**آزمایشگاه آپا**

**آگاهی‌رسانی، پشتیبانی و امداد در**

**حوزه امنیت سیستم‌عامل**

**دانشگاه صنعتی امیرکبیر**

**(با حمایت مرکز تحقیقات مخابرات ایران)**

**گروه مدیریت**

# جریانهای کاری مربوط به رویه ایجاد آمادگی/تقویت/پیشرفت در یک گروه پاسخگویی به حوادث کامپیوتری رسمی

**FC_۸۷_۰۶_۰۲**

**تاریخ: ۸۷/۰۶**

| مشخصات سند | | | |
|---|---|---|---|
| **نام سند:** جریانهای کاری مربوط به رویه ایجاد آمادگی/تقویت/پیشرفت در یک گروه پاسخگویی به حوادث کامپیوتری رسمی | | | |
| **کد فایل** | **آخرین نسخه** | **تاریخ آخرین بازبینی** | **گروه** |
| FC_۸۷_۰۶_۰۲ | ۱،۱ | ۸۷/۰۸/۱۷ | مدیریت |

| سابقه سندها | | | |
|---|---|---|---|
| **نسخه** | **تاریخ تنظیم** | **تنظیم‌کننده** | **توضیحات** |
| ۱،۰ | ۸۷/۰۶/۰۳ | خدیجه محمدزاده | ایجاد |

## چکیده

در این مستند ،جریانهای کاری مربوط به رویه ایجاد آمادگی/تقویت/پیشرفت که اولین رویه برای ایجاد یک گروه پاسخگویی به حوادث کامپیوتری رسمی است مورد بررسی قرار می گیرد.

## فهرست مطالب

**۱ ایجادآمادگی /تقویت /پیشرفت ..... ۱**

۱-۱ نمودار جریان کاری رویه ایجادآمادگی /تقویت /پیشرفت ..... ۲

**۲ منابع و مراجع ..... ۱۸**

## فهرست شکلها

شکل ۱- نمودار جریان کاری رویه ایجاد آمادگی/ تقویت/ پیشرفت..... ۲

## فهرست جداول

جدول ۱-توضیح جریان کاری رویه ایجاد آمادگی/تقویت/پیشرفت ..... ۲

# ۱ ایجادآمادگی /تقویت /پیشرفت

این رویه شامل کارهای لازم برای انجام مدیریت حوادث در یک زمان کوتاه و موثر است و شامل موارد زیر است:

- کارکنان مورد نیاز و آموزشهایی که این کارکنان برای انجام کار خود به آن‌ها نیاز دارند.
- ابزار، تجهیزات و زیرساختارهای حمایتی لازم مانند ارتباطات امن شبکه ای ، مکانیسم هایی برای ایجاد ارتباطات امن ، ابزار آنالیز ، ابزاری برای گزارش حوادث به صورت آنلاین و پایگاه داده‌هایی برای پیگیری حوادث.
- سیاستها و رویه‌هایی که نحوه برقراری ارتباط مدیریت حوادث با بقیه بخشها و همچنین نحوه عملکرد آن را تعیین می‌کنند. این بخش ممکن است شامل سیاستهای افشاء اطلاعات ، رویه‌های استاندارد انجام اعمال و یا هر گونه توافقی در سطح سرویس‌ها باشد .

یک بخش از این رویه برای ایجاد یک مدیریت حوادث ابتدایی یا یک گروه پاسخگویی به حوادث کامپیوتری ابتدایی است. برای این مرحله، زیر رویه اصلی را می‌توان به دو بخش تقسیم کرد:

- برنامه ریزی و طراحی (PC۱-PC۳)
- پیاده سازی (PC۵-C۷)

در فاز برنامه ریزی و طراحی، آنالیز نیازها و تعریف نیازمندیها انجام می‌شود تا مشخص شود که گروه پاسخگویی به حوادث کامپیوتری در واقع چه کاری را انجام خواهد داد (PC۱). نیازمندیها ممکن است از منابع مختلفی مانند مذاکره و بحث با گروههای ذی نفع، بررسی سیاستها و راهنماهای موجود، نیازهای تجاری و قوانینی که برای پیاده سازی مدیریت حوادث باید در نظر گرفت جمع‌آوری شده باشند.

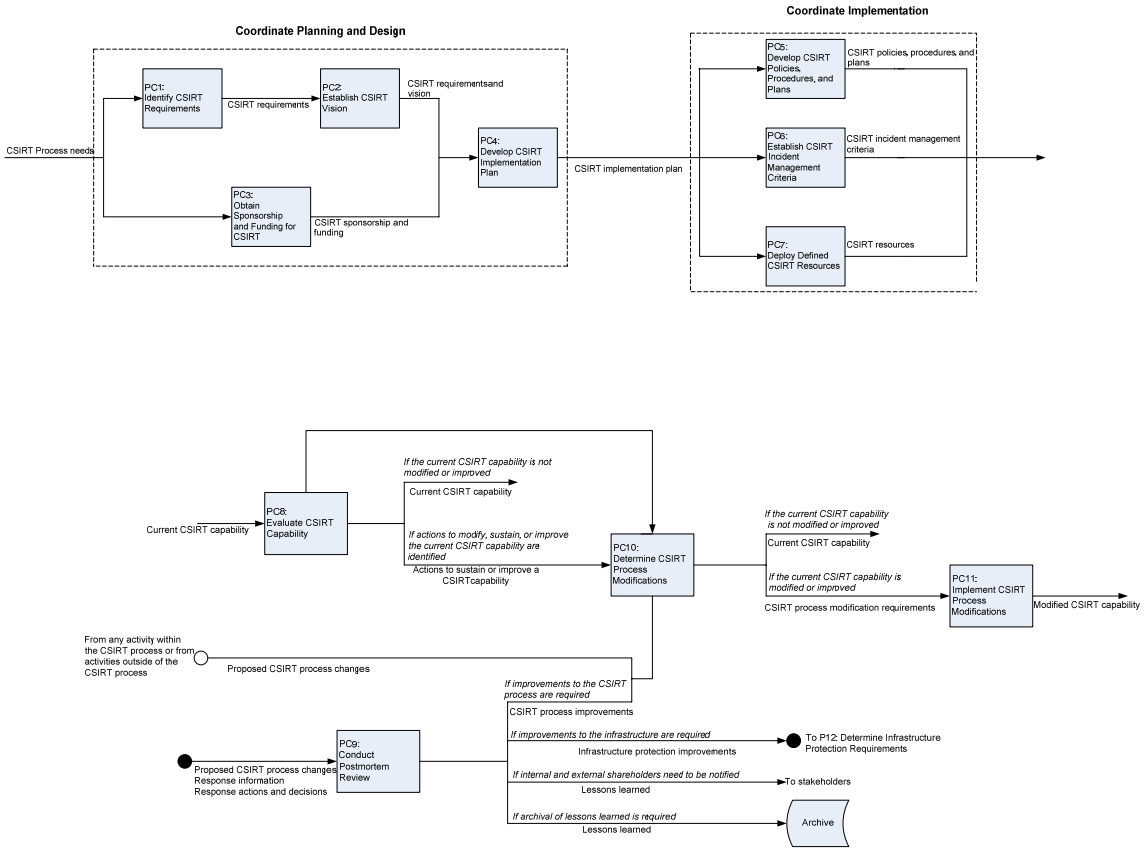
از تعریف نیازها می‌توان برای مشخص کردن اهداف گروه پاسخگویی به حوادث کامپیوتری (شامل تعریف ماموریت، مشتریان، سرویس‌ها، مدل ساختاری و منابع لازم) استفاده کرد (PC۲). یک رویه موازی به دنبال تامین منابع از طریق پشتیبان مالی می گردد (PC۳).

سپس طرح پیاده سازی ایجاد می گردد (PC۴) و این طرح برای ساخت، تامین پرسنل و تجهیزات گروه پاسخگویی به حوادث کامپیوتری مورد استفاده قرار می گیرد (PC۵-PC۷) رویه‌های PC۵-PC۷ ترتیبی نیستند و می‌توانند به صورت موازی انجام شوند.

رویه آمادگی شامل زیر رویه‌هایی برای پیشرفت و تقویت توانایی های موجود است . زمانی که یک مدیریت حوادث یا گروه پاسخگویی به حوادث کامپیوتری به وجود آمد می‌تواند مورد ارزیابی قرار گیرد(PC۸). اگر در انتهای رویه پاسخگویی، نیاز به یک بازبینی پس از حادثه وجود داشته باشد این فعالیت به عنوان بخشی از وظایف رویه آمادگی انجام می‌شود (PC۹). اطلاعات به دست آمده از ارزیابی یا بازبینی پس از حادثه مرور می‌شوند و تغییراتی که باید در رویه‌ها اعمال شوند مشخص می گردند (PC۱۰) و سپس این تغییرات اعمال می‌شوند(PC۱۱ ).

## ۱-۱ نمودار جریان کاری رویه ایجادآمادگی /تقویت /پیشرفت

برنامه ریزی و طراحی




**شکل ۱- نمودار جریان کاری رویه ایجاد آمادگی/ تقویت/ پیشرفت**

**جدول ۱-توضیح جریان کاری رویه ایجاد آمادگی/تقویت/پیشرفت**

| ماموریتها/اهداف | زمان فعال شدن |
|---|---|
| • ایجاد یک گروه پاسخگویی به حوادث کامپیوتری رسمی به نحوی که اهداف و نیازهای مشتریان را تامین کند.<br>• پیشرفتهایی در گروه پاسخگویی به حوادث کامپیوتری موجودبه نحوی که نیازهای مشتریان را تامین کند. | • زمانی که یک سازمان تصمیم به ایجادیک گروه پاسخگویی به حوادث کامپیوتری می گیرد.<br>• زمانی که یک سازمان تصمیم به ارزیابی گروه پاسخگویی به حوادث کامپیوتری موجود می گیرد.<br>• زمانی که سازمان تصمیم می گیرد تغییراتی در گروه پاسخگویی به حوادث کامپیوتری ایجاد کند تصمیم گیری برای ایجاداین تغییرات از راههای |

| | |
|---|---|
| | دیگری به غیر از بازبینی پس از حادثه به دست آمده است. |

| ورودیها | | |
|---|---|---|
| **ورودی** | **توضیح** | **شکل** |
| نیازهای گروه پاسخگویی به حوادث کامپیوتری | این بخش، وضعیتی است که گروه پاسخگویی به حوادث کامپیوتری وجود ندارد و نیاز به ایجاد یک گروه پاسخگویی به حوادث کامپیوتری احساس می شود. نیاز به ایجاد گروه پاسخگویی به حوادث کامپیوتری ممکن است از جاهای مختلفی مانند سازمان، کشور و قوانین بین‌الملل و نیازهای امنیتی نشات گرفته باشد | شفاهی، فیزیکی، الکترونیکی |
| تواناییهای موجود گروه پاسخگویی به حوادث کامپیوتری | شامل منابع موجود برای تامین سرویس‌هایی که مورد نیاز مشتریان است می‌باشد. | افراد ، رویه‌ها ، تکنولوژیها |
| تغییرات پیشنهاد شده برای اعمال در گروه پاسخگویی به حوادث کامپیوتری | ایجاد تغییراتی در گروه پاسخگویی به حوادث کامپیوتری موجود. این پیشنهادات ممکن است از جاهای مختلفی مطرح شده باشند از جمله:<br>• اطلاعات ناشی از مشاهداتی که به دنبال پیدا کردن نقاط آسیب‌دیده هستند.<br>• تغییراتی که از جانب مدیریت بیان می‌شوند. (تصمیم در جهت واگذاری بخشی از رویه‌ها به خارج از سازمان، تغییر در اهداف یا نیازمندیها و یا سرویس‌ها)<br>• تغییراتی که از جانب قوانین وآیین نامه ها اعمال می‌شوند. | شفاهی ، فیزیکی ، الکترونیکی |
| اطلاعات مربوط به پاسخهای داده | شامل همه پاسخها و اطلاعات | شفاهی ، فیزیکی ، الکترونیکی |

| | | |
|---|---|---|
| شده | مربوط به آن‌ها که برای بازبینی پس از حادثه به آن‌ها نیاز داریم می‌باشد. | |
| فعالیتها و تصمیمات رویه پاسخگویی | شامل اطلاعات زیر درباره پاسخها است:<br>• اعمال فنی ،مدیریتی یا حقوقی انجام شده<br>• تصمیمات فنی ، مدیریتی و حقوقی گرفته شده | شفاهی ، فیزیکی ، الکترونیکی |

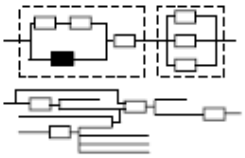
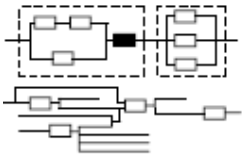
| معیارهای اتمام | سیاستها و قوانین | نیازهای عمومی |
|---|---|---|
| • زمانی که گروه پاسخگویی به حوادث کامپیوتری رویه‌های خود را رسمی کرد و یا تیم پاسخگویی به حوادث کامپیوتری به وجود آمد.<br>• زمانی که رویه‌های گروه پاسخگویی به حوادث کامپیوتری بهبود یافت. | • سیاستهای گروه پاسخگویی به حوادث کامپیوتری/ فناوری اطلاعات<br>• معیارها، استانداردها، راهنماها و قوانین مربوط به امنیت<br>• سیاستهای امنیتی سازمان<br>• سیاستهای سازمان که بر اعمال گروه پاسخگویی به حوادث کامپیوتری تاثیر گذار است.<br>• مقررات گزارش دهی (حفاظت از زیرساختار، نظامی ، اقتصادی ، دانشگاهی و دولتی) | • پرسنل معینی آموزشهای لازم جهت انجام مشاغل خود را دریافت می‌کنند.<br>• پرسنل معینی رویه‌های گروه پاسخگویی به حوادث کامپیوتری را پس از بررسی استانداردها، راهنماها و قوانین مربوطه مدل می‌کنند.<br>• پرسنل معینی، نتایج را مطابق با سیاستهای گروه پاسخگویی به حوادث کامپیوتری و سازمان ،مستندسازی می‌کنند. |

| خروجیها | | | |
|---|---|---|---|
| **تصمیم** | **خروجی** | **توضیح** | **شکل** |
| یک گروه پاسخگویی به حوادث کامپیوتری ابتدایی به وجود آمده است. | گروه پاسخگویی به حوادث کامپیوتری ابتدایی | این مرحله شامل مجموعه ابتدایی از منابع( افراد ،رویه‌ها و تکنولوژیها) که برای مدیریت حوادث و پیاده سازی آن لازم | افراد، رویه‌ها و تکنولوژی ها |

| | | | |
|---|---|---|---|
| | | است می‌باشد. گروه پاسخگویی به حوادث کامپیوتری شامل عناصر زیر است:<br>• ماموریت<br>• کاربران<br>• مجموعه سرویس‌ها<br>• یک مدل ساختاری یا چارچوب تعریف شده<br>• منابع تخصیص داده شده به همراه تعیین وظایف و اختیارات<br>• تجهیزات لازم برای انجام توابع مدیریت حوادث<br>• زیرساختار امن فیزیکی و الکترونیکی | |
| گروه پاسخگویی به حوادث کامپیوتری موجود تغییر یا بهبود پیدا نمی‌کند. | گروه پاسخگویی به حوادث کامپیوتری موجود | این مرحله شامل منابع موجود (افراد، رویه‌ها و تکنولوژیها) است و تغییری در گروه پاسخگویی به حوادث کامپیوتری موجود داده نمی‌شود. | افراد، رویه‌ها و تکنولوژیها |
| گروه پاسخگویی به حوادث کامپیوتری موجود تغییر یا بهبود می‌یابد. | گروه پاسخگویی به حوادث کامپیوتری تغییریافته | این مرحله با اعمال تغییرات لازم که از راههای مختلفی به دست آمده است انجام می‌شود. حاصل این مرحله مجموعه تغییریافته‌ای از منابع (افراد، رویه‌ها وتکنولوژیها) می‌باشد. | افراد، رویه‌ها وتکنولوژیها |
| بهبودهایی در زیرساختار لازم است. | بهبود حفاظت از زیرساختار | بهبود حفاظت از زیرساختار شامل راههایی برای | شفاهی ، الکترونیکی یا فیزیکی |

| | | | |
|---|---|---|---|
| | | افزایش امنیت زیرساختاراست. در طی رویه آمادگی این پیشنهادات در طی بازبینی پس از حادثه به دست می آید و به رویه حفاظت از زیرساختار ارسال می شود. | |
| گروههای ذی نفع داخلی یا خارجی باید آگاه شوند.<br>ذخیره سازی مطالبی که آموخته شده است. | مطالبی که آموخته شده است. | این مطالب از بازبینی رسمی یا غیررسمی فعالیتها، تصمیمات و رخدادهای مربوط به پاسخ به دست می آید. | شفاهی، الکترونیکی یا فیزیکی |

| زیررویه | نیازمندیهای زیررویه | رویه‌های نوشته شده |
|---|---|---|
| PC۱: تعیین نیازمندیهای گروه پاسخگویی به حوادث کامپیوتری<br> | • نیروهای معینی نیازهای رویه گروه پاسخگویی به حوادث کامپیوتری را جمع‌آوری و مرور می‌کنند. | • پرسنل معینی رویه‌ها و راهنماهای مدیریت پروژه و پیاده سازی سازمان را دنبال می‌کنند.<br>• پرسنل معینی در زمانی که نیازمندیهای گروه پاسخگویی به حوادث کامپیوتری را تعیین می‌کنند رویه‌ها ، قوانین و راهنماهای سازمان‌های دیگر را مطالعه می‌کنند.<br>• پرسنل معینی راهنماها و رویه‌های مربوط به مدیریت تغییرات سازمان را دنبال می‌کنند. |
| PC۲ : تعریف اهداف گروه پاسخگویی به حوادث کامپیوتری<br> | • پرسنل معینی اهداف گروه پاسخگویی به حوادث کامپیوتری که شامل ماموریت، کاربران، سرویس‌ها، چارچوب سازمانی و منابع است را تعیین می‌کنند.<br>• پرسنل معینی این اهداف را تصویب می‌کنند. | • پرسنل معینی رویه‌ها و راهنماهای مدیریت پروژه و پیاده سازی سازمان را دنبال می‌کنند.<br>• پرسنل معینی در زمانی که مقررات گروه پاسخگویی به حوادث کامپیوتری را تعیین |

| | | |
|---|---|---|
| | ورودیها: نیازمندیهای گروه پاسخگویی به حوادث کامپیوتری<br>خروجیها: اهداف گروه پاسخگویی به حوادث کامپیوتری | می‌کنند رویه‌ها، قوانین و راهنماهای سازمان‌های دیگر را مطالعه می‌کنند.<br>• پرسنل معینی راهنماها و رویه‌های مربوط به مدیریت تغییرات سازمان را دنبال می‌کنند. |
| PC۳: تامین منابع مالی گروه پاسخگویی به حوادث کامپیوتری<br>  | • پرسنل معینی برای تاسیس گروه پاسخگویی به حوادث کامپیوتری، منابع مالی را تامین می‌کنند.<br>ورودیها: نیازهای گروه پاسخگویی به حوادث کامپیوتری<br>خروجیها: پشتیبان مالی گروه پاسخگویی به حوادث کامپیوتری و سرمایه | • پرسنل معینی راهنماهای سازمان را برای به دست آوردن پشتیبان مالی دنبال می‌کنند.<br>• پرسنل معینی راهنماهای بودجه‌ای را برای محاسبه و تامین سرمایه لازم برای انجام پروژه دنبال می‌کنند. |
| PC۴: ایجاد یک طرح برای پیاده سازی گروه پاسخگویی به حوادث کامپیوتری<br>  | • نیروهای معینی طرحی برای پیاده سازی گروه پاسخگویی به حوادث کامپیوتری ایجاد می‌کنند. | • پرسنل معینی رویه‌ها و راهنماهای مدیریت پروژه و پیاده سازی سازمان را دنبال می‌کنند.<br>• پرسنل معینی در زمان ایجاد طرح برای پیاده سازی گروه پاسخگویی به حوادث کامپیوتری، رویه‌ها، قوانین و راهنماهای سازمان‌های دیگر را مطالعه می‌کنند.<br>• پرسنل معینی راهنماها و رویه‌های مربوط به مدیریت تغییرات سازمان را دنبال می‌کنند. |

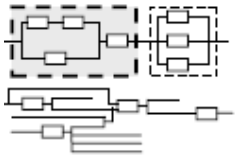
| ورودیها | خروجیها |
|---|---|
| نیازمندیها و اهداف گروه پاسخگویی به حوادث کامپیوتری<br><br>پشتیبان مالی و سرمایه گروه پاسخگویی به حوادث کامپیوتری | طرح پیاده سازی گروه پاسخگویی به حوادث کامپیوتری |

| افراد مورد نیاز | تکنولوژی |
|---|---|
| • از پرسنل زیر برای تعیین نیازمندیهای تیم پاسخگویی به حوادث کامپیوتری می‌توان استفاده کرد:<br>- مدیران اجرایی (مدیران سطح C)<br>- مدیران تجاری<br>- کارکنان فناوری اطلاعات<br>- نمایندگانی از امور اداری (حقوقی، منابع انسانی )<br>- نمایندگانی از کاربران<br>- نمایندگانی از امور قانونی<br>- نمایندگانی از زیرساختارهای حساس<br>- شرکت ثالث فراهم کننده سرویس امنیت | • این افراد می‌توانند از تکنولوژیهای زیر برای تعیین نیازمندیهای گروه پاسخگویی به حوادث کامپیوتری استفاده کنند:<br>- تکنولوژیهای مستندات و انتشار<br>- کانالهای ارتباطی که می‌توانند در صورت نیاز رمزنگاری شوند(پست الکترونیک، ویدئو کنفرانس، نرم‌افزارهای مورد استفاده گروه[1] و وب) |
| • از نیروهای زیر برای تعیین اهداف گروه پاسخگویی به حوادث کامپیوتری می‌توان استفاده کرد:<br>- مدیران اجرایی (مدیران سطح C) | • این افراد می‌توانند از تکنولوژیهای زیر استفاده کنند:<br>- مستندات و انتشارات<br>- کانالهای ارتباطی که می‌توانند در صورت |

[1] Groupware

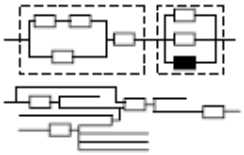
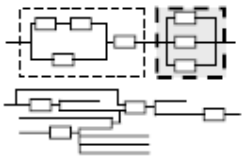
[2] decision support systems

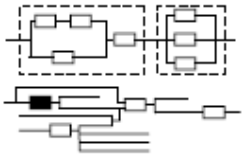
| | |
|---|---|
| - مدیران تجاری<br>- کارکنان فناوری اطلاعات<br>- نمایندگانی از امور اداری (حقوقی ، منابع انسانی)<br>- نمایندگانی از کاربران<br>- نمایندگانی از امور قانونی<br>- نمایندگانی از زیرساختارهای حساس<br>- شرکت ثالث فراهم کننده سرویس امنیت | نیاز رمزنگاری شوند(پست الکترونیک، ویدئو کنفرانس، نرم‌افزارهای مورد استفاده گروه و وب)<br>- *"سیستم‌های حمایت از تصمیم"*[۲] |
| • از نیروهای زیر برای تامین سرمایه و به دست آوردن پشتیبان مالی می‌توان استفاده نمود:<br>- تیم ایجاد کننده گروه پاسخگویی به حوادث کامپیوتری<br>- مدیران اجرایی (مدیران سطح C)<br>- مدیران تجاری<br>- مدیر گروه پاسخگویی به حوادث کامپیوتری<br>- پشتیبان مالی گروه پاسخگویی به حوادث کامپیوتری<br>- کارکنان بازاریابی و امور تجاری | • این افراد می‌توانند از تکنولوژیهای زیر استفاده کنند:<br>- کانالهای ارتباطی که می‌توانند در صورت نیاز رمزنگاری شوند(پست الکترونیک ، ویدئو کنفرانس ،نرم‌افزارهای مورد استفاده گروه و وب)<br>- سیستم‌های اقتصادی و حسابداری |
| • برای ایجاد طرح پیاده سازی گروه پاسخگویی به حوادث کامپیوتری می‌توان از نیروهای زیر استفاده کرد:<br>- تیم ایجاد کننده گروه پاسخگویی به حوادث کامپیوتری<br>- مدیران اجرایی (مدیران سطح C)<br>- مدیران تجاری<br>- کارکنان فناوری اطلاعات<br>- نمایندگانی از امور اداری (حقوقی ، منابع انسانی )<br>- نمایندگانی از کاربران<br>- نمایندگانی از امور قانونی<br>- نمایندگانی از زیرساختارهای حساس<br>- شرکت ثالث فراهم کننده سرویس امنیت<br>- مدیر گروه پاسخگویی به حوادث کامپیوتری<br>- پشتیبان مالی گروه پاسخگویی به حوادث کامپیوتری | • از تکنولوژیهای زیر می‌توان بدین منظور استفاده کرد:<br>- نرم افزارهای مدیریت و برنامه ریزی پروژه<br>- مستندات و انتشارات<br>- کانالهای ارتباطی که می‌توانند در صورت نیاز رمزنگاری شوند(پست الکترونیک ، ویدئو کنفرانس ،نرم‌افزارهای مورد استفاده گروه و وب) |

| زیررویه | نیازمندیهای زیررویه | رویه‌های نوشته شده |
|---|---|---|
| برنامه ریزی و طراحی  | نیروهای معینی در برنامه ریزی با هم همکاری می‌کنند.<br>اطلاعاتی که به اشتراک گذشته می شود:<br>• نیازمندیها و اهداف گروه پاسخگویی به حوادث کامپیوتری<br>• پشتیبان مالی و سرمایه گروه پاسخگویی به حوادث کامپیوتری<br>خروجی:<br>طرح پیاده سازی گروه پاسخگویی به حوادث کامپیوتری | • پرسنل معینی رویه‌هایی که برای تعیین نیازمندیها و اهداف گروه پاسخگویی به حوادث کامپیوتری، به دست آوردن پشتیبان مالی و سرمایه و ایجاد طرح پیاده‌سازی گروه پاسخگویی به حوادث کامپیوتری لازم است را دنبال می‌کنند.<br>• نیروهای معینی رویه های مناسب برای طراحی گروه پاسخگویی به حوادث کامپیوتری را دنبال می‌کنند.<br>• نیروهای معینی راهنماهای مدیریت تغییرات سازمان یا گروه پاسخگویی به حوادث کامپیوتری را دنبال می‌کنند.<br>• نیروهای معینی در زمان طراحی گروه پاسخگویی به حوادث کامپیوتری ، راهنماها ، رویه‌ها و قوانین مربوط به سازمان‌های دیگر را مطالعه می‌کنند. |
| PC۵ : تعریف سیاستها، رویه‌ها و طرحها | • نیروهای معینی، سیاستها، طرحها و رویه‌های مرکزی گروه پاسخگویی به حوادث کامپیوتری را با توجه به طرح پیاده سازی تعریف می‌کنند و نتایج را مستندسازی می‌کنند.<br>• نیروهای معینی ، سیاستها، رویه‌ها و طرحهای گروه پاسخگویی به حوادث کامپیوتری را به تصویب می رسانند. | • نیروهای معینی رویه‌های سازمان را برای مستندسازی و رسمی کردن رویه‌ها، سیاستها و طرحها دنبال می‌کنند.<br>• نیروهای معینی راهنماها و رویه‌های مدیریت پروژه و پیاده سازی سازمان را دنبال می‌کنند.<br>• نیروهای معینی در زمانی که سیاستها، رویه‌ها و طرحهای گروه پاسخگویی به حوادث کامپیوتری را ایجاد می‌کنند راهنماها، قوانین، طرحها و رویه‌های سازمان‌های دیگر را مطالعه می‌کنند. |

| | | |
|---|---|---|
| | ورودیها: طرح پیاده سازی گروه پاسخگویی به حوادث کامپیوتری<br>خروجیها: سیاستها، طرحها و رویه‌های گروه پاسخگویی به حوادث کامپیوتری | |
| PC۶: تعریف معیارها و ضوابط گروه پاسخگویی به حوادث کامپیوتری<br> | • نیروهای معینی به منظور پشتیبانی از رویه‌های مشخص شده در طرح پیاده سازی گروه پاسخگویی به حوادث کامپیوتری، راهنماهایی برای<br>• طبقه بندیها<br>• الویتها<br>• استراتژیهای پاسخگویی<br>• لیستهای آگاه سازی<br>• رویه‌های تعدیل کننده<br>ایجاد می‌کنند.<br><br>ورودیها: طرح پیاده سازی گروه پاسخگویی به حوادث کامپیوتری<br>خروجیها: ضوابط و معیارهای گروه پاسخگویی به حوادث کامپیوتری | • نیروهای معینی راهنماها، رویه‌ها و قوانین مربوط به سازمان‌های دیگر را مطالعه می‌کنند. |

| افراد مورد نیاز | تکنولوژیها و اطلاعات |
|---|---|
| • از نیروهای زیر برای برنامه ریزی و طراحی گروه پاسخگویی به حوادث کامپیوتری می‌توان استفاده کرد:<br>- افرادی که در مراحل تعیین نیازمندیها و اهداف، به دست آوردن پشتیبان مالی و سرمایه و ایجاد طرح پیاده سازی گروه پاسخگویی به حوادث کامپیوتری شرکت کردند. | • این افراد می‌توانند از تکنولوژیهای زیر استفاده کند:<br>- کانالهای ارتباطی که می‌توانند در صورت نیاز رمزنگاری شوند(پست الکترونیک، ویدئو کنفرانس ، نرم‌افزارهای مورد استفاده گروه و وب)<br>- تکنولوژی مستندات و انتشارات |
| • از نیروهای زیر برای تعریف سیاستها، طرحها و رویه‌های گروه پاسخگویی به حوادث کامپیوتری می‌توان استفاده کرد:<br>- تیم ایجاد کننده گروه پاسخگویی به حوادث کامپیوتری<br>- مدیران اجرایی (مدیران سطح C)<br>- مدیران تجاری<br>- کارکنان فناوری اطلاعات<br>- نمایندگانی از امور اداری (حقوقی ، منابع انسانی )<br>- نمایندگانی از کاربران<br>- نمایندگانی از امور قانونی<br>- نمایندگانی از زیرساختارهای حساس<br>- شرکت ثالث فراهم کننده سرویس امنیت<br>- نویسندگان فنی | • این افراد می‌توانند از تکنولوژیهای زیر استفاده کنند:<br>- کانالهای ارتباطی که می‌توانند در صورت نیاز رمزنگاری شوند(پست الکترونیک، ویدئو کنفرانس ،نرم‌افزارهای مورد استفاده گروه و وب)<br>- تکنولوژی مستندات و انتشارات<br>- نرم افزارهای مدیریت و برنامه ریزی پروژه |
| • از نیروهای زیر برای تعیین معیارها و ضوابط گروه پاسخگویی به حوادث کامپیوتری می‌توان استفاده کرد:<br>- تیم ایجاد کننده گروه پاسخگویی به حوادث کامپیوتری<br>- مدیران اجرایی (مدیران سطح C)<br>- مدیران تجاری<br>- کارکنان فناوری اطلاعات<br>- نمایندگانی از امور اداری (حقوقی ، منابع انسانی )<br>- نمایندگانی از کاربران<br>- نمایندگانی از امور قانونی<br>- نمایندگانی از زیرساختارهای حساس<br>- شرکت ثالث فراهم کننده سرویس امنیت | • این افراد می‌توانند از تکنولوژیهای زیر استفاده کنند:<br>- کانالهای ارتباطی که در صورت نیاز رمزنگاری می‌شوند(پست الکترونیک، ویدئو کنفرانس ،نرم‌افزارهای مورد استفاده گروه و وب)<br>- تکنولوژی مستندات و انتشارات<br>- نرم افزارهای مدیریت و برنامه ریزی پروژه |

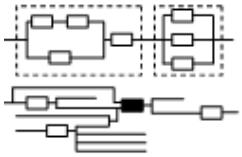
| زیر رویه | نیازمندیهای زیررویه | رویه‌های نوشته شده |
|---|---|---|
| PC۷: تامین منابع گروه پاسخگویی به حوادث کامپیوتری<br>  | • نیروهای معینی منابع لازم را با توجه به طرح پیاده سازی گروه پاسخگویی به حوادث کامپیوتری مشخص و سازماندهی می‌کنند (کارکنان، تجهیزات و زیرساختار)<br><br>ورودی: طرح پیاده سازی گروه پاسخگویی به حوادث کامپیوتری<br>خروجی: منابع گروه پاسخگویی به حوادث کامپیوتری | • نیروهای معینی راهنماها، رویه‌ها و قوانین مربوط به سازمان‌های دیگر را مطالعه می‌کنند.<br>• نیروهای معینی سیاستهای مربوط به نیروی انسانی و رویه‌هایی برای پرداخت و آموزش کارکنان را دنبال می‌کنند.<br>• نیروهای معینی راهنماها و رویه‌های خرید سازمان را دنبال می‌کنند.<br>• نیروهای معینی راهنماها یا رویه‌های سازمان در ارتباط با مدیریت پروژه و پیاده سازی را دنبال می‌کنند.<br>• نیروهای معینی سیاستهای امنیتی و استانداردها را به هنگام نصب منابع، تجهیزات و زیرساختار دنبال می‌کنند. |
| پیاده سازی<br>  | • نیروهای معینی در فعالیتهای پیاده سازی با هم همکاری می‌کنند.<br>اطلاعاتی که به اشتراک گذاشته می شود:<br>• سیاستها، رویه‌ها و طرحهای گروه پاسخگویی به حوادث کامپیوتری<br>• معیارها و ضوابط گروه پاسخگویی به حوادث کامپیوتری<br>• منابع گروه پاسخگویی به حوادث کامپیوتری<br>خروجی:<br>یک گروه پاسخگویی به حوادث | • نیروهای معینی، رویه‌هایی که برای تعریف سیاستها، معیارها و تامین منابع گروه پاسخگویی به حوادث کامپیوتری لازم است را دنبال می‌کنند.<br>• نیروهای معینی راهنماها یا رویه‌های سازمان در ارتباط با مدیریت پروژه و پیاده سازی را دنبال می‌کنند.<br>• نیروهای معینی راهنماها، رویه‌ها و قوانین مربوط به سازمان‌های دیگر را مطالعه می‌کنند.<br>• نیروهای معینی، راهنماها و رویه‌های مدیریت تغییرات سازمان یا گروه پاسخگویی |

| | | |
|---|---|---|
| | کامپیوتری ابتدایی | به حوادث کامپیوتری را دنبال می‌کنند. |
| PC۸: ارزیابی گروه پاسخگویی به حوادث کامپیوتری<br>  | • نیروهای معینی، گروه پاسخگویی به حوادث کامپیوتری را ارزیابی و توانایی های آن را برآورد می‌کنند و تصمیم گیرند که گروه پاسخگویی به حوادث کامپیوتری چه کاری انجام دهد(در جهت بهبود تغییر یابد یا تغییری نیابد)<br><br>ورودی: توانایی‌های موجود گروه پاسخگویی به حوادث کامپیوتری<br>خروجی: توانایی‌های موجود گروه پاسخگویی به حوادث کامپیوتری<br>اعمالی برای بهبود این تواناییها | • نیروهای معینی راهنماها، رویه‌ها و قوانین مربوط به سازمان‌های دیگر را مطالعه می‌کنند.<br>• نیروهای معینی رویه‌ها و متدلوژیهای سازمان برای انجام ارزیابی را دنبال می کنند. |

| افراد مورد نیاز | تکنولوژیها |
|---|---|
| • از نیروهای زیر برای تعیین و سازماندهی منابع می‌توان استفاده کرد:<br>- تیم ایجاد کننده گروه پاسخگویی به حوادث کامپیوتری<br>- مدیران اجرایی (مدیران سطح C)<br>- مدیران تجاری<br>- کارکنان فناوری اطلاعات<br>- نمایندگانی از امور اداری (حقوقی ، منابع انسانی )<br>- نمایندگانی از کاربران | • این افراد می‌توانند از تکنولوژیهای زیر استفاده کنند:<br>- مستندات و انتشارات<br>- سیستم‌های منابع انسانی<br>- سیستم‌های خرید<br>- سیستم‌ها و تکنولوژیهای شبکه که گروه پاسخگویی به حوادث کامپیوتری به آنها نیاز دارد.<br>- سیستم‌های امنیت فیزیکی<br>- کانالهای ارتباطی که می‌توانند در صورت نیاز رمزنگاری شوند(پست الکترونیک، |

| | |
|---|---|
| - نمایندگانی از امور قانونی<br>- نمایندگانی از زیرساختارهای حساس<br>- شرکت ثالث فراهم کننده سرویس امنیت | ویدئو کنفرانس ،نرم‌افزارهای مورد استفاده گروه و وب)<br>- نرم افزارهای مدیریت و برنامه ریزی پروژه |
| • برای فعالیتهای پیاده سازی می‌توان از نیروهای زیر استفاده کرد:<br>- افرادی که در تعریف سیاستها، رویه‌ها، طرحها، معیارها و ضوابط و تامین منابع شرکت داشتند. | • این افراد می‌توانند از تکنولوژیهای زیر استفاده کنند:<br>- کانالهای ارتباطی که می‌توانند در صورت نیاز رمزنگاری شوند(پست الکترونیک، ویدئو کنفرانس ،نرم‌افزارهای مورد استفاده گروه و وب)<br>- مستندات و انتشارات |
| • از نیروهای زیر برای برآورد توانایی‌های گروه پاسخگویی به حوادث کامپیوتری می‌توان استفاده کرد:<br>- تیم ایجاد کننده گروه پاسخگویی به حوادث کامپیوتری<br>- مدیران اجرایی (مدیران سطح C)<br>- مدیران تجاری<br>- شرکت ثالث فراهم کننده سرویس امنیت<br>- ماموران بازرسی ، کارکنان مدیریت ریسک<br>- ارزیابی کننده هایی مستقل (از سازمان‌های دیگر) | • این افراد می‌توانند از تکنولوژیهای زیر استفاده کنند:<br>- ابزارهای ارزیابی یا تشخیص الکترونیکی<br>- سیستم‌های نوشتن گزارش<br>- سیستم‌های پایگاه داده<br>- کانالهای ارتباطی که می‌توانند در صورت نیاز رمزنگاری شوند(پست الکترونیک، ویدئو کنفرانس ،نرم‌افزارهای مورد استفاده گروه و وب)<br>- سیستم‌های پیگیری حوادث<br>- سیستم‌های گزارش حوادث |

| زیررویه | نیازمندیهای زیررویه | رویه‌های نوشته شده |
|---|---|---|
| PC۹: انجام بازبینی پس از حادثه<br> | • نیروهای معینی یک بازبینی رسمی یا غیر رسمی پس از حادثه انجام می‌دهند و مشخص می کنند چه درسهایی از پاسخ، یاد گرفته شده است و تصمیم می گیرند که آیا باید تغییراتی در رویه‌ها انجام شود یا خیر. | • نیروهای معینی راهنماها، رویه‌ها و قوانین مربوط به سازمان‌های دیگر را مطالعه می‌کنند.<br>• نیروهای معینی راهنماها و رویه‌های مدیریت تغییرات سازمان را دنبال می‌کنند. |

| | | |
|---|---|---|
| | ورودیها<br>تغییرات پیشنهاد شده برای گروه پاسخگویی به حوادث کامپیوتری<br>اطلاعات پاسخ<br>فعالیتها و تصمیمات مربوط به پاسخ<br><br>خروجیها<br>پیشرفت گروه پاسخگویی به حوادث کامپیوتری<br>پیشرفت در حفاظت از زیرساختار<br>مطالبی که فرا گرفته شده است | |
| PC۱۰: تعیین تغییراتی که باید به گروه پاسخگویی به حوادث کامپیوتری اعمال شود<br>  | • نیروهای معینی تغییرات پیشنهاد شده را مطالعه می کنندو تصمیم می گیرند که چه عملی انجام دهند (تغییرات را اعمال کنند یا خیر) | • نیروهای معینی راهنماها و رویه‌های مدیریت پروژه و پیاده سازی سازمان را دنبال می‌کنند.<br>• نیروهای معینی راهنماها، رویه‌ها و قوانین مربوط به سازمان‌های دیگر را ، در زمانی که چگونگی اعمال تغییرات به گروه پاسخگویی به حوادث کامپیوتری را بررسی می‌کنند، مطالعه می‌کنند.<br>• نیروهای معینی راهنماها و رویه‌های مدیریت تغییرات سازمان را دنبال می‌کنند. |

<table>
<tr>
<td></td>
<td>
<table>
<tr><th>ورودیها</th><th>خروجیها</th></tr>
<tr><td>توانایی‌های موجود گروه پاسخگویی به حوادث کامپیوتری</td><td>توانایی‌های موجود گروه پاسخگویی به حوادث کامپیوتری</td></tr>
<tr><td>تغییراتی در جهت اصلاح گروه پاسخگویی به حوادث کامپیوتری</td><td>نیازمندیهای اصلاح گروه پاسخگویی به حوادث کامپیوتری</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>PC۱۰: پیاده سازی تغییرات رویه‌ها<br> </td>
<td>• نیروهای معینی منابع لازم (کارکنان ، تجهیزات و زیرساختار ) برای اعمال تغییرات گروه پاسخگویی به حوادث کامپیوتری را تامین و سازماندهی می کنند.
<table>
<tr><th>ورودیها</th><th>خروجیها</th></tr>
<tr><td>نیازمندیهای اعمال تغییرات به گروه پاسخگویی به حوادث کامپیوتری</td><td>گروه پاسخگویی به حوادث کامپیوتری تغییر یافته</td></tr>
</table>
</td>
<td>• نیروهای معینی، در زمانی که تغییرات در گروه پاسخگویی به حوادث کامپیوتری را اعمال می کنند، راهنماها، رویه‌ها و قوانین مربوط به سازمان‌های دیگر را مطالعه می‌کنند.<br>• نیروهای معینی راهنماها و رویه‌های مدیریت تغییرات سازمان یا گروه پاسخگویی به حوادث کامپیوتری را دنبال می‌کنند.<br>• نیروهای معینی سیاستهای امنیتی و استانداردهای موجود را به هنگام اعمال تغییرات در منابع، تجهیزات و زیرساختار دنبال می کنند.</td>
</tr>
</table>

## ۲ منابع و مراجع


۱. *A STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT*. ۲۰۰۶, European Network and information Security Agency (ENISA). Available at www.enisa.europa.eu/cert_guide/downloads/CSIRT_setting_up_guide_ENISA.pdf

۲. Albert,C , Dorofee,A ,Killcrece, G, Ruefle, R,Zajicek, M. *Defining Incident Management Processes for CSIRTS:A Work in Progress*. Available at www.cert.org/archive/pdf/۰۴tr۰۱۵.pdf

۳. Grance, T,Karent, k,Kim, B., *Computer Security Incident Handling Guide*.

۴. Killcrece, G.,Kossakowski ,K., Ruefle ,R.,Zajicek ,M., *State of the Practice of Computer Incident Response Teams (CSIRTs)*. p. ۲۹۱.Available at www.cert.org/archive/pdf/۰۳tr۰۰۱.pdf

۵. Stikvoort, D,Kossakowski, K,Killcrece, G,Ruefle, R,Zajicek, M. *Handbook for Computer Security Incident Response Teams(CSIRTs)*.Available at www.cert.org/archive/pdf/csirt-handbook.pdf