

عن حكومة [البلد]	عن الاتحاد الدولي للاتصالات
XXX XXX	**السيد براهيما سانو** مدير مكتب تنمية الاتصالات (BDT)
المكان: _____	المكان: _____
التاريخ: _____	التاريخ: _____
XXX XXX	
المكان: _____	
التاريخ: _____	

رقم المشروع:

اسم المشروع: إنشاء مركز فريق وطني للتصدي للحوادث الحاسوبية (CIRT)

الاسم المختصر للمشروع: مركز CIRT [البلد]

تاريخ البداية: [تاريخ]

التاريخ المتوقع للانتهاء: [تاريخ]

وكالة التعاون الحكومية: [الكيان المسؤول]

البلد المستفيد: [البلد]

مدير المشروع في الاتحاد: ماركو أوبيزو

ملخص المساهمات

أ)	***ميزانية المشروع (بالفرنك السويسري)***	
	الخدمات الخارجية	93 564
	نفقات المهمات	34 960
	المجموع الفرعي	128 524
	نصيب تكاليف الدعم الإداري والتشغيلي (7,5%) من المساهمة النقدية	9 639
	المجموع الكلي:	138 163

ب) ***تقاسم التكاليف***

- مساهمة الاتحاد (العينية) المقدرة بمبلغ: 25 000,00 فرنك سويسري على شكل موارد بشرية
- [البلد] نقداً: 138 163 فرنك سويسري

وصف موجز:

الهدف الرئيسي للمشروع هو مساعدة حكومة [البلد] على إنشاء (فريق وطني للتصدي للحوادث الحاسوبية)، يعمل كنقطة تنسيق مركزية وموثوقة للاتصال من أجل الأمن السيبراني الذي يهدف إلى تحديد التهديدات السيبرانية والدفاع إزاءها والتصدي لها وإدارة مخاطرها.

وسيساعد الاتحاد حكومة [البلد] في بناء القدرات التقنية ونشرها وتوفير التدريب اللازم لإنشاء فريق وطني للتصدي للحوادث الحاسوبية. ومن ثم يتوقع أن يُفضي إلى تطوير قدرة الأمن السيبراني مع المضي قدماً نحو تعزيز التعاون الإقليمي والدولي.

عن	التوقيع	التاريخ	الاسم/اللقب
الاتحاد الدولي للاتصالات:	_____	_____	السيد براهيما سانو مدير مكتب تنمية الاتصالات
[البلد]	_____	_____	
	_____	_____	

1 الخلفية والسياق

1.1 مقدمة عامة

تستعمل العديد من البلدان والحكومات البيئة الديناميكة والمترابطة لأنظمة المعلومات الشبكية من أجل تحسين الاتصالات، وتوفير الضبط، وحماية المعلومات، وتشجيع التنافسية. وأصبحت الحواسيب جزءاً لا يتجزأ من الأنشطة اليومية بحيث لا يمكن فصل المخاطر المرتبطة باستعمال الحاسوب عن الأعمال التجارية العامة والصحة والمخاطر المتصلة بالخصوصية. وأصبحت الآن أصول البلدان الثمينة والهياكل الأساسية الوطنية الحيوية عرضة للخطر من خلال الإنترنت.

ويتواصل تزايد الاعتماد الكلي على الإنترنت[1]. ولسوء الحظ، تحدث ضمن هذه البيئة الديناميكية المتشعبة والمترابطة هجمات سيبرانية سريعة يمكن أن تنتشر في أرجاء العالم خلال دقائق بغض النظر عن الحدود أو الجغرافيا أو الولاية الوطنية. ونتيجةً لذلك، هناك حاجة متزايدة للقدرة على الاتصال والتنسيق والتحليل والتصدي للهجمات السيبرانية عبر مختلف قطاعات الأعمال والحدود الوطنية. وأصبحت شبكة الإنترنت نفسها تشكل بنية تحتية حيوية[2] بالنسبة للعديد من الأمم والأعمال والأشخاص ينبغي حمايتها.

ومن المهم أن تقوم الحكومات بإنشاء أو تحديد منظمات وطنية تعمل كجهات اتصال لضمان الفضاء السيبراني وحماية البنية التحتية الحيوية للمعلومات وتتضمن المهام الموكل إليها المراقبة والإنذار والاستجابة والإنعاش وتيسير التعاون بين الكيانات الحكومية والقطاع الخاص والهيئات الجامعية والمجتمع الدولي[3] عند معالجة قضايا الأمن السيبراني.

ولذلك، يُعد التعاون على الصعيدين الوطني والدولي ضرورياً للربط الفعال للقدرات والخبرات بغية إدارة الحوادث وإذكاء الوعي بشأن الحوادث المحتملة واتخاذ الخطوات اللازمة لمعالجتها. وتضطلع الحكومات بالدور الرئيسي في ضمان التنسيق بين هذه الكيانات.

وهناك ضرورة لإنشاء أفرقة وطنية للتصدي للحوادث الحاسوبية لضمان حماية البنى التحتية الوطنية الحيوية للمعلومات والمساعدة على صياغة خطط إجمالية بشأن النُهج التي تتبعها البلدان فيما يخص قضايا الأمن السيبراني والعمل من ثم كجهات اتصال لمواصلة بناء وتنفيذ الثقافات الوطنية للأمن السيبراني.

2.1 بيان المشكلة

يضطلع فريق التصدي الوطني للحوادث الحاسوبية بدور رئيسي في دعم الحكومة في معالجة القضايا المتصلة بالأمن السيبراني على الصعيد الوطني حيث إن هذا يتعلق بالاستعداد للحوادث السيبرانية واكتشافها وإدارتها والتصدي لها عند حدوثها. ورغم ذلك، يتطلب تنفيذ آلية إدارة الحوادث دراسة مسألة التمويل وتوفير الموارد البشرية والتدريب والقدرة التكنولوجية والعلاقة بين الحكومة والقطاع الخاص والمتطلبات القانونية[4].

وإذا أخذنا في الاعتبار ما ذُكر آنفاً، تواجه البلدان النامية التي لديها موارد بشرية ومؤسساتية ومالية محدودة تحديات خاصة لوضع وتنفيذ السياسات والأطر الوطنية بشأن الأمن السيبراني وحماية البنى التحتية الحيوية للمعلومات.

---

1 http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

2 http://www.itu.int/ITU-D/connect/flagship_initiatives/impact.html

3 http://www.itu.int/md/D06-SG01-C-0249/en

4 http://www.itu.int/md/D06-SG01-C-0249/en

3.1 مسوغات المشروع

يُركز هذا المشروع على مساعدة حكومة [البلد] على تنظيم وتجهيز نفسها بغية النهوض باستجابتها إزاء التهديدات السيبرانية. ويولي المشروع اهتماماً خاصاً لتحسين الأمن السيبراني لتعزيز حماية البنى التحتية [للبلد] الخاصة بتكنولوجيا المعلومات والاتصالات، بما في ذلك البنى التحتية الحيوية للمعلومات، وإتاحة خدمات موثوقة إلى الوكالات الحكومية والمواطنين والأعمال التجارية. ويُعتبر العديد من هذه الخدمات جزءاً من الحياة اليومية وله تأثير مباشر على الرفاه والتقدم الاقتصادي [للبلد].

ويندرج إنشاء فريق وطني للتصدي للحوادث الحاسوبية في عداد العناصر الرئيسية للنهج الوطني الخاص بالأمن السيبراني ولبنة متينة يمكن أن ترتبط بها أنشطة أخرى متصلة بالأمن السيبراني. وبالمستطاع أن يشكل إنشاء فريق وطني للتصدي للحوادث الحاسوبية، وإعداد عمليات متصلة به على الصعيد الوطني، مرتكزاً لاستحداث الأنشطة التالية:

- بناء قاعدة معرفية تدعم إعداد وتنفيذ استراتيجية وطنية [في البلد] للأمن السيبراني فضلاً عن وضع نهج وطني لحماية البنى التحتية الحيوية للمعلومات؛
- دعم بناء ثقافة وطنية للأمن السيبراني وتعزيز مبادرات إذكاء الوعي ذات الصلة؛
- دعم تطوير المنصات الوطنية للأمن السيبراني ذات الصلة، على سبيل المثال: البنية التحتية الوطنية للمفاتيح العمومية (PKI)، وإطار ونهج إلكترونيان حكوميان، وإطار إدارة الهوية الوطنية والنفاذ، ومكافحة الرسائل الاقتحامية، والبرمجيات الروبوتية، وما إلى ذلك؛
- المساعدة في تخطيط ووضع استراتيجية وطنية بشأن حماية الأطفال على الخط؛
- مواصلة تمكين [البلد] لتطوير وتعزيز استجابته الوطنية إزاء حوادث الإنترنت وقدراته في مجال الإدارة.

4.1 العلاقة مع برامج مكتب تنمية الاتصالات وأنشطته

إن الهدف من البرنامج 2 من خطة عمل حيدر آباد هو دعم الدول الأعضاء في الاتحاد، لا سيما البلدان النامية في معالجة القضايا التي حددها المؤتمر العالمي لتنمية الاتصالات لعام 2010، ومن بينها *إنشاء الهياكل التنظيمية مثل أفرقة التصدي للحوادث الحاسوبية (CIRT) لتحديد التهديدات السيبرانية وإدارتها والتعامل معها، ووضع آليات التعاون على المستويين الإقليمي والدولي.*

ولهذا السبب، فقد اعتمد المؤتمر العالمي لتنمية الاتصالات لعام 2010 القرار 69 بشأن "*إنشاء أفرقة استجابة وطنية للحوادث الحاسوبية خاصة في البلدان النامية، والتعاون فيما بينها*".

ويضطلع الاتحاد الدولي للاتصالات، باعتباره المسهل الرئيسي لخط العمل جيم[5] للقمة العالمية لمجتمع المعلومات، بمسؤولية مساعدة أصحاب المصلحة في بناء الثقة والأمن في استعمال تكنولوجيات المعلومات والاتصالات (ICT)[6] على الأصعدة الوطنية والإقليمية والدولية.

وبالإضافة إلى ذلك، فإن القرار 130 للاتحاد (غوادالاخارا، 2010) بشأن "تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات"، ***يكلف بشكل خاص مدير مكتب تنمية الاتصالات بدعم الدول الأعضاء في جهودها الرامية للحماية من التهديدات السيبرانية على الأصعدة الوطنية والإقليمية والدولية، حسب الاقتضاء، من خلال إنشاء آليات مثل أفرقة التصدي للحوادث الحاسوبية لتحديد التهديدات السيبرانية وإدارتها والتعامل معها ووضع آليات التعاون على المستويين الإقليمي والدولي.***

---

5 http://www.itu.int/osg/csd/cybersecurity/WSIS/

6 http://www.itu.int/wsis/docs/geneva/official/poa.html

ودعا المؤتمر العالمي لتنمية الاتصالات لعام 2010 أيضاً إلى مساعدة الدول الأعضاء لإنشاء هياكل تنظيمية، مثل أفرقة التصدي للحوادث الحاسوبية، لتحديد التهديدات السيبرانية وإدارتها والتعامل معها، ووضع آليات التعاون على المستويين الإقليمي والدولي.

وفي هذا الإطار، أطلق الأمين العام للاتحاد البرنامج العالمي للأمن السيبراني (GCA) باعتباره إطار الاتحاد بشأن التعاون الدولي لأصحاب المصلحة المتعددين بغية تحقيق مجتمع معلومات أكثر أمناً وأكثر سلامة، ويركز البرنامج على مجالات العمل الرئيسية الخمس التالية:

- التدابير القانونية
- التدابير التقنية والإجرائية
- الهياكل التنظيمية
- بناء القدرات
- التعاون الدولي

وقد قام الاتحاد في سبتمبر 2008، في إطار البرنامج العالمي للأمن السيبراني وكجزء من الجهود المبذولة لتحقيق التنسيق العالمي والتعاون الدولي بشأن الأمن السيبراني، بتوقيع مذكرة تفاهم مع الشراكة العالمية المتعددة الأطراف لمكافحة التهديدات السيبرانية (IMPACT).

2 الاستراتيجية

1.2 الهدف الإجمالي للمشروع

إن الهدف من هذا المشروع هو مساعدة حكومة [البلد] في إرساء قدراته الخاصة بالأمن السيبراني ومواصلة تطويرها بما في ذلك إنشاء فريق التصدي للحوادث الحاسوبية تكون له مسؤولية على الصعيد الوطني.

2.2 استراتيجية المشروع

تهدف الاستراتيجية الإجمالية إلى تسهيل العملية الرامية إلى وضع استراتيجية وطنية للأمن السيبراني في [البلد]. وهكذا فإن الهدف هو تزويد حكومة [البلد] في البداية بمركز فريق وطني للتصدي للحوادث الحاسوبية قادر على العمل.

وسيقوم هذا المشروع بما يلي:

- تسهيل إرساء قدرات للمراقبة والإنذار والتصدي للحوادث الحاسوبية للنهوض بتحديد التهديدات السيبرانية وإدارتها والتعامل معها؛
- مساعدة [البلد] في تحديد قطاعات البنى التحتية الوطنية الحيوية للمعلومات ووضع مرتكز على الصعيد الوطني يتيح مواصلة وضع وتنفيذ الاستراتيجية الوطنية للأمن السيبراني؛
- بناء القدرة الوطنية ونقل الدراية اللازمة من أجل تيسير مواصلة التطوير ضمن مجال حماية البنى التحتية الوطنية الحيوية للمعلومات مثل إنشاء الأفرقة القطاعية للتصدي للحوادث الحاسوبية وما إلى ذلك.

3 النتائج المتوقعة

من خلال تنفيذ هذا المشروع، من المتوقع التوصل إلى النتائج الأولية والثانوية التالية:

1.3 النتائج الأولية المتوقعة:

- مركز فريق وطني للتصدي للحوادث الحاسوبية قادر على تزويد الجهات المعنية [في البلد] بمجموعة أساسية من الخدمات.

2.3 النواتج الثانوية المتوقعة:

- خبرة وطنية معززة بشأن الأمن السيبراني وسد الفجوة المتعلقة بالقدرة البشرية الخاصة بالأمن السيبراني.
- تحسين التأهب الوطني بشأن تحديد الحوادث الحاسوبية ومنعها والتصدي لها وإيجاد حلول لها (من المطلوب إعداد تقييم أولي وتقييم لاحق لعملية التنفيذ).
- استعمال وتشغيل فريق التصدي للحوادث الحاسوبية من خلال بناء فريق استجابة فعال وكفء وقادر ومستعد للتصدي للهجمات السيبرانية التي تستهدف البنى التحتية الوطنية الحيوية للمعلومات. وسيضطلع فريق التصدي للحوادث الحاسوبية بمهمة المستشار الموثوق لدى الحكومة فيما يخص القضايا المتعلقة بالأمن السيبراني.
- وضع برامج تدريبية وطنية للتوعية من شأنها تحسين إجراءات الأمن السيبراني للدفاع عن البنى التحتية والوكالات الحكومية وحمايتها.
- زيادة القدرة على سن تدابير أمنية فعالة وإرساء استجابات معقولة عندما تحدث هذه التهديدات الحقيقية.

4 مؤشرات الأداء

المؤشرات هي:

- إنشاء فريق وطني للتصدي للحوادث الحاسوبية وتشغيله بحلول نهاية المشروع؛
- تدريب (3) ثلاثة مسؤولين حكوميين من [البلد] على الأقل لإدارة الفريق الوطني للتصدي للحوادث الحاسوبية؛
- صياغة خارطة طريق بشأن بناء ثقافة وطنية للأمن السيبراني كجزء من الاستراتيجية الوطنية للأمن السيبراني في إطار تدابير تعزيز الفريق الوطني للتصدي للحوادث الحاسوبية.

5 الأنشطة

بغية الوفاء بأهداف المشروع، يقوم الطرفان بعدد من الأنشطة:

1.5 أنشطة الاتحاد الدولي للاتصالات

ستكون أنشطة المشروع المنفذة متضافرة مع البرنامج 2 من خطة عمل حيدر آباد وأنشطة الاتحاد الإقليمية المزمعة وذلك لضمان التنفيذ الفعال للمشروع.

وتشمل الأنشطة الخاصة بالاتحاد في المشروع ما يلي:

- إعداد اختصاصات المتعاقد الخارجي (IMPACT) والتعاقد مع هذا الأخير وفقاً للاتفاق الإداري.

- تقييم الموقع والإعداد للشروع في المشروع.
- تقديم وتحديث خطة المشروع وخارطة طريقه من خلال جدولة مواعيد معقولة طيلة المشروع.
- توفير بناء القدرات والتدريب على أساس الثغرات في المجالات المحددة خلال تنفيذ المشروع.
- وضع مواد تدريبية مصممة خصيصاً لتحقيق أهداف [البلد] فيما يخص بناء القدرات بشأن الأمن السيبراني.
- تدريب الخبراء – مواصلة تطوير المهارات الموجودة المتيسرة في البلد.
- تصميم العمليات خصيصاً وتطويرها لإدارة عمليات فريق التصدي للحوادث الحاسوبية.
- تصميم برمجيات فريق التصدي للحوادث الحاسوبية على نحو يلبي احتياجات [البلد] ويتماشى مع العمليات والاستراتيجية ذات الصلة.
- تركيب أدوات برمجية عن بُعد خاصة بفريق التصدي للحوادث الحاسوبية – وتشمل الأنشطة المتضمنة في تركيب البرمجيات:
  - بوابة عامة
  - وسيلة تتبع الطلبات لأغراض الاستجابة للحوادث (RTIR)
  - قائمة بريدية

وسيضطلع أعضاء فريق [البلد] بالمسؤولية الحصرية عن تلبية المتطلبات الأساسية للمخدمات التي تستضيف هذه الأدوات الثلاث مثل تشكيلات نظام التشغيل وتشكيلات الشبكات أو أي أعمال تضبيط أخرى تتعلق بإتاحة هذه الأنظمة للخبراء من الاتحاد ومؤسسة إمباكت أو للمستعملين النهائيين المعنيين.

- بداية التشغيل وإجراء تقييم للعمليات/تنفيذ مشروع فريق التصدي للحوادث الحاسوبية لضمان الجودة.

2.5 أنشطة البلد المستفيد

تشمل أنشطة [البلد] الخاصة بالمشروع ما يلي:

- المساعدة في إعداد الموقع لإقامة فريق التصدي للحوادث الحاسوبية.
- توفير المعدات الموصى بها – تكوين المعدات الحاسوبية/البرمجيات الأساسية لنظام التشغيل لنشر الحلول التي وضعها فريق التصدي للحوادث الحاسوبية.
- مساعدة فريق المشروع فيما يخص توفير اللوجستيات للدورات التدريبية.
- القيام مع فريق المشروع بإعداد مواد لتنفيذ الأنشطة الوطنية الخاصة بإذكاء الوعي.

6 المدخلات/المساهمات

1.6 الاتحاد الدولي للاتصالات:

المساهمة العينية	الموارد البشرية والمهارات اللازمة لتنسيق المشروع وإدارته – سيقدم الاتحاد المهارات وسيبدي الاهتمام والعناية التي من شأنها أن توفر أساساً معقولاً لضمان نجاح المشروع الذي تقدر تكاليفه بمبلغ 000 25 فرنك سويسري

2.6 [البلد]:

المساهمة النقدية	163 138 فرنك سويسري (ترد التفاصيل في ميزانية المشروع – انظر الملحق 1)
المساهمة العينية	1 الالتزام المالي بإنشاء فريق للتصدي للحوادث الحاسوبية واستدامته. 2 الموارد البشرية لتنفيذ وإدارة المشروع بأكمله (على الأقل 3 أفراد). 3 المرفق (الموقع الفعلي والبنى التحتية المتصلة). 4 المعدات الحاسوبية والبرمجيات الأساسية (المخدّمات والعملاء ونظام التشغيل والشبكة وما إلى ذلك.).

سيقوم [البلد] بتوفير فريق للمشروع مؤلف من موظفيه (على الأقل (3) ثلاثة مسؤولين) لتنفيذ وتنسيق المشروع في عين المكان مع الاتحاد؛ وتعبئة الشركاء المحليين؛ واستضافة اجتماعات الفريق القائم بالمشروع؛ وتأهيل المدربين الذين يتألفون من مدير فريق التصدي للحوادث الحاسوبية ومحللين؛ وتوفير المتطلبات اللوجستية المحلية بما في ذلك نشر المعدات والموارد البشرية؛ والتوصيل بالإنترنت والمعدات الحاسوبية والترويج المشروع لدى أصحاب المصلحة في الوكالات الحكومية وما إلى ذلك.

وسيشرف [البلد] على اشتراك الكيانات الوطنية المطلوبة ويكون مسؤولاً عن الترويج للمشروع لدى وسائل الإعلام الوطنية والمجتمعات المحلية بهدف الحصول على الانخراط المتواصل لأصحاب المصلحة ومعرفتهم بالمشروع وأهميته. ويضطلع انخراط أصحاب المصلحة بدورٍ مهم في نجاح المشروع وفعاليته على الصعيد الكلي.

7 إدارة المخاطر

- يكمن الخطر الأساسي الذي يواجه هذا المشروع في أن الأنشطة داخل البلد يمكن أن تعاني من تأخيرات ناتجة عن أحداث وظروف محلية غير متوقعة. وسيؤدي استخلاص التزام من الحكومة خلال المراحل الأولى للتخطيط من التقليل من هذا الخطر.
- هناك خطر آخر متعلق بالمشروع وهو احتمال ألا تكون الموارد البشرية المخصصة للمشروع (من طرف حكومة [البلد]) غير مناسبة، وهو ما قد يطيل الوقت اللازم لإكماله. ويمكن التقليل من هذا الخطر بتوفير موقع ملائم وتنفيذ الاتحاد لدورات تدريبية قطرية.
- وكخطوة أولى فقد أجرى قطاع تنمية الاتصالات دراسة جدوى مقدماً [للبلد] بشأن إنشاء فريق للتصدي للحوادث الحاسوبية لتعزيز إدارة المخاطر المتعلقة بالتأخيرات أو زيادة التكاليف المحتملة للمشروع.

8 إدارة المشروع

سينفذ المشروع مدير المشروع الذي يعينه الاتحاد بالتنسيق الوثيق مع جهة (جهات) اتصال [البلد] والمتعاقد الخارجي (إمباكت).

وسيشرف الاتحاد، باعتباره الوكالة المنفذة، ويدير عملية التنفيذ الشاملة للمشروع وفقاً لقواعد الاتحاد ولوائحه وإجراءاته.

9 الأدوار والمسؤوليات

1.9 الاتحاد الدولي للاتصالات (ITU)

سيقوم الاتحاد بما يلي:

- توفير الموارد من الموظفين لتنسيق وإدارة المشروع والاضطلاع بمسؤولية الإدارة الإجمالية لتنفيذه والإشراف عليه ومراقبته وتنسيق عملياته وتقييمه.
- تقديم خبرته وتجربته الدولية للتمكين من تحقيق أهداف المشروع بصورة فعالة وكفؤة.
- تخصيص الخبراء للمشروع وفقاً للعقد والاختصاصات.
- الاتصال بالأطراف المعنية لضمان نجاح المشروع.
- إسداء المشورة وبذل المساعدة لفريق المشروع عند اللزوم قبل وخلال وبعد تنفيذ المشروع.
- إيجاد الحلول/شفرة مصدر البرمجيات وتقديم وثائق التطوير ذات الصلة إلى البلد المستفيد دون فرض تكاليف إضافية باعتبار ذلك جزءاً من المشروع.
- تحديد احتياجات البلد المستفيد والمساعدة في وضع خارطة طريق لتطور فريق وطني للتصدي للحوادث الحاسوبية.
- توفير خارطة طريق لبناء القدرة البشرية والاحتياجات المتعلقة بالتدريب لتطوير خدمات فريق وطني للتصدي للحوادث الحاسوبية.
- نقل الدراية إلى [البلد] بشأن الحلول التي يقدمها فريق التصدي للحوادث الحاسوبية وعمله اليومي وآليات وعمليات الدفاع من أجل الأمن السيبراني ضد بعض الهجمات الشائعة على البنى التحتية الحيوية الوطنية للمعلومات.
- إعداد تقارير دورية بشأن تقدم المشروع.
- إعداد تقرير ختامي عن المشروع يتضمن بياناً مالياً عند إكمال المشروع.

2.9 البلد المستفيد

سيقوم [البلد] بما يلي:

- نقل الأموال المخصصة للاتحاد وتقديم المدخلات/المساهمات الواردة في القسم 2.6.
- توفير النفاذ الفعلي والافتراضي للمرفق المحدد والمخصص لفريق التصدي للحوادث الحاسوبية وإتاحة النفاذ إلى الشبكة. ويلزم النفاذ الفعلي لتمكين خبراء الاتحاد ومؤسسة إمباكت من تنفيذ جزء المشروع الذي يلزم تنفيذه في الموقع، ويلزم النفاذ الافتراضي لتمكين خبراء الاتحاد ومؤسسة إمباكت من تنفيذ جزء المشروع الذي يلزم تنفيذه خارج الموقع عن بُعد.
- شراء المعدات الموصى بها – المعدات الحاسوبية/البرمجيات على أساس التصميم المتفق عليه للمركز، وتشكيل المعدات الحاسوبية/البرمجيات اللازمة لتمكين خبراء الاتحاد ومؤسسة إمباكت من التنفيذ عن بُعد للحلول الخاصة بالفريق. وعلى أعضاء فريق [البلد] حل جميع مشاكل المتعلقة بالشبكات والمخدمات من أجل تمكين خبراء الاتحاد ومؤسسة إمباكت من تنفيذ هذه الحلول.
- توفير الموارد والمرافق للمشروع عندما يُقام مكتب للمشروع ويكون بالمستطاع إجراء دورات تدريبية.

- تعيين النظراء الوطنيين (موظفون تقنيون مؤهلون) الذين سيساعدون في استضافة فريق المشروع وتوفير الموارد اللوجستية المحلية بما في ذلك نشر المعدات. وسيقوم النظراء الوطنيون الذين عينهم [البلد] بمساعدة الاتحاد والمجموعة المختارة من المتعاقدين من الباطن من خلال توفير المعلومات الدقيقة وذات الصلة بالمشروع.
- توفير المعلومات اللازمة لتنفيذ أنشطة المشروع المخطط لها والمتفق عليها.
- توفير الموارد البشرية لتشغيل فريق التصدي للحوادث الحاسوبية بفعالية.
- توفير الحيز المكاني والمعدات الحاسوبية ومرافق للبرمجيات على النحو الذي تتطلبه طبيعة المشروع ويحتاجه إنشاء فريق للتصدي للحوادث الحاسوبية.
- توفير الدعم الإداري (بما في ذلك إصدار وتسليم التأشيرات لأعضاء فريق المشروع وتسهيل إجراءات التخليص الجمركي لكل المعدات الضرورية والمواد، وما إلى ذلك) خلال تنفيذ المشروع وتوفير أي مساعدة ضرورية للتنفيذ الناجح للمشروع.
- جمع البيانات بشأن الهجمات السيبرانية وتلخيص التوجهات الإحصائية وأنماط الهجمات واستخلاص المعلومات على أساس ذلك، والتوصل إلى تقاسم فعلي للمعرفة.
- رصد الموارد اللازمة لمواصلة تشغيل مرافق فريق التصدي للحوادث الحاسوبية بعد إكمال المشروع.
- إصدار جميع الشهادات والتصاريح والرخص والإعفاءات وموافقات التخليص وأي مستندات أخرى قد يحتاجها الاتحاد أو المتعاقد الخارجي للمشروع فيما يتعلق بتوفير خدمات أو منتجات [للبلد] في إطار هذا المشروع.

10 استدامة المشروع

تؤثر التهديدات السيبرانية بشكل متزايد على الحياة اليومية لمستعملي تكنولوجيا المعلومات والاتصالات، ولذلك يُعتبر الفريق الوطني للتصدي للحوادث الحاسوبية حلاً مستداماً بسبب قدراته في مواجهة التهديدات السيبرانية. وعلاوةً على ذلك، يضمن [البلد] استدامة إنشاء فريق وطني للتصدي للحوادث الحاسوبية. وعلى النحو الموضح في القسم 9 من وثيقة المشروع، يتعهد [البلد] باتخاذ التدابير اللازمة لإبقاء الفريق الوطني للتصدي للحوادث الحاسوبية قيد التشغيل.

11 الرصد والتقييم

يقوم مدير المشروع بإعداد تقارير دورية عن التقدم المحرز وهو ما يتيح ملخصاً عن الإنجازات والأنشطة فضلاً عن التحديات التي واجهها المشروع خلال فترة زمنية معينة.

وسيقوم الاتحاد بالتعاون مع [البلد] عند نهاية المشروع بإعداد تقرير نهائي لتقييم نجاح المشروع من حيث بلوغ أهدافه الرئيسية المحددة، وإحراز النتائج المتوقعة، وتحقيق تأثير على تطور البلد المستفيد في المستقبل.

وبغية تقييم المشروع، قد تطلب تعليقات بعد التنفيذ من كل [بلد] لاستخلاص دروس مفيدة فيما يخص التخطيط وتكرار مشاريع تنفيذية مماثلة في ظروف مماثلة في المستقبل وتكييف المواد التدريبية.

12 الميزانية

ترد الميزانية في الملحق ألف.

13 خطة العمل ونظرة عامة على منهجية الفريق الوطني للتصدي للحوادث الحاسوبية

ترد خطة العمل ونظرة عامة على منهجية الفريق في الملحق باء.

الملحق ألف – ميزانية المشروع (مساهمة نقدية)

يعرض الجدول 1 الميزانية الإجمالية المقدرة لهذا المشروع بحسب بنود الإنفاق. ويستند التصنيف بحسب بند الإنفاق على أحدث المعلومات المتوفرة حالياً وهو قابل للتغيير خلال تنفيذ المشروع. ولضمان التنفيذ الناجح للمشروع، سيتمتع مدير المشروع بالمرونة التي تسمح له بنقل الأموال من بند إلى آخر من بنود الميزانية حسب الاقتضاء.

الجدول 1 – ميزانية المشروع بالفرنك السويسري

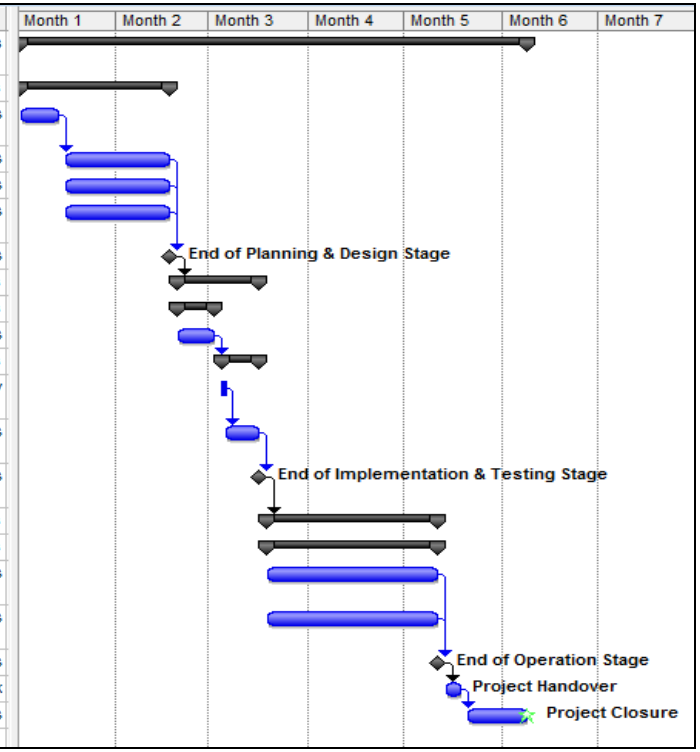
فئات الجهات الراعية	الوصف	تقديرات
	الخدمات الخارجية*	
3310	تعاقدات خارجية لقطاع تنمية الاتصالات	**93 564**
	تكاليف المهمات	
3111	موظفون – DSA	2 300
3112	نقل الموظفين	4 140
3113	نفقات مختلفة خاصة بالمهمة – الموظفين	920
3141	خدمات استشارية DSA-SSA	14 720
3142	خدمات نقل – خدمات استشارية SSA	9 200
3143	نفقات مختلفة خاصة بالمهمة – خدمات استشارية SSA	3 680
	المجموع الفرعي	**34 960**
	المجموع	**128 524**
	تكاليف أخرى	
3730	الدعم التشغيلي والإداري (AOS) (7,5%)	**9 639**
	المجموع	**138 163**

تفاصيل الخدمات الخارجية	
الوصف	**المبلغ**
تصميم وتطوير الفريق وما يقدمه من حلول	12 512
إعداد مواد التدريب وأنشطة التدريب المناسبة	12 512
تكييف وتطوير العمليات	25 024
تحديد وصقل الحلول التي يقدمها الفريق	17 204
إرساء الحلول التي يقدمها الفريق واختبارها	6 256
تقييم العمليات والتنفيذ	6 256
دعم مرحلة ما بعد التنفيذ بواسطة الاتصالات الهاتفية والبريد الإلكتروني (12 شهراً)	13 800
بما في ذلك التقييم والتوعية والتخطيط والتصميم والتنفيذ والدعم وإعداد التقارير وتحصين المخدّم	**93 564**

الملحق باء – خطة العمل ونظرة عامة على منهجية الفريق الوطني للتصدي للحوادث الحاسوبية

يبين الجدول 2 الوارد فيما يلي المهام الرئيسية اللازمة لنجاح تنفيذ هذا المشروع والمدة الزمنية اللازمة لإنجازها، ويوفر نظرة عامة على منهجية الفريق.

	Task Name	Duration
1	**National CIRT Establishment**	**115 days**
2	**Planning & Design Stage (Offsite)**	**35 days**
3	Create & Approve User Requirement Specification (URS)	2 wks
4	Design CIRT According to URS	5 wks
5	Network Design according to URS	5 wks
6	Pre-Installation & Preparation Step by Step Guide for Network & Hardware	5 wks
7	End of Planning & Design Stage	0 days
8	**Implementation & Testing Stage**	**20 days**
9	**Offsite**	**10 days**
10	Remote Installation & Testing	2 wks
11	**Onsite**	**10 days**
12	Project Kick-off Meeting & Signing of Approved URS	1 day
13	Fine-tuning of CIRT Application & Training	1.8 wks
14	End of Implementation & Testing Stage	0 days
15	**Operation Stage**	**40 days**
16	**Offsite**	**40 days**
17	Service Desk Support for CIRT Operations	8 wks
18	Final Project Handover Documentation Preparation	8 wks
19	End of Operation Stage	0 days
20	Project Handover	1 wk
21	Project Closure	3 wks



1 اسم المهمة

إنشاء فريق وطني للتصدي للحوادث الحاسوبية

مرحلة التخطيط والتصميم الأولين (خارج الموقع)

وضع وإقرار مواصفات متطلبات المستعمل (URS)

تصميم فريق للتصدي للحوادث الحاسوبية وفقاً لمواصفات متطلبات المستعمل

تصميم الشبكة وفقاً لمواصفات متطلبات المستعمل

الدليل التدريجي للتركيب والإعداد الأوليين الشبكة والمعدات الحاسوبية

نهاية مرحلة التخطيط والتصميم

مرحلة التنفيذ والاختبار

خارج الموقع

التركيب والاختبار عن بُعد

في الموقع

اجتماع بدء المشروع والتوقيع على مواصفات متطلبات المستعمل (URS) المعتمدة

صقل تطبيقات وتدريبات فريق التصدي للحوادث الحاسوبية

نهاية مرحلة التنفيذ والاختبار

مرحلة التشغيل

خارج الموقع

دعم مكتب الخدمات لعمليات فريق التصدي للحوادث الحاسوبية

إعداد الوثائق النهائية لتسليم المشروع

نهاية مرحلة التشغيل

تسليم المشروع

إقفال المشروع

2 المدة

3 الأيام

4 الأسابيع

5 الشهور

6 نهاية مرحلة التخطيط والتصميم

7 نهاية مرحلة التنفيذ والاختبار

8 نهاية مرحلة التشغيل

9 تسليم المشروع

10 إقفال المشروع


CIRT Methodology Overview
Planning & Design
Implementation
Operations
Collaboration
• Determine & Confirm Constituency
• Define & Confirm Mission Statement
• Determine CIRT Services
People:
• Trainings
• Incident Handling Activities
• Information Dissemination
• Cooperation Between Other CIRTS
• Determine ReportingStructure, Authority &Organisation Model
• Define CIRT Processes & Workflow
• Develop Policies, Procedures and Documentations
Process:
• Finalised CIRT Processes & Workflow
• Finalised Policies, Procedures&Documentations
• Managing CIRT Staff
• Managing CIRT Infrastructure
• Identify CIRT Media Spokesperson(s)
• Identify Interactions with Key Parts of the Constituency
• Define Roles and Responsibilities for Interactions
• Determine Technology Requirements (HW, SW, Tools, etc.)
Technology:
• Assess Infrastructure for theConstituency
• Hardware & Software Installation
• Disaster Recovery Plan
• Quality Assurance Review
• Human Resource Requirements
• Capacity Building
• Communications Approach
• CIRT Facilities
Others:
• Legal Issues
• CIRT Announcement

1 **نظرة عامة على منهجية فريق التصدي للحوادث الحاسوبية**

2 **التخطيط والتصميم**

- تحديد وتأكيد الجهات المعنية
- تحديد وتأكيد بيان المهمة
- تحديد خدمات فريق التصدي للحوادث الحاسوبية
- تحديد هيكل إعداد التقارير وسلطة ونموذج التنظيم
- تحديد عمليات فريق التصدي للحوادث الحاسوبية وتسلسل سير العمل
- وضع السياسات والإجراءات وإعداد الوثائق
- تحديد التفاعلات بين الأعضاء الرئيسيين من الجهات المعنية
- تحديد أدوار ومسؤوليات التفاعلات
- تحديد متطلبات التكنولوجيا (HW، SW، أدوات، إلخ.)
- متطلبات الموارد البشرية
- بناء القدرة
- نهج الاتصالات
- مرافق فريق التصدي للحوادث الحاسوبية

3 **التنفيذ**

الأشخاص:

- التدريبات

العملية:

- إتمام وضع عمليات فريق التصدي للحوادث الحاسوبية وتسلسل سير العمل
- إتمام وضع السياسات والإجراءات وإكمال الوثائق

التكنولوجيا:

- تقييم البنى التحتية للجهات المعنية
- تركيب المعدات الحاسوبية والبرمجيات

مسائل أخرى:

- مسائل قانونية
- إعلان فريق التصدي للحوادث الحاسوبية

4 **العمليات**

- أنشطة معالجة الحوادث
- نشر المعلومات
- إدارة موظفي فريق التصدي للحوادث الحاسوبية
- إدارة البنى التحتية لفريق التصدي للحوادث الحاسوبية
- تحديد الناطق (الناطقين) باسم فريق التصدي للحوادث الحاسوبية لدى وسائل الإعلام
- خطة التعافي من الكوارث
- استعراض ضمان الجودة

5 التعاون

- التعاون مع الأفرقة الأخرى للتصدي للحوادث الحاسوبية